Government of India
Ministry of Defence
Department of Defence Production

SECURITY MANUAL FOR LICENSED DEFENCE INDUSTRIES (SMLDI)

(Revised in June, 2025)

INDEX

S. No.	Topic	Page No.
1	List of Abbreviations used	7
2	Foreword	9
3	Executive Summary	10
	Category-A	12
4	**Chapter 1- General Provisions, Requirements and Responsibilities** 1.1 Scope 1.2 Authority 1.3 Responsibility of the Management and Employees	13
5	**Chapter 2- Security Organisation and Personnel Security** 2.1 Company Chief Security Officer (CCSO) 2.2 Cyber Information Security Officer (CISO) 2.3 Security Staff 2.4 Responsibilities and duties of CCSO 2.5 Reporting procedure 2.6 Personnel Security	15
6	**Chapter 3- Security of Premises and Physical Security Measures** 3.1 General 3.2 Physical Security Measures 3.3 Layout of Premises 3.4 Reception Office and Visitors 3.5 Material Gate 3.6 Watch Tower 3.7 Setting up of Plant Security Council 3.8 Identity Badges, Entry Passes for personnel /vehicle and Parking of Vehicles 3.9 Keys of the organization 3.10 Late sitting in Office 3.11 Photography 3.12 Carriage of weapons 3.13 Carriage of liquor 3.14 Security measures for Sensitive / Secure/ storage areas for classified equipment 3.15 Building Security 3.16 Emergency response/contingency plan	22
7	**Chapter 4- Material Security** 4.1 Incoming and Outgoing Material 4.2 Inward Material Register 4.3 Material Gate Pass Register 4.4 Material Gate Pass 4.5 Authority 4.6 Gate Pass specification 4.7 Returnable Material Register 4.8 Material sent out register 4.9 Abnormal Delays 4.10 Issue of Gate Passes 4.11 Transfer of classified information	30

	4.12 Items brought by customers/suppliers as samples or for demonstration 4.13 Bulk materials 4.14 Secret Documents 4.15 Material brought on cash purchase basis 4.16 Repair hand tools 4.17 Use of ERP/IFS 4.18 Transportation of Explosive and other classified materials	
8	**Chapter 5- Handling of Documents and Equipment** 5.1 Security classification of Documents and Equipment 5.2 Guidelines on Classification 5.3 Marking of Classified Documents and Equipment 5.4 Accounting of Classified Documents and Equipment 5.5 List of Documents, Checks and Annual accounting 5.6 Care and Custody of Classified Documents and Equipment / Responsibility of holders 5.7 Notebooks of PAs 5.8 Segregation and Care of SECRET Section 5.9 Security Arrangements for SECRET Section 5.10 Guarding - Provision for Lighting 5.11 Duplicating Work. 5.12 Reprographic Equipment. 5.13 Opening and Diarizing of Classified Documents. 5.14 Transmission of Classified Documents 5.15 Emergency Procedures 5.16 Disclosure 5.17 Down Grading, Disposal and Destruction of Classified Documents and Equipment	34
9	**Chapter 6- Communication Security** 6.1 General 6.2 Telephones 6.3 Cell or Mobile Phones /Data Cards /Voice Modems 6.4 Fax Communications	47
10	**Chapter 7- Computer and Cyber Security (Information Systems Security)** 7.1 General 7.2 ISO 27001 7.3 Common Requirements 7.4 Enterprise Resource Planning (ERP) 7.5 Physical and software security 7.6 Acquisition of Computer hardware and software 7.7 Miscellaneous aspects 7.8 Guidelines for computer users or operators 7.9 Instructions for use of Internet within classified area / zone 7.10 Cyber Posture Enhancement via integration with Defence CSOC	50
11	**Chapter 8- Subcontracting** 8.1 General 8.2 Terms and conditions related to classified information 8.3 Engagement of Consultants/Advisers	71

	8.4 Audit Recommendations	
12	**Chapter 9- International Security** 9.1 Imports of Equipment/Materials 9.2 Warning to Consignees 9.3 Handing and Taking Over 9.4 NDA for transfer of classified information between two countries 9.5 Movement	72
13	**Chapter 10- Visits and Meetings** 10.1 Visit of foreign nationals 10.2 Meetings 10.3 Nomination of employees from ILDC to attend Classified Meetings	74
14	**Chapter 11- Training** 11.1 General 11.2 Security briefing 11.3 Training 11.4 Refresher Training 11.5 Security training of Vendors/Contractors and Casual Labourers 11.6 Training of project work Trainees 11.7 Training on Cyber Security	77
15	**Chapter 12- Miscellaneous** 12.1 General 12.2 Publicity and Photography 12.3 Trials / Demonstration 12.4 Rejects and Salvage 12.5 Disaster Management 12.6 Internal Security Audit 12.7 Action on Completion of Audit 12.8 External Security Audit 12.9 Penalty for Non-compliance of security guidelines by ILDC 12.10 Alternate Power Source 12.11 Investigations of compromising emanations 12.12 Retention of Classified Documents Generated Under IR&D Efforts 12.13 Classified Waste Management 12.14 Waste Management 12.15 Compliance Statement	79

S. No.	Topic	Page No.
	Category-B	84
16	**Chapter 1- General Provisions, Requirements and Responsibilities** 1.1 Scope 1.2 Authority 1.3 Responsibility of the Management and Employees	85
17	**Chapter 2- Security Organization and Personnel Security**	87

	2.1 Company Chief Security Officer (CCSO) 2.2 Cyber Information Security Officer (CISO) 2.3 Security Staff 2.4 Responsibilities and duties of CCSO 2.5 Reporting procedures 2.6 Personnel Security	
18	**Chapter 3- Security of Premises and Physical Security Measures** 3.1 General 3.2 Physical Security Measures 3.3 Layout of Premises 3.4 Reception Office and Visitors 3.5 Material Gate 3.6 Watch Tower 3.7 Setting up of Plant Security Council 3.8 Identity Badges, Entry Passes for personnel /vehicle and Parking of Vehicles 3.9 Keys of the organization 3.10 Late sitting in Office 3.11 Photography 3.12 Carriage of weapons 3.13 Carriage of liquor 3.14 Security measures for Sensitive / Secure/ storage areas for classified equipment 3.15 Building Security 3.16 Emergency response/contingency plan	94
19	**Chapter 4- Material Security** 4.1 Incoming and Outgoing Material 4.2 Inward Material Register 4.3 Material Gate Pass Register 4.4 Material Gate Pass 4.5 Authority 4.6 Gate Pass specification 4.7 Returnable Material Register 4.8 Material sent out register 4.9 Abnormal Delays 4.10 Issue of Gate Passes 4.11 Transfer of classified information 4.12 Items brought by customers/suppliers as samples or for demonstration 4.13 Bulk materials 4.14 Secret Documents 4.15 Material brought on cash purchase basis 4.16 Repair hand tools 4.17 Use of ERP/IFS 4.18 Transportation of Sensitive and Classified Materials	101
20	**Chapter 5- Handling of Documents and Equipment** 5.1 Security Classification of Documents and Equipment 5.2 Guidelines on Classification 5.3 Marking of Classified Documents and Equipment 5.4 Accounting of Classified Documents and Equipment	105

	5.5 List of Documents, Checks and Annual accounting 5.6 Care and Custody of Classified Documents and Equipment / Responsibility of Holders 5.7 Notebooks of PAs 5.8 Segregation and Care of SECRET Section 5.9 Security Arrangements for SECRET Section 5.10 Guarding - Provision for Lighting 5.11 Duplicating Work. 5.12 Reprographic Equipment. 5.13 Opening and Diarizing of Classified Documents. 5.14 Transmission of Classified Documents 5.15 Emergency Procedures 5.16 Disclosure 5.17 Down Grading, Disposal and Destruction of Classified Documents and Equipment	
21	**Chapter 6 – Communication Security** 6.1 General 6.2 Telephones 6.3 Cell or Mobile Phones /Data Cards /Voice Modems 6.4 Fax Communications	118
22	**Chapter 7 - Computer and Cyber Security (Information Systems Security)** 7.1 General 7.2 ISO 27001 7.3 Common Requirements 7.4 Enterprise Resource Planning (ERP) 7.5 Physical and software security 7.6 Acquisition of Computer hardware and software 7.7 Miscellaneous aspects 7.8 Guidelines for computer users or operators 7.9 Instructions for use of Internet within classified area / zone 7.10 Cyber Posture Enhancement via integration with Defence CSOC	121
23	**Chapter 8 - Subcontracting** 8.1 General 8.2 Terms and conditions related to classified information 8.3 Engagement of Consultants/Advisers 8.4 Audit Recommendations	142
24	**Chapter 9 - International Security** 9.1 Imports of Equipment/ Materials 9.2 Warning to Consignees 9.3 Handing and Taking Over 9.4 NDA for transfer of classified information between two countries 9.5 Movement	143
25	**Chapter 10 - Visits and Meetings** 10.1 Visit of foreign nationals 10.2 Meetings 10.3 Nomination of employees from ILDC to attend Classified Meetings	145

26	**Chapter 11- Training** 11.1 General 11.2 Security Briefing 11.3 Training 11.4 Refresher Training 11.5 Security Training of Vendors/Contractors and Casual Labourers 11.6 Training of Project Work Trainees 11.7 Training on Cyber Security	148
27	**Chapter 12- Miscellaneous** 12.1 General 12.2 Publicity and Photography 12.3 Trials and Demonstration 12.4 Rejects and Salvage 12.5 Disaster Management 12.6 Internal Security Audit 12.7 Action on Completion of Audit 12.8 External Security Audit 12.9 Penalty for Non-compliance of security guidelines by ILDC 12.10 Alternate Power Source 12.11 Investigations of compromising emanations 12.12 Retention of Classified Documents Generated Under IR&D Efforts 12.13 Classified Waste Management 12.14 Waste Management 12.15 Compliance Statement	150
28	Appendix	155
29	Formats for all the compliances	155
	1. Annexure-I	157
	2. Annexure-II	158
	3. Annexure-III	159
	4. Annexure-IV	160
	5. Annexure-V	161
	6. Annexure-VI	162
	7. Annexure-VII	162
	8. Annexure-VIII	162
	9. Annexure-IX	162
	10. Annexure-X	162
	11. Annexure-XI	163
	12. Annexure-XII	163
	13. Annexure-XIII	163
	14. Annexure-XIV	163
	15. Annexure-XV	163

*****

LIST OF ABBREVIATIONS USED

S. No.	Abbreviation	Full Form
A.1	ANPR	Automatic Number Plate Recognition
A.2	ARC	Authentication Received Chain
A.3	BIMI	Brand Indicators for Message Identification
A.4	CC EAL	Common Criteria- Evaluation Assurance Level
A.5	CCSO	Company Chief Security Officer
A.6	CCTV	Closed Circuit TV
A.7	CDN	Content Delivery Network
A.8	CEO	Chief Executive Officer
A.9	CERT-IN	Computer Emergency Response Team - India
A.10	CISF	Central Industrial Security Force
A.11	CMD	Chairman and Managing Director
A.12	CONFD	Confidential
A.13	COTS	Commercial of The Shelf
A.14	CPMF	Central Para Military Force
A.15	CrPC	Criminal Proceeding Code
A.16	CSA	Competent Security Authority
A.17	CISO	Cyber Information Security Officer
A.18	DDoS	Distributed Denial of Service
A.19	DDP	Department of Defence Production
A.20	DFMD	Door Framed Metal Detector
A.21	DGR	Director General of Resettlement
A.22	DKIM	Doman Keys Identified Mall
A.23	DMARC	Domain-based Message Authentication, Reporting, and Conformance
A.24	DoC	Department of Commerce
A.25	DoS	Denial of Service
A.26	DPIIT	Department for Promotion of Industry & Internal Trade
A.27	DPSU	Defence Public Sector Undertaking
A.28	DSA	Designated Security Agency
A.29	DSC	Defence Security Corps
A.30	GSM	Global System Monitoring
A.31	HQ	Head Quarters
A.32	IAM	Identity and Access Management
A.33	ID	Identification Card
A.34	I(D&R)	Industries Development & Regulations Act
A.35	ILDC	Indian Licensed Defense Company
A.36	IoT	Internet of Things

A.37	IPC	Indian Penal Code
A.38	IPS	Internet Protocol Security
A.39	IR&D	In-house Research and Development
A.40	IS	Information Systems
A.41	ISMS	Information Security Management System
A.42	LAN	Local Area Network
A.43	MFA	Multi Factor Authentication
A.44	MFO	Multi Facility Organization
A.45	MHA	Ministry of Home Affairs
A.46	MoD	Ministry of Defence
A.47	NCIIPC	National Critical Information Infrastructure Protection Center
A.48	NSA	National Security Authority
A.49	OEM	Original Equipment Manufacturer
A.50	OSA	Official Secrets Act
A.51	PC	Personal Computer
A.52	PDCA	Plan Do Check Act
A.53	PIDS	Perimeter Intrusion Detection System
A.54	PSARA	Private Security Agencies (Regulations) Act, 2005
A.55	QA	Quality Assurance
A.56	RAX	Rural Automatic Exchange
A.57	RESTD	Restricted
A.58	SIEM	Security Incident and Event Management
A.59	SOAR	Security Orchestration Automation and Response
A.60	SPF	Sender Policy Framework
A.61	SSO	Single Sign On
A.62	STQC	Standardization, Testing & Quality Certification
A.63	TOP SEC	Top Secret
A.64	UEBA	User and Entity Behaviour Analytics
A.65	VMC	Verified Mark Certificates
A.66	WAF	Web Application Firewall
A.67	WAN	Wide Area Network
A.68	WMIC	Windows Management Instrumentation Code

Foreword

The first revision of Security Manual for licensed defence industries involved in the production of defence products is issued in pursuance of para 12 of the Press Note No.2(2002 series) issued by the Department for Promotion of Industry and Internal Trade (DPIIT), Ministry of Commerce and Industry, Government of India. Presently, licensed defence companies are required to put in place adequate safety and security procedures as per Security Manual for Licensed Defence Industries – 2014 once licence is granted and production commences and this would be subject to verifications by authorized Government agencies.

2. Security Manual is applicable to all Defence Public Sector Undertakings (DPSUs) and the companies which hold Defence Industrial Licence(s)[#] issued by licensing authorities i.e. MHA (Ministry of Home Affairs), DPIIT and DoC (Department of Commerce) under Arms Act, 1959 and I(D&R) Act, 1951.The Defence Licence contains a Footnote to the effect that the licensee company shall fully comply with the security conditions as contained in Security Manual for Licensed Defence Industries and adequate safety & security procedures needs to be put in place by the licensee. The licensee shall follow the detailed instructions issued by the concerned licensing authorities and Department of Defence Production, Ministry of Defence from time to time for strict compliance. This Security Manual therefore, is issued for compliance by licensed defence companies in the private sector as a part of the licensing conditions prescribed in the Industrial License. In the context of this Manual, License means Manufacturing license/Industrial License/Defence License issued by the licensing authorities. Further, the term ILDCs denotes all the private companies which have been issued Defence Industrial License and DPSUs of Ministry of Defence.

3. This Security Manual prescribes minimum standards of security and other safeguards required to be put in place by the licensee in the interest of national safety and security. The contracting agencies such as Service Headquarters/DRDO/DPSUs etc may specify higher degree of cyber security requirements over and above the baseline requirements mentioned in this manual for specific projects based on risk assessment undertaken by them. Specific attention in this regard is also drawn to the Official Secrets Act 1923, particularly Section 2(a) thereof which defines “prohibited place”. All units/ offices/ areas of licensed defence industries in the private sector dealing with any classified information/ document/ material are also “prohibited places” in terms of the provisions of the Official Secrets Act, 1923.

4. Indian Licensed Defence Companies can also have additional security safeguards over and above those prescribed in this Manual, specific to their requirements as considered necessary. The Government (MoD, MHA and their respective agencies etc) may also prescribe additional safeguards, if required, in any particular case and such safeguards would also be required to be followed by the company. Any violation/ non-adherence to any such instructions would be liable for action under the relevant Acts/ Rules/ Guidelines.

5. The companies would be required to follow this Security Manual whenever they undertake the manufacturing of any Defence item for which they have been issued Industrial Licences. The security instructions relating to the category, to which the Defence product belongs, would be applicable in such case.

6. The Security Manual may be revised with necessary consultation as required.

[#] Defence Industrial Licence(s) include Industrial Licence/Defence Licence /Manufacturing Licence as issued by DPIIT, DoC and MHA.

Executive Summary

Introduction

This Security Manual provides the security architecture that needs to be put in place by DPSUs and the Indian defence companies(License holders)in the private sector before undertaking the manufacturing of Defence products for which they have been issued industrial licences by licensing authorities i.e. Ministry of Home Affairs (MHA), Department for Promotion of Industry & Internal Trade (DPIIT) & Department of Commerce (DoC) under I(D&R) Act, 1951 and Arms Act, 1959.The provisions mentioned in the Security Manual have been segregated into two Categories i.e. Category A and Category B. The Category of the items will be specified along with the comments of DDP on IL applications received from DPIIT, MHA and DoC. If any company is involved in the manufacturing of the Defence products which lie in more than one category, then either the company should clearly segregate the areas of operation/ manufacturing for different categories of products and apply the related security instructions or if the areas of operation/ manufacturing are not possible to be segregated, the security instructions applicable to the higher level of security would be applied. Categorisation of the companies/products will be as per orders issued by the MoD from time to time. Presently, the items classified into Category A and Category B broadly includes below mention attributes :–

Category- A: Products that are highly classified and sensitive from the security angle and the manufacturing of these items would require the highest level of security. The illustrative examples of products under this category are arms, ammunitions, explosives, propellants, propulsion, aircrafts, warships, battle tanks, radars, weapons, software and various types of charges.

Category- B: Semi-finished products, sub-assemblies, sub-systems of main weapons/ equipment/ platforms and some finished products of lesser degree of sensitivity. The illustrative examples of products under this category are wing assemblies/ structural assemblies/ barrel assemblies/ turret/ avionics etc.

2. The level of security will depend upon the category of the product that the company intends to manufacture. Under all circumstances, the companies with whom any classified information is shared by the Government as a part of the procurement contract or otherwise would come under the purview of Official Secrets Act, 1923.

Responsibilities of ILDC

The Indian Licensed Defence Company (ILDC) is required to give an undertaking before commencing production of defence products that it shall comply with the provisions of the Security Manual. Simultaneously, the ILDC shall take steps to create the security mechanism and apparatus in its production/manufacturing facility(ies) fully meeting the security standards prescribed in this Security Manual in order to safeguard the security of the Government classified information shared with ILDC as well as materials and end products in all phases of production activity till the end products are finally delivered/handed over to the authorised agency.

The Security Manual contains below mentioned chapters for each category –

I. **General Provisions, Requirements and Responsibilities –** Enshrines general responsibility and requirements by the ILDCs, explains authority of CCSO, CISO, management tier etc.

II. **Security Organization and Personnel Security -** Prescribes role, responsibilities, reporting mechanism of CCSO, CISO, duties of management tier, procedure to be followed in the event of breach of security etc.

III. **Security of Premises and Physical Security Measures–** Prescribes parameters to be followed while designing the Layout of Premises and various other guidelines.

IV. **Material Security–**Prescribes Guidelines regarding Incoming and outgoing Material, Transportation of Explosives and Other Classified Materials.

V. **Handling of Documents &Equipment–** Prescribes Security Classification, Marking of Classified Document and Equipment, Procedure for Accounting of Classified Documents and Equipment Care and Custody

VI. **Communication Security–**Prescribes guidelines on usage of Telephone, Cell/Mobile Phones, checks that have to be ensured and precautions to be followed in Restricted areas

VII. **Computer and Cyber Security (Information Systems Security)–**Prescribes Guidelines for computer users and operators, Instructions on use of Internet, Common Requirements

VIII. **Subcontracting–** Prescribes Guidelines for engagement of Consultants/Advisers,Applicability of Security Manual on subcontracting

IX. **International Security -** Procedure for Import of equipment, movement of equipment; Handing and Taking Over procedures.

X. **Visits and Meetings -** Guidelines on visits of foreign national(s),procedure to be adopted for processing security clearance

XI. **Training–** Describes responsibility of ILDCs to provide Security training and briefing of employees.

XII. **Miscellaneous - G**uidelines on Internal Security Audit, Waste Management, Disaster Management and Compliance Statement.

The provisions of the Security Manual are applicable to CEO/Head of the organisation, CCSO, CISO, Management tier including all the employees of the ILDCs alongwith the contractors, sub-contractors, dealing with the affairs of the company. In the event of non-adherence of security guidelines by ILDC, action shall be taken against the ILDC and/or individual person(s) as per relevant Government regulations/provisions in various Acts, such as IPC, CrPC, I(D&R) Act, Arms Act, OSA 1923 etc.

*****

CATEGORY A

CHAPTER – 1 - General Provisions, Requirements and Responsibilities

1.1 **Scope:**

1.1.1 The Manual is applicable to all Licensee companies engaged in the production of defence products and issued Industrial License by the Department for Promotion of Industry and Internal Trade (DPIIT)/ Ministry of Home Affairs (MHA)/ Department of Commerce (DoC).

1.1.2 This Manual applies to and shall be used by all ILDCs to safeguard Government classified information and materials released to an ILDC, including, but not limited to, such information released during all phases of the contracting, licensing and grant process, bidding, negotiation, award, performance, and termination, or any product, assembly or component arising out of such classified information.

1.1.3 When an ILDC is executing a Govt Project, dealing with classified information, material, document, it will be the responsibility of CEO, who in consultation with CCSO will earmark the areas as classified/sensitive, depending upon the nature of work being carried out in such areas/zones.

1.2 **Authority:**

1.2.1 The implementation of the manual is the overall responsibility of the Chief Executive Officer (CEO) / Head of ILDCs.

1.2.2 Agencies of MHA and MoD are the designated agencies for inspecting and auditing ILDCs who require or will require access to, or will store classified information and materials covered by this Manual.

1.3 **Responsibility of the Management and Employees**:

1.3.1 It is the responsibility of the management and every employee of the company to safeguard the security of all classified information and materials for which the access has been granted in course of duties or which comes into possession in any other way.

1.3.2 It is the duty of each employee of the company to immediately bring to the notice of his superior officer or the Company Chief Security Officer (CCSO), any breach of security regulations in general and/or in particular, any compromise on classified information or materials, either deliberately or inadvertently.

1.3.3 Every employee in the supervisory level is required to ensure, by frequent surprise checks, visits to office rooms and other places where his subordinates work or which they frequent and by all other means in his power, that the instructions laid down for the conduct of business and maintenance of security in company are fully understood and complied with by all of them. It will also be his duty to bring immediately to the notice of his superior officer, or to the officers responsible for security in his department, any instance of breach of security regulations by any member of the staff working under him or in that

department, or of any misconduct, of such a nature as would give rise to doubts about the staff member's integrity/ reliability from the security point of view. The CCSO will maintain the data of all such reported instances along with the Action Taken which will be made available to the external security audit team.

1.3.4 Whenever a new employee joins the company and/or the department, the superior officer of the employee will ensure that the new incumbent has read and understood the contents of the manual and shall take an undertaking in writing to this effect.

CHAPTER – 2 - Security Organisation and Personnel Security

2.1 Company Chief Security Officer (CCSO):

Each ILDC or its multi-location units shall appoint an Indian Citizen as the CCSO, the CCSO should be an ex-Army/ ex-Air Force/ ex-Navy/CPMF/Police Officer who would ensure that security measures necessary for implementing applicable provisions of this Manual are in place and the manual is being implemented in the true spirit of the intention. Persons of Indian Origin and Non-Resident Indians shall be excluded from such appointments. Person with adverse remarks, if any, in his/her release certificate shall not be considered for appointment. The security qualifications of CCSO will be as per Government guidelines issued from time to time. Further, the CCSO will be positively vetted by agencies of Government through Nodal Office, DDP before hiring and after every 3 years. The CCSO will be responsible for framing internal security policies, Internal Audit, Training, Review and up-gradation of Security procedures, Up-gradation of Security Equipment etc., Liaison with other Departments / Organizations, Civil and Law Enforcement Authorities and Intelligence Agencies of Centre and State, etc. The CCSO may be assisted by additional staff based on requirement and size of the company and should report directly to CEO or Executive Head of the Company.

2.2 Cyber Information Security Officer (CISO):

Each ILDC shall appoint/ nominate a Cyber Information Security Officer (CISO). The CISO will be positively vetted by agencies of Government through Nodal Office, DDP before hiring and after every 3 years. The function may be accomplished by one senior officer having necessary and sufficient knowledge on IT system of the organisation in addition to his/her job. In case of company with more than Rs 250 crore turnover, a dedicated CISO shall be appointed. The CISO will be responsible for framing and implementing a suitable Cyber Security policy, conduct of cyber security audit and cyber security training for the organization etc. He shall also be responsible for incident management, identification of the organizations Critical Information Infrastructure assets and interaction with NCIIPC/CERT-In/Nodal Office, DDP and other agencies of MHA and MoD, as the case may be. The CISO must be of sufficient seniority to report directly to senior most management of the organization to ensure functional independence. The CISO may be assisted by additional staff as per the requirement of ILDC. It is the responsibility of the CISO to ensure that the organizational cyber security policy is adequately framed, implemented and audited to ensure necessary and sufficient protection from cyber threats. The CISO shall also clearly identify residual risk subsequent to implementation of requisite cyber security mechanisms.

2.2.1 Following organizational structure for Cyber Security shall be followed in ILDCs:-

2.2.1.1 Duties of Management Tier

The Management Tier, headed by the CEO/MD, assisted by CISO, shall have the following roles and responsibilities: -

a) Responsible for taking executive decisions pertaining to ICT infrastructure for Organisation.
b) Decision making body for overall policy matters.
c) To take strategic decisions and evaluate opportunities in the field of Cyber Security and Cyber Defence, and countering cyber threats.
d) To ensure maintenance and enhancement of the overall cyber posture of the organisation.

2.2.1.2 Duties of Cyber Information Security Officer–

a) Ensuring cyber security posture of the Organisation
b) Implementation of cyber security controls over entire network.
c) Cyber security and incident response.
d) Maintain awareness of emerging threats and vulnerabilities.
e) Implementation of Cyber Crisis Management plan.
f) Internal Information security audit of IT systems and controls
g) Maintaining and updating the threat landscape for the Organisation.
h) Ensuring review of the Cyber Security Policy by the designated expert agency to check for the adequacy and effectiveness of the existing policy in force.
i) Disseminate information security policies, procedures and guidelines to all concerned.
j) The CISO through Cyber Security Division is to ensure that the following activities are carried out at regular intervals: -
    i. Internal Information Security Audit is carried out of all IT Assets on a yearly basis
    ii. Periodic assessment/ audits of third party service providers to assess risks to the Organisation.
    iii. Ensuring that clauses pertaining to Information Security are incorporated into contracts/ agreements/ MoUs with service providers.
    iv. Ensuring that Incidents, especially repeat incidents are investigated and corrective action taken as identified through a comprehensive Root Cause Analysis (RCA).
    v. Implementing automated and continuous monitoring of security incidents and breaches, and maintaining record of the same.

2.2.1.3 Duties of Information Security Officer (At Wing / Division / Section level)

The ISO shall be responsible for the following: -

a) Training & awareness at Division/ Section level.
b) Information privacy at Division/ Section level.
c) Implementation of Cyber Crisis Management plan at Division/ Section level.

d) Information security audit of IT systems and controls at Division/Section level.
e) Ensure that every IT Asset under his/ her administrative control is assigned a custodian.
f) Ensure that an IT inventory file is maintained for the respective Division which will define the details of the IT Asset along with the custodian/ user.
g) Ensure that the changes in the ownership are logged in the IT Asset file. The format for collating the details of IT Assets.
h) Ensure that the IT Assets are not moved out of the respective division for which they were initially allocated without approval of the CISO. However, the same shall be properly documented.
i) Ensure that the policies as laid down in this Cyber Security Policy are disseminated across to all personnel within the division.
j) Ensure strict compliance with the laid down policies with respect to physical security of IT Assets.
k) Comply with the instructions/ guidelines laid down as a part of the Cyber Security Policy.
l) Act as the Nodal Officer for his/ her particular Wing/ Division/ Section as applicable for matters related to Cyber Security.

2.2.1.4 Duties of Cyber Security Division

a) Cyber Security Audits of the Organisation.
b) Function as operations support and emergency response provider in case of Cyber Security incidents with the Organisation.
c) Handling cyber threats, vulnerability detection/ mitigation etc.
d) Advise IT division of the organisation for effective patch management of ICT infrastructure. Issue guidelines for timely dissemination of patches/Hot fixes/Service packs/Updates for IT assets.
e) Formulate and disseminate Cyber Security advisory on latest cyber security threats and trends.
f) Issue security advisories and instructions.
g) Ensure the cyber hygiene and compliance to Cyber Security policies of the Organisation's IT assets.
h) Carry out risk analysis and suggest mitigation measures/ enhancing security of the organisation.
i) Support in formulating Cyber Security policy and carrying out periodic review in consultation with ISO & CISO.
j) Organise periodic training and awareness campaigns for personnel on Cyber Security.
k) Organise seminar/conference on cyber security to brainstorm/assess the current challenges/requirements of the Organisation.
l) Ensuring furnishing of all reports mandated by Security Manual to MHA/DDP/DPIIT/DoC/Nodal Office in DDP.

2.3 **Security Staff:**

The ILDC must employ armed security guards. These guards should preferably be from Defence Security Corps (DSC)/ Central Industrial Security Force (CISF)/ Director General Resettlement (DGR) empanelled agencies having Private Security Agencies Regulation Act (PSARA) License.

2.4 **Responsibilities and Duties of CCSO:**

a) To implement the security provisions as laid down in this Manual.
b) To clearly demarcate the areas as Sensitive/Classified area/zone/manufacturing facility where the work related to MoD Project is going on and ensures that necessary boards indicating such areas are displayed.
c) To keep himself fully conversant with all security instructions and ensure that the security instructions are fully understood by all employees and are implemented or complied with, within their respective sections and offices.
d) To be responsible for the proper conduct, discipline and performance of all the personnel in Security department.
e) To be responsible and ensure that fire service section is fully equipped and personnel are well trained. He shall take prompt action whenever necessity arises.
f) To be responsible for the duties of his subordinate staff and carry out any other lawful and reasonable orders issued to him by management.
g) To carry out periodic surprise checks and maintains a record of such checks.
h) To submit report to the CEO/Head of the sub units/division of the company indicating lapses noticed by him as and when it occurs.
i) To arrange regular programs to apprise the employees on security matters.
j) To maintain constant liaison with law enforcing agencies and nodal offices in Ministries.
k) To carry out improvement in the security system for the premises under his charge, as required, over and above the security manual.
l) To arrange Internal & External Security Audits
m) To carry out a comprehensive personnel risk assessment, short listing of suspects and keeping them on watch list in coordination with HR and Vigilance Department.

2.4.1 When breach of security occurs, the main objectives shall be: -

a) To swiftly find out what has happened and modus operandi of the breach committed.
b) To minimise the damage done.
c) To investigate/ trace the culprit and report to CEO/ head of the company by fastest mode of communication.
d) To prevent recurrence and suggest remedial measures.
e) To report Cyber Attack/Data Breach to CISO.

2.4.2 If classified information or materials have been compromised/ lost/ found in wrong place, it is to be reported by concerned employee immediately in writing to the CCSO who shall take necessary action.

2.4.3 As and when cases of security violations are detected by the Security Staff, the same is to be reported to the CCSO on occurrence. These will be followed immediately by formal violation reports addressed to the head of the department who will thoroughly investigate the matter and furnish an action report within a week.

2.4.4 Enquires to have a tentative time frame by which it will be completed, in addition, progress report shall be submitted to the office of the Company Chief Security Officer till the case is finalized.

2.5 **Reporting Procedure:**

2.5.1 The ILDC shall, at the earliest, report in writing to the nearest Police Station, local office of agencies of MHA and the Nodal Office, DDP regarding any information or materials in regard to actual, possible or probable espionage, sabotage, terrorism, subversive activities or adverse information about any employee(s) in any of the ILDC locations immediately on occurrence. In addition, if the breach has led to data loss/compromise in cyber-security, the same will also be intimated to the Nodal Office, DDP at the earliest. Logs of all security violations/reporting shall be maintained by CCSO /CISO with the corrective actions taken in this regard as shown below -

S.No	Description of violation	Date and Time of incident	Date and Time of reporting to the authorities	Action Taken

2.5.2 The ILDC shall also report to the Nodal Office, DDP the following: -

a) Unauthorized receipt of classified material.
b) Any significant vulnerability identified in the equipment or material being manufactured.
c) Inability to safeguard classified material.
d) Report of loss or suspected compromise.

2.5.3 The ILDC shall forward to designated agency the reports as given below: -

S. No.	**Periodicity**	**Title of Report**	**Report to be rendered**
1	Quarterly	Loss /recovery/ unearthed Arms and Ammunition and Explosives – Annexure-VIII	Nodal Office, DDP
2	Immediately & Quarterly	Fire accidents & other incidents / accidents – Annexure-XII & Annexure-XIII	
3	Quarterly	Visits of foreign business visitors–	

		Annexure-X	
4	Quarterly	Action taken report on, MoD/MHA agencies' visit - Annexure-XI	
5	Quarterly	Cyber Incidents- Annexure-XII & Annexure-XIII	Nodal Office, **DDP**

Incident pertaining to theft, fire, espionage, loss of ammunition etc., will be reported to nearest Police Station and Nodal Office, DDP immediately on occurrence, over and above, the same will be reflected in quarterly report.

2.6 **Personnel Security:**

2.6.1 Every ILDC shall ensure that no security leakage occurs through any personnel due to any reason, including, but not limited to, the following: -

a) For personal gain.
b) For political affiliations.
c) Carelessness in talk and in handling documents.
d) In correspondence.
e) In communication.
f) Transmission of classified documents.
g) Conversations.
h) In case of any breach in the cyber security infrastructure of the ILDC, (National Critical Information Infrastructure Protection) NCIIP / (Computer Emergency Response Team- India) CERT-In/ shall be notified at earliest with a copy to Nodal Office, DDP. The ILDC shall ensure that all requisite information / assistance is provided by its personnel to support activities of NCIIP / CERT-In/ Nodal Office, DDP /other agencies of MHA and MoD.

2.6.2 To ensure that there is no leakage of information it is necessary to observe the precautions given below: -

a) Character and antecedent verification through police, reference checks, previous employment verification has to be carried out for all persons before joining the ILDC.
b) In case any adverse police report is received against an individual dealing with classified matters, on re-verification, generally after every three years, he or she shall be transferred out immediately. Persons employed on TOP SECRET work shall be subjected to prior positive vetting by Nodal Office, DDP, and also every two years thereafter. In case adverse police report pertains to national security, an enquiry shall be initiated by Plant Security Council(defined in para 3.7) under relevant law/act/internal guidelines, the individual shall not only be suspended but also barred from office access during the course of enquiry.

c) Only permanent employees shall be posted in TOP SECRET and in SECRET sections to deal with classified documents.
d) Police Verification shall be conducted i.r.o. all contractual / temporary employees /casual workers, before being engaged.
e) The employees of the company including those of the foreign collaborator, involved in design, development and production of Defence materials shall be cleared from security angle. The list of employees cleared from security angle and engaged by the licensee in design, development and production of defence materials shall be maintained by the licensee and furnished to Nodal Office every quarter. The licensee shall define the code of conduct of such persons.
f) All Officers should abide by the provisions laid down in the Official Secrets Act, 1923 and give a declaration to that effect.

2.6.3 It is the duty of every employee to bring to the notice of CCSO if they notice any suspicious behaviour of employees dealing with classified information like late staying in the office, making copies of document, frequent unauthorized absence, drunkenness and living beyond means etc.

2.6.4 Unconscious leakage due to carelessness or egoism often occurs at all levels, and even senior officers are not immune from this fault. It is the duty of every superior officer to make note of any such faults if any of his subordinates and suitably caution the officer against such lapses.

CHAPTER – 3 - Security of Premises and Physical Security Measures

3.1 **General:**

All Defence related installations automatically fall under category of 'Prohibited Place' under the Official Secrets Act, 1923. A display board to this effect shall be installed in trilingual at the main gate and around, also contemplating 'trespassers shall be prosecuted'.

3.2 **Physical Security Measures**:

Physical security means security in the form of safeguarding the installation which would comprise of providing adequate safeguards against an intruder coming from outside to damage the installation. This includes securing the perimeter walls, gates, lighting, access control system of entry, protection of vital stores and designating restricted areas.

3.3 **Layout of Premises**:

The installation must have perimeter as under

3.3.1 A 10' high wall with 2' overhangs of punched tape, or an anti-scaling device.

3.3.2 The wall should have manned guard posts (bastions) at regular intervals to ensure that the complete area is under observation both by day and night. Alternately, electronic surveillance with motion-detection cameras along with manned controlled room may be put into place for perimeter security.

3.3.3 There should be lighting arrangement all along the perimeter wall to allow clear observation during hours of darkness.

3.3.4 To reinforce manual observation and to have data available for investigation, the perimeter should be covered by CCTV with recording facility for 90 days. The Guidelines issued by Ministry of Electronics and Information Technology (MeitY) on CCTVs from time to time shall be strictly adhere to.

3.3.5 If required, electric fence may be deployed along the perimeter wall. Further, Tunnelling and culvert protection measures shall be undertaken for perimeter security.

3.3.6 If possible the patrolling track should be on either side of perimeter wall so that security personnel manning the watchtowers have clear view of the perimeter wall; besides, they can quickly move to the spot for the problem, if situation so arises.

3.3.7 There should be no construction close to the wall and a distance of minimum 05 mtrs be maintained inside the wall. Wherever possible, no construction zone of 50ft from the compound wall may be maintained. Vegetation near the perimeter wall shall be properly maintained.

3.3.8 There should be minimum number of gates. The material gate should be different from those meant for the employees.

3.3.9 Biometric Access Control system must be installed.

3.3.10 At the employee's gate, there should be provision for Door Frame Metal Detector, Hand Held Metal Detector, separate frisking room for ladies.

3.3.11 The gates must be covered by CCTV.

3.3.12 A control room to monitor the CCTV's be established and manned round the clock.

3.3.13 The administrative area should be well demarcated from the manufacturing area.

3.3.14 Road barriers, speed breakers, boom barriers, Tyre busters etc., be employed at the gate.

3.3.15 Under Vehicle Scanning System (UVSS) to be used for inspecting under carriage of vehicles.

3.3.16 All vulnerable areas/places, perimeter wall, gates, parking area and building/structures should be adequately illuminated.

3.3.17 Sitting of electric poles should not facilitate scaling of perimeter wall / fence by intruder.

3.3.18 'Armed Morchas' shall be placed at all vital entry/exit points including Main gate and Material gate.

3.4 **Reception Office and Visitors:**

3.4.1 Entry of visitors to classified area/zone/office shall be regulated through the Reception Office. The reception shall ascertain the purpose of visit and obtain the concurrence from the officer to be visited. A visitor management system be put in place for issue of photo passes to all visitors. Entry of the visitor in the classified area/zone/office would be authorised by CEO/Head of ILDC for official purpose only.

3.4.2 No visitor would be allowed to carry laptops, pen drives, mobile phones and any kind of storage devices or Bluetooth devices inside the premises. Entry of such items could be allowed only to non-classified area for the purpose of meetings that too on specific permission of CEO/CCSO of the installation.

3.4.3 Visitor's vehicle shall not be permitted to enter in the installation and would be parked at designated parking areas for visitors. If required, the visitors shall be taken to the designated classified area/zone/office in vehicles; specially used for such purposes by the concerned office/company or organisation.

3.4.4 The visitors will, at all times, be escorted during their visit to the classified area/zone/office and will not be left unattended or unescorted. The visitor shall not be allowed to leave the reception office without an escort.

3.4.5 Official visitors from Ministry of Defence, Government of India, MHA in possession of valid ID cards will also be issued with the visitors ID card at the reception office; however, such visitors need not be escorted inside the classified area/zone/office.

3.4.6 No visitor shall be entertained after working hours. In exceptional circumstances where a visitor has to stay beyond the specified time, clearance of designated officer as decided by CCSO should be taken and security should be kept informed of the same.

3.4.7 Security Control room shall be situated near the factory main gate.

3.4.8 Medics: First Aid Room to be set up.

3.5 **Material Gate**:

Entry & exit of all material, raw, processes, garbage and scrap must take place only through the designated gate, which, as far as possible, should be divested from the employees. Provision of Weigh Bridge be made at the material gate

3.5.1 Communication: Gates are required to be connected to the security control room besides the office and residence of the security officer through a communication network that is dependable and operational around the clock. Also, alternate means of communication in the form of radio telephony should be available at the gates/ watch towers to ensure uninterrupted communication.

3.6 **Watch Tower**:

The following points need to be kept in mind while siting and constructing watch towers:

(i) Sighting: Watch towers should be sited tactically so that the area around is dominated with clear visibility towards both the adjacent towers. There should be no dead ground or blind spots between any two towers. In case of any dead ground, the area should be covered with artificial obstacles.

(ii) Height: Depending on the height of the perimeter wall and the construction around and within the installation, the height of the watch tower from the ground should be at least 15’ to 20’ in order to provide a clear field of observation all around.

(iii) Staircase: The stair case leading to the watch tower should be made in such way that the security personnel on duty do not find any difficulty in negotiating the same while carrying their weapons and other equipment.

(iv) Sentry Post: The cubicle on the top of the watch tower should facilitate in the performance of watch duties of the sentry and also allow him to use his weapon effectively when the need arises:

a) The walls should not be more than 4 feet.
b) There should be protection from incoming harsh sunlight and rain.
c) The size should permit the sentry adequate space for movement.
d) In case windows are provided they should have wide angles for maximum observation.

e) Lighting inside the post should be avoided to prevent outsiders from keeping a watch on the movement of the sentry and also facilitate a clear and effective observation of the area during hours of darkness / poor visibility.

(v) Vision Devices: Day and night vision devices may be provided to the sentries based on the criticality of the installation and the assessed threat perception. Watch Towers may be equipped with dragon lights, Walkie-Talkie sets/intercoms and High mast light/revolving flash lights etc.

3.7 **Setting up of Plant Security Council:**

A Council to be constituted under the chairmanship of Head of Unit with CCSO as member Secretary, CISO as a permanent member and other divisional/section heads as members. The Council shall meet quarterly and review the existing security requirements/arrangements and take corrective actions. In case of Multi Facility Organisation, Headquarters security representative will also be included as a member in the quarterly reviews. The Record of the proceedings shall be maintained by the company.

The council may also bring to the notice of Local Police/Nodal Office of DDP any cases pertaining to security violation, theft/pilferage, espionage, sabotage, terrorism, subversion activities or adverse information about any employee.

3.8 **Identity Badges, Entry Passes for personnel /vehicle and Parking of Vehicles**:

Entry into Classified zone/area/offices would be regulated on the basis of photo Identity cards issued by the CCSO. The Identity Badge should have following details:

a) Company logo
b) Name and photograph of the employee
c) Staff Number and pass number
d) Signature of issuing authority
e) Blood group
f) Date of issue and validity
g) Signature of employee
h) Address of Unit

3.8.1 These ID cards are to be returned to CCSO on the date of expiry of their validity or when no longer required. The identity badges should be reissued once in 5 years so that latest photo is reflected on the badge. The Security Department should keep relevant account of badges issued. All employees shall follow the following instructions: -

a) Every person, irrespective of designation, rank and status will display his or her Identity Card or any other identity document issued by the CCSO for verification by the security personnel on duty at all times while inside classified area/zone/office.

b) Impersonation of the authorised holder of identity card or its alteration, destruction or transfer to another person would be a punishable under relevant laws.

c) In case any individual found within the classified area/zone/office is notable to produce his or her identity card or pass, he or she will be brought to the office of the CCSO for necessary further action.

3.8.2 Other than the Identity cards for the permanent employees working in the classified area/zone/office, the CCSO may also issue following Identity documents: -

a) Temporary Photo Identity Card: To be issued to personnel of the company or organisation who are working in the classified area/zone/office on temporary basis or for a short duration.

b) Visitor Pass: A list of officers who are authorised to receive visitors as per the Company rolls shall be available at reception. Passes would be issued using Visitor Management System by the reception/security office on production of a valid identity photo document by the visitor (like passport, services ID card, driver's license, PAN card, Voters I card). The pass should be returned by the visitor at the gate on completion of the visit and endorsement of time and signature by the officer visited upon is to be checked. Online system should be in place for min 1year retention and tracking of visitor details along with the photo for future analysis / investigations required if any.

c) Labour Pass: Labour pass with photo would be issued by the office of CCSO for casual labourers who are working for a specific period/term. These passes should be issued to labourers whose character and antecedents have been verified by the police.

d) Token labourer: Tokens should be issued on daily basis for labourers employed for constructions/other duties. The contractor employing such labourers should be accountable & responsible for such casual labourers for the duration of working inside the plant. To this effect, an undertaking may be obtained from the contractor.

3.8.3 Vehicle Stickers: Vehicle stickers would be issued by the CCSO to employees who are on permanent basis and who have a valid photo ID card issued by the CCSO for parking in designated area outside the installation.

3.8.4 Loss of Identity Cards: Loss of ID card should be reported immediately to the CCSO along with an investigation report from the concerned section/office. CCSO may thereafter take further necessary action as per the policy of the company/office/organization. A database of stolen/lost ID cards will also be maintained with proper and regular Cyber audit of the computers used in the issuance of ID cards.

3.8.5 All sections shall maintain a list showing name, designation, identity card number, local resident address and permanent home address contact number of the employees working in area/zone/office handling classified information.

3.8.6 The ID card, vehicle sticker and any other documents issued to an employee would be withdrawn and submitted to the CCSO prior to dismissal, suspension or transfer of the employee.

3.9 **Keys of the Organization:**

3.9.1 Keys to the offices rooms/areas/zones holding classified information should be kept in a secured designated placed at the office of CCSO. The access to the secured designated place will be strictly limited. The keys can be drawn or deposited by an employee who has been authorised to do so by the head of department/officer in charge of the section or office. While authorising employees to draw the keys, it would be ensured that rotation system is followed and casual labourer is not detailed for opening and closing duties. In case of loss of keys, the matter shall be reported to the CCSO. Key registers shall be maintained for record.

3.9.2 Prior to submitting the keys, the nominated person shall ensure that all the windows are closed and window blinds and curtains are open to detect any unauthorized movement / fire.

3.9.3 A Team under CCSO should carry out random checks of the rooms after office hours to find security lapses, if any, on the part of the occupants of the rooms after they leave the premises.

3.10 **Late Sitting in Office:** Staff may sit in their office in the classified rooms/areas/zones under supervision of an officer. In case any staff is required to work on Holidays, or beyond stipulated working hours, a letter authorising him to do so would be sent to the CCSO by the departmental head. However, work classified as TOP SECRET and SECRET can only be performed under the supervision of an Officer. The person so authorised shall also be responsible for drawing and submitting of the room keys.

3.11 **Photography:** Photography/Videography on ground or aerial (through drones/UAVs) wherein any work related projects/ manufacturing of MoD is being carried out will not be permitted without the approval of MoD. Warning sign boards to this effect shall also be displayed at the main gate as well as inside the premises at vantage points. The guidelines of Ministry of Civil Aviation on Drone/ Drone threats issued from time to time shall be strictly adhere to.

3.12 **Carriage of Weapons:** Carriage of weapons, other than by the staff of CCSO would be strictly prohibited inside the Classified Zone/Area. Permission may be accorded to official security guards of visiting personnel, after obtaining specific prior permission of the CCSO. A kote is to be made near the office of CCSO where weapons can be stored and only authorised supervisor cadre is allowed to operate.

3.13 **Carriage of Liquor:** Carriage and consumption of all kinds of liquor(including beer, wine and all alcoholic drinks) would be strictly prohibited inside the plant.

3.14 **Security Measures for Sensitive / Secure / Storage Areas for Classified Equipment:**

The storage area may be declared as Vital Point with the following safeguards: -

a) Additional Boundary Wall and Power Fence to prevent any intrusion, if required.
b) Access control for authorised personnel through photo identity and/or proximity/smart/biometric card based systems.
Biometric Access Control System must be installed at vital/sensitive points. Further, facilities shall devise second level access authorization for entering the operational area/server room.
c) Frisking and Baggage screening of employees of persons moving in/ out of the Vital Point shall be enforced.
d) Banning electronic gadgets, cameras, storage devices inside the Vital Points shall be enforced. Carrying of Smart phones high-end mobiles with cameras and other features also to be banned.
e) Patrolling in and around the Vital Points including night patrolling by Guards and Dog squads if required shall be carried out. Night patrolling should be mandatorily provisioned at staggered intervals covering the entire perimeter along with vital points.
f) CCTV surveillance must be provided at entry / exit of Vital Points and other sensitive locations inside the factory. Recording of all CCTV footage should be kept for 90 days.
g) A two key system may be used for stores holding sensitive hardware wherein two authorised persons, one from Security and the other from stores / user Department, may be detailed.
h) Suitable fire-fighting and Emergency / Disaster management measures to be instituted.
i) Proper fool proof access control to be established.
j) ILDC should ensure that adequate fire-fighting mechanism is in place so as to ensure that no untoward incidents happen in the premises due to fire.

3.15 **Building Security:**

It shall be ensured that the buildings are constructed at least 05mtrs away from the compound wall so that there is no intrusion from outsiders. Wherever possible no construction zone of 50 ft from compound wall may be maintained.

3.16 **Emergency response/contingency plan:**

In the event of emergencies like accidents, terror attacks, strikes, etc. the following procedure is to be followed:

a) Activation of control room with immediate intimation to police and local authorities and a team of other officers, disaster management mechanism to be activated for taking charge of the situation.
b) Display of contact details along with telephone numbers of the higher officials.

c) Display of contact details of local police, special branch, hospitals, bomb disposal team and local authorities in conspicuous places within premises of ILDC besides at security control rooms.

d) Emergency exits/ route plan to be identified.

e) The above actions should be in accordance with the Disaster Management Plan as per the guidelines/instructions issued by the National Disaster Management Authority/State Disaster Management Authority.

CHAPTER – 4 - Material Security

4.1 Incoming and Outgoing Material:

No railway car, truck or other vehicle conveying crates, boxes, machinery, repair parts, fuel or other material should be admitted to the plant without first being examined and thoroughly searched by a guard for concealed explosives, contraband items, incendiary devices or other hazardous items. No material should be allowed to go out of the factory area without a proper pass from an authority authorized for the purpose. Such authority should be restricted to a few officers only and their specimen signatures should be available at the gate for easy and quick identification. Computerized Material Management System (CMMS) for returnable/non-returnable goods shall be installed for generating gate pass and data backup.

4.2 Inward Material Register:

Entry will be made in the register in respect of all materials that come into the plant, either brought by the contractors as sample, or brought by the stores officers as supplies/samples, for which inward materials gate pass has been issued by the security gate officers. Samples and such other materials taken back should be crossed out after the party has returned the inward materials gate pass.

4.3 Material Gate Pass Register:

This register shows materials that went out of the factory under an authorized gate pass. The time and nature of materials sent out and brought back be recorded by the gate staff. The time of return however should be noted. A specimen signature book showing the signature of the officer authorized to sign passes should also be maintained.

4.4 Material Gate Pass:

A model material gate pass procedure is given below. The ILDC should, as far as possible, evolve a proper gate pass procedure to suit the conditions prevailing in the respective divisions and get it issued under the signature of the competent authority for compliance: -

4.4.1 <u>Description of material gate pass</u>

There will be two types of material gate passes, viz.

(a) Non-returnable material gate pass; and

(b) Returnable gate passes.

4.4.2 A non- returnable gate pass should be issued for the materials, which are taken out of the factory on permanent basis or for materials issued to sub-contractors etc.

4.4.3 A returnable gate pass will be issued for materials, which are sent out of the factory on returnable basis. Returnable gate pass will be issued only to such

materials, which will come back in the same form without undergoing any change. For finished goods and items against customer order, gate pass will be issued only by the stores.

4.5 **Authority:**

The CEO/Head of the Organisation will authorise a limited number of Officers who will be authorised to sign the material gate passes. The specimen signatures of authorised officers signing the material gate pass will be made available at the security gates.

4.6 **Gate Pass Specification:**

The concerned officer of the security department in charge of the guard room should take the following action: -

(a) Verify the signature in gate pass with the specimen.

(b) Check the materials as per the gate pass.

(c) Affix security outward seal and attest his signatures on the gate pass.

4.7 **Returnable Material Register:**

Control SL. Nos. Should be given to the gate passes for taking out returnable materials A 'RETURNABLE MATERIAL REGISTER' should be maintained by the officer in charge. Proper entries should be maintained giving the reference numbers of the gate pass, authority for sending out materials.

4.8 **Material Sent Out Register:**

It is the responsibility of the department concerned to account for the materials sent out. Proper register should be maintained giving the reference number of the gate pass, authority for sending out materials.

4.9 **Abnormal Delays:**

The material sent out on returnable basis should be brought back within the stipulated period mentioned in the gate pass. Cases where there is abnormal delay will be brought to the notice of the concerned departmental head by CCSO for taking suitable action. All abnormal delays will be documented with specific reasons.

4.10 **Issue of Gate Passes:**

Gate pass should be issued to all materials including stationary items taken out of the gate.

4.11 **Transfer of Classified information:**

When drawing in CDs/any electronic form are exchanged with subcontractors/ vendors in case outsourcing activity involving technology transfer of classified projects or indigenous classified projects for manufacturing components, it should be sent in sealed cover with material gate pass signed by authorized personnel. The CCSO will authorise a person for supervising the movement of such information.

Sealing & dispatch should be done appropriate to the classification of projects. The subcontractor/vendor who has been given any classified project or information would also be bound by the provisions under "Official Secrets Act, 1923".

4.12 **Items brought by customers/suppliers as samples or for demonstration:**

Items brought by customers/suppliers as samples or for demonstration/try out/rectification/repairs etc. should be allowed 'INWARD GATE PASS' by 'Security in-charge' at gates. The materials will be allowed to be taken out on the same gate pass after making proper entry in the office copy of the INWARD GATE PASS book. This procedure will be applicable to materials brought as samples. In case any electronic item(s) is/are brought inside by the customers or suppliers as samples or for demonstration/try out/rectification/repairs etc., it/they shall be authenticated through the CISO.

4.13 **Bulk materials:**

For bulk materials brought by contractors for their work, a proper gate pass should be issued for taking out the balance materials giving reference of the INWARD GATE PASS issued by the security department.

4.14 **Secret Documents:**

The officers of the civil engineering department, purchase department and technical department should ensure that graded official documents of any nature including blue print should not be sent out without gate pass. A broad outline of instructions on handling of classified documents and safe guarding against the exchange of information is given at chapter-5.

4.15 **Material brought on cash purchase Basis:**

Certain materials are purchased on cash purchase basis. Once a gate entry is made for such materials the materials should also be taken out only on material gate pass. This is accounting for control purpose.

4.16 **Repair hand tools:**

Hand tools by plumber, electricians and mechanics of transport department who attend to repair will be taken out after making proper entries in the register maintained at the guard room.

4.17 **Use of ERP/IFS:**

A system to be evolved for recording & tracking of materials using ERP/ IFS.

4.18 **Transportation of Explosive and Other Classified Materials:**

a) There shall be empanelment of only security vetted transporter/carriers and drivers verified through local police for transportation of classified material/sensitive goods.
b) In order to avoid any sabotage en-route it should be ensured that the vehicles carrying explosives and classified materials are escorted by armed guards.
c) Secrecy should be maintained about the transportation plans/date/route etc.

d) Constant communication should be maintained while transporting explosives and classified materials.
e) It is the responsibility of the company to hand over classified material/finished product to the rightful owner, i.e. purchaser.
f) Superintendent of police of the districts falling on way should be kept informed about transportation of explosive and classified materials. Consignor as well as consignee would keep the Superintendent of Police of the district falling on way between the place of consigner and the place of consignee informed.
g) When classified Equipment is sent by road in India, the vehicles will, as far as possible, be harboured during the night in Military unit en-route. The information for such an arrangement has to be forwarded to MoD well in advance of the planned movement, to arrange for the necessary security clearance with the military authorities concerned. In absence of Military units, they will harbour within civil police station. Where neither of the two courses is possible, the dispatching authority will approach the civil authorities through their higher formation, for affording security protection and other assistance to the convoy en-route. The superintendent of police of the district falling on the way between the place of consignor and the place of consignees should to be informed. GPS tracking devices on the equipment / vehicles to continuously monitor the movement of classified materials / equipment may be installed.

CHAPTER – 5 - Handling of Documents and Equipment

5.1 Security Classification of Documents and Equipment:

5.1.1 Aims & objective of Document / equipment Security: To prevent a spy or an enemy agent from access to classified information/ equipment, to help CCSO in investigations into cases of leakage and spying and to implement the theory of security based on the principle of need to know, need to take and need to retain. Besides, classified document should be kept in such a secure place, where only authorized officials should have access.

5.1.2 Matters related to suspicious cases of leakages of classified information/theft should immediately be informed to CCSO and head of the company for a thorough investigation, taking serious view of such security lapses and breaches, dealing appropriately against delinquent official / person. However, outcome of investigations should be reported to CCSO and head of the company, for taking preventive and remedial measures for strengthening the security system.

5.1.3 **Classification of Documents and Equipment:** A clearly laid out Data Classification policy shall be put in place by ILDC. Absence of policy and its implementation shall be treated as a violation of this Manual. Documents and equipment shall be classified as follows: -

a) TOP SECRET: "TOP SECRET" shall be applied to information and equipment, the unauthorized disclosure of which could be expected to cause exceptionally grave damage to the National Security or national Interest. This category is reserved for the nation's closest SECRETs and is to be used with great reserve.

b) SECRET: "SECRET" shall be applied to information and equipment, the unauthorized disclosure of which could be expected to cause serious damage to the National Security or National Interests or cause serious embarrassment to the Government in its functioning. This classification should be used for highly important matters and is the highest classification normally used.

c) CONFIDENTIAL: "CONFIDENTIAL" shall be applied to information and equipment, the unauthorized disclosure of which could be expected to cause damage to National Security or could be prejudicial to the National Interests or would embarrass the Government in its functioning.

d) RESTRICTED: "Restricted" shall be applied to information and equipment which is essentially meant for official use only and which should not be published or communicated, to anyone except for official purpose.

e) UNCLASSIFIED: The designation UNCLASSIFIED is used to identify information and equipment that does not require a security classification.

Note: Documents or equipment not covered by any of the above categories shall be regarded as unclassified.

5.2 **Guidelines on Classification:**

5.2.1 A document should be given a classification which it really deserves. Over classification or under classification can be detrimental.

5.2.2 If a document or equipment bearing higher security classification is added to a file, document or material, the file/document/ material itself will be upgraded to that classification.

5.2.3 The document or equipment as a whole shall bear the highest security grading that any particular part of it may deserve. The grading of a file or of a group of physically connected documents or materials must be that of the higher graded document/ material therein.

5.2.4 Officers authorized to classify: The originator of the document will be authorized to classify the document / upgrade / downgrade the same. It is the responsibility of the originator that care is taken of such documents so that the same do not fall in the wrong hands. The overall responsibility of safeguarding classified documents will be of the CEO/ head of the company who shall take all necessary precautions / audits / review mechanisms as deemed fit. The level of officer in a company to initiate/handle classification of classified documents (Top Secret, Secret, Confidential & Restricted), should be designated by the CEO/Head of the Company.

5.3 **Marking of Classified Documents and Equipment**:

The classified documents and equipment shall be prepared and marked as per the guidelines described below, as applicable, in the following manner:

5.3.1 All documents including Files, folders, binders, envelopes, and other items containing classified documents, noting of the file containing classified matter will have the security classification printed, stamped or typed in bold capital letters on the top and bottom centre of each page of the document. Any insertions, such as maps, or illustrations of an individually classified nature will also be similarly marked.

5.3.2 File covers containing TOP SECRET documents will be marked with a diagonal Red Cross of one cm in width thickness extending from corner to corner on both the front and back covers.

(a) A separate record of all TOP SECRET case files will be maintained in a register of TOP SECRET documents and docketed by the authorized officer. He should also carefully monitor movement of such files.

(b) Even part files, if opened in relation to any classified document, will have the same security classification and will also be properly docketed.

5.3.3 SECRET files covers should carry a red vertical line in the centre.

5.3.4 TOP SECRET, SECRET, CONFIDENTIAL OR RESTRICTED drawings or tracings are to be marked in such a manner that the marking will be reproduced along with the main text whenever copies are made there from.

5.3.5 TOP SECRET, SECRET OR CONFIDENTIAL maps and charts are to be marked under or near the scale. For marking by stamp, red endorsing ink pads are to be used.

5.3.6 TOP SECRET documents should, wherever feasible, be printed or written on coloured paper, so that they may be easily recognized.

5.3.7 Marking for ILDC Developed Information and Equipment: Any information or materials arising in any manner out of classified information released to an ILDC shall be treated at the same classification level as was attached to the original information or material released.

5.4 **Accounting of Classified Documents and Equipment:**

5.4.1 Reference Number: Classified documents and equipment shall be given code or other reference number, which will be used in correspondence to avoid reference to their titles and subject matter.

5.4.2 Copy numbers or Receipts or making of Spare Copies. The following important aspects shall be kept in view in this regard: -

(a) When more than one copy of TOP SECRET document is made, they shall be given copy numbers and each page shall be serially numbered.

(b) The transmission of TOP SECRET and SECRET documents shall be covered by a receipt system. The sender shall enclose a receipt for completion and return to the sender by the addressee.

(c) If the receipt for a classified document does not reach the issuing authority within seven days, the issuing authority shall ascertain whether the document has in fact been received, if not the same to be reported to CCSO.

(d) Letters or documents including appendices, if any, shall have continuous page numbers. The total number of pages of a TOP SECRET or SECRET letter or document will be indicated in words below the security classification on the top centre of the front page.

(e) The Typist besides noting down his initials at the foot of each classified paper typed by him/her, should also note the number of copies made.

(f) Whenever a TOP SECRET document is required for preparation of additional copies for simultaneous examination, the same may be made after obtaining order in writing from the CEO/ Head of the ILDC. It is, however very essential that the originator be informed along with its distribution.

5.5 **List of Documents, Checks and Annual Accounting**:

5.5.1 All personnel who are holding classified documents and materials shall check all accountable classified documents and materials, and render certificate of safe custody on 31st Dec of each year to the next Superior officer. A copy of the certificate will be sent to the CCSO.

5.5.2 Two security inspections and verification shall be carried out, one by the Officer in charge of the section/wing/department/unit and another by the CCSO during the calendar year. A physical verification of all the classified files and materials shall be carried out during these inspections.

5.5.3 During the checking or inspections, the officers shall recommend destruction of classified papers and materials, wherever required.

5.5.4 A separate Diary and Dispatch book shall be maintained for TOP SECRET and other classified correspondence.

5.5.5 While making cyclostyled copies of SECRET or CONFIDENTIAL documents, a register indicating the number of copies, their copy numbers and to whom issued, would be maintained. The copy shall be made in a controlled environment under supervision.

5.5.6 End of Day Security Checks

a) ILDCs that store classified material shall establish a system of security checks at the close of each working day.

b) ILDCs that operate multiple work shifts shall perform the security checks at the end of the last working shift.

5.6 **Care and Custody of Classified Documents and Equipment /Responsibility of Holders**:

ILDC authorized to store classified documents and equipment shall establish and maintain a system to deter and detect unauthorized intrusion or removal of classified documents and equipment from their facility. Personnel who have a legitimate need to remove or transport classified material should be provided with appropriate authorization for passing through designated entry/exit points.

5.6.1 All categories of classified documents and equipment will be regarded as under the personal charge of the individual to whom the same is issued as recorded and by whom a receipt has been given.

5.6.2 Other Classified Documents and Equipment will be regarded as under the charge of the person to whom the custody of these documents and materials has been entrusted by the Head of the office concerned.

5.6.3 Individuals in charge of Classified Documents and Materials are responsible for their safe custody and their disclosure is limited to only those required to know. The concept of need to know to be followed.

5.6.4 Proper handing /taking over of all documents to be carried out whenever an individual is transferred or superannuating.

5.6.5 In case any employee transferred from one classified section to other section, an undertaking should be obtained from the employee that "No information regarding the functional aspects of the section, cases or reference of any cases will be discussed / disclosed by him / her.

5.6.6 The holders of classified documents will carry out periodic checks.

5.6.7 Classified documents will not be studied in the presence of a person who is not entitled to see them or left exposed during the absence of the authorized holder.

5.6.8 When an individual is the sole occupant of a room and during working hours leaves the room for a short period/lunch hour, he must ensure that all TOP SECRET documents are locked in safes or cupboards.

5.6.9 The last two officials/late hour duty officers leaving the office will ensure that almirahs, drawer of tables containing classified documents inside the room / office are properly locked and that no document / paper has been left inside / on table, floor of the room and also in waste paper basket. They will deposit the sealed key to the Caretaker with proper entries.

5.6.10 No single official will open the almirah containing classified document in the office while joining the office in the morning.

5.6.11 The following instructions will always be strictly observed: -

a) When it is necessary to open a safe, it will be opened for the shortest possible time and locked immediately.
b) Keys, receptacles containing classified documents will be invariably carried by the person responsible for the receptacle.
c) Duplicate keys should be kept in a sealed packet which will be in the custody of a nominated officer. A yearly report regarding this should be sent to the CCSO. The Duplicate keys will not be drawn in normal circumstances and shall be with the approval of CCSO only. The keys can be drawn or deposited by an employee who has been authorised to do so by the head of department/officer in charge of the section or office. While authorising employees to draw the keys, it would be ensured that rotation system is followed and casual labourer is not detailed for opening and closing duties. In case of loss of keys, the matter shall be reported to the CCSO. Separate duplicate key registers shall be maintained for record.
d) In case of loss of a key, the matter should be immediately reported to CCSO and concerned lock should be changed. Even if the key is recovered subsequently, it should be regarded as compromised and a fresh lock and key should be issued with proper record.
e) Keys should, where possible, be passed from hand to hand only. Should it be necessary to transmit a key by post, it will be made up into a

package so that the contents cannot be recognized, and will be handled according to the highest category of document contained in the safe.

f) The company security staff must check employees / staff carrying briefcase, purses at exit/entry to see that no official takes out/in any classified paper without written authority from the Competent Authority.

g) All almirahs containing classified documents will have a cross marking on it and it shall be written as "to be removed first in case of fire".

5.7 **Notebooks of PAs:**

5.7.1 Note-books after utilization of PAs should be returned to the officer under whom he works who will keep it in his personal custody and destroy it after the expiry of three months from the date of the last entry in the note book.

5.7.2 The Short-hand note books should remain in the custody of the officer. After typing out the dictation, the PA should return it to the officer. In no case will it be kept in the locker provided to the PA for storing stationery etc.

5.7.3 Any notebook, disc, tape, film, cassette laptop, PCs etc. which has been used to record classified material, should be treated as a classified document and should be kept in the custody of the officer. Classified work done on Laptops, PCs will not be stored in the hard disk or CDs and zip drives etc. If used, these will be handled as per the security classification of data contained therein.

5.8 **Segregation and Care of SECRET Section:** Any branch/ department or sections dealing with classified documents (i.e. Top Secret, Secret, Confidential and Restricted) must segregate its SECRET sections from the non-SECRET sections. There must be adequate provision of steel safes for the custody of classified documents in SECRET sections. Doors of rooms of these sections shall be provided with security locks of proper make and quality in addition to the existing inset locks. Non adherence to this Provision shall be viewed as violation and shall entail punitive action.

5.9 **Security arrangements for SECRET section:** The window or the skylight of the SECRET section should be fitted with wire netting or Iron bars and, if it is accessible from outside, it should, in addition, be fitted with strong wire meshing. Lighting arrangements both inside a section dealing with classified documents and in the corridors approaching it, should be adequate.

5.10 **Guarding - Provision for Lighting:** There must be provision of adequate guards both by day and by night to prevent the entry of unauthorized persons. The officer in charge of such a section shall ensure that only authorized persons have legitimate access to his section. If a paper is brought by a person not authorized to enter the SECRET Section, arrangements should be made for such paper being taken into the section without the person concerned being allowed access to the room.

5.11 **Duplicating Work:** Offices or Branches or Sections using Xerox and Photostats Machines etc., shall keep a record of all classified duplicating work done in their respective offices. The supervision of duplicating work will be done in accordance with the following: -

(a) Whenever any TOP SECRET letters or documents are required to be photocopied or cyclostyled, it would be done under the personal supervision of the custodian of the TOP SECRET documents.

(b) Xeroxing a classified document of Top-Secret nature should be facilitated through a requisition slip duly signed by a designated officer by the CEO/ Head of the Company, with proper record maintenance at Reprography section. Similarly, in case of Xeroxing confidential document, requisition slips shall be signed by a senior officer authorized by the CEO/ Head of the Company.

5.12 **Reprographic Equipment:** The reprographic equipment shall be under the personal custody of an officer. It shall be located in his room and he shall be personally responsible for the custody, operation and accounting of the documents reproduced. Any change of the officer or change of location of equipment should immediately be reported to the CCSO, whose personnel shall make periodic checks to verify the system of the accounting. The machine should always be kept under lock, while not in use.

5.13 **Opening and Diarizing of Classified Documents:**

(a) Opening

(i) On receipt of TOP SECRET documents the inner cover will be handed over by the opening personnel to the Officers. All TOP SECRET covers will be opened by the addressee or in his absence by the officer officiating for him.

(ii)SECRET or CONFIDENTIAL documents will be opened either by the addressee or a person so authorised by him.

(b) Diarizing

(i) The diarizing of all TOP SECRET documents shall be carried out either by the officer to whom it is addressed or by his personal staff so authorised by him. The diarizing of SCERET documents may be entrusted to the lower level at the discretion of the concerned officer. The responsibility of the safe custody of the documents will, however, rest with the officer concerned

(ii) The diarizing of CONFIDENTIAL documents may be carried out by selected nominated office staff.

5.14 **Transmission of Classified Documents:**

(a) Preparation of Envelopes

i. TOP SECRET, SECRET and CONFIDENTIAL documents will be sent in two envelopes. To assist the recipient in verifying that there has been no tampering in transit, the inner envelope will invariably be a new one. The outer envelope will bear only the address, and will not be marked with the security classification of the contents. The inner envelop will be marked with the appropriate security classification, and if TOP SECRET, it will also be marked "to be opened personally by or officer officiating" (the holder of an appointment or the name of the individual being stated).

ii. In respect of TOP SECRET and SECRET documents, the dispatcher shall sign the inner cover at two prominent places (e.g. joint-line or the flap), with his name, date and time of dispatch clearly written. The time of dispatch would also be indicated in the dispatch register. The receiver shall scrutinize such covers carefully to ensure that no undue time has been taken in receipt and shall clearly indicate the time of receipt in the register of the receipts.

iii. In every case, where single envelope is used, the appropriate classification of the enclosed document will be marked on the envelope, except when Restricted documents are dispatched by civil post and they may be sent in single envelope.

iv. Care will be taken to ensure that envelopes are not of poor quality and are not overloaded. If the documents to be included are likely to be too heavy for an envelope, they shall be made into a parcel, or the envelope will be tied with a string. Cloth-lined envelopes, if available, may be used.

v. Classified material shall be handled with similar care and attention to record keeping.

(b) Sealing of Envelopes

i. Inner envelopes of TOP SECRET, SECRET and CONFIDENTIAL documents shall be wax sealed. Special Seals shall be used to seal TOP SECRET documents.

ii. The closing and sealing of "TOP SECRET" inner covers will be done under the personal supervision of the officers. The inner cover of the top secret documents will be sealed only by top secret seal bearing a number issued by the CCSO. The closing and sealing of SECRET and CONFIDENTIAL inner covers shall be carried out by or under the supervision of Section Officer or Personal Assistant or equivalent.

iii. All departmental seals issued to different branches/groups/ units must be numbered and a list must be maintained by the issuing authority showing person to whom it has been issued. All such persons will be responsible for the security of these seals.

iv. In case of any loss of such seal, matter should immediately be reported to the CCSO and authority concern for necessary action on their parts. Besides, other seals of the same series should be treated as compromised. Later, a new series of seal with different shape and design should be issued as early as possible.

(c) Movement of Classified Documents

i. For movement of classified paper within office, a box, may be of steel or of thick leather / Rexene/ canvas provided it has a proper locking arrangement and cannot be easily cut/pierced/ opened/ tampered, need to be used. Under no circumstances should classified documents be carried loose in the hands of the messengers/ orderlies.

ii. A messenger carrying secret covers should not leave them unattended at any time till they are delivered.

iii. Within the Same Block or Building: TOP SECRET files or documents shall be taken only by the officer entrusted to deal with them. In rare cases, if a document is to be conveyed through another Officer authorized to handle the document, it shall be put in a single sealed envelope and then carried. SECRET files or documents shall be taken by hand by a person authorised by CEO/ Head of ILDC. CONFIDENTIAL files or documents may be transmitted through any member of the staff entrusted to deal with it.

iv. Movement of Classified Documents Within the Same Station: Movement of TOP SECRET documents between one block to another within the station, shall be through an authorized courier and not through peons or registry. If the carriage involves movement in public area Journey shall be undertaken only in an authorized transport. Wherever feasible, a second person shall also be nominated to accompany the courier.

v. The responsibility of the safe custody and handling of the TOP SECRET document will be that of the recipient officer.

vi. SECRET or CONFIDENTIAL: Officers may carry classified documents, other than TOP SECRET in locked brief cases. In case, brief cases are not available, these may be carried in a single sealed envelope. The documents too bulky to be carried in a brief case may be carried in locked and sealed canvas bag or boxes by messengers accompanying the officers.

vii. If employees (other than officers) are required to carry classified mail, it shall be carried in a locked box or bag, the operating key of which shall be with the originator and the duplicate with the addressee. In the event of more number of addressees, a special box with multiple keys will be used, one key of which shall be with the originator and the rest (one each) with individual addressees. Such keys will not be handed over to the person carrying the box.

viii. All classified mail inside the Mail Box or Bag shall be kept in a sealed cover: While doing so, it will be ensured that classification of the letter is not mentioned on the outer cover.

ix. Section / Unit Officers must ensure that no mail is left undelivered with the person carrying them particularly on Fridays or on days preceding closed holidays.

x. Similar care shall be taken in the movement of classified equipment.

(d) Carrying Classified Documents or Equipment to Residence or Outside Office. Carrying of classified documents and equipment to residence of officers is prohibited. All Top Secret papers should be dealt with in office only.

i. Officers are generally prohibited to carry any Top Secret paper to their residence. When it is necessary to send a Top Secret paper to CEO/ authorized senior officer at his residence after office hours, the dispatching officer should obtain his specific instructions that it may be sent to his residence and that he would be ready to receive the document at his residence.

ii. The dispatching officer must ensure that the box in which Top Secret document is sent, is locked and fastened to the vehicle in which the messenger is carrying it.

iii. When an officer having authority to do so carries any Top secret document to his residence, he must take the documents only in securely locked bag/box, the key of which must be in his possession. The bag/box must be kept all along in his personal custody till he reaches his residence where also this must be placed in a secure place to which no outsider may have access.

iv. Whenever an officer requires a Top Secret document for meetings /discussions, etc. either at the place of his posting or at a place other than the place of posting and Top Secret documents have to be taken out of the office, the following procedure shall be followed:

Only Officers authorized by CEO/ Head of the Company will be permitted in special circumstances for taking top secret documents out of the building to facilitate official meetings with explicit approval of CEO / Head of the Company.

(e) Transmission of Classified Documents to Outstations within India: Classified documents will be dispatched through civil postal service subject to the under mentioned instructions:-

i. TOP SECRET: TOP SECRET documents will only be sent by special couriers. In no circumstances will they be transmitted by civil post. TOP SECRET mail, however, will not be dispatched by "AIR DESPATCH SERVICE." unless accompanied by special couriers.

ii. SECRET or CONFIDENTIAL: Documents can be sent by Registered Civil Post and marked "Registered AD" post on the outer envelope of documents.

iii. RESTRICTED: Document may be sent by civil post, and it is left to the discretion of the originator to decide whether or not registration is necessary.

(f) Transmission of Classified Documents to Foreign Countries. Transmission of classified documents is prohibited in any form, either electronic/ fax or otherwise, to any foreign country.

(g) Circulation and Carriage of Documents/Papers Containing Sensitive Information for Official Interdepartmental and Other Meetings. Utmost care will be taken to ensure security of classified information required to be circulated for Inter-departmental and Other Meetings. Following additional precautions will be taken:-

i. Need to know principle will be strictly applied while circulating sensitive information.

ii. No extra copies of papers etc. will be prepared.

iii. Security classification commensurate with the contents will be assigned to the papers/documents required to be circulated.

iv. The papers/documents if required to be sent in advance will be sent by name and acknowledgement/receipt obtained. The document/ paper will be handed over to the addressee and not their personal staff.

v. The paper/documents should be retrieved by concerned office after the meetings and accounted for.

vi. Only authorized officers will carry such papers/documents for the meeting. These documents will not be carried to residence except where permitted.

5.15 **Emergency Procedures:** ILDCs shall develop procedures for safeguarding classified equipment in emergency situations. The procedures shall be as simple and practical as possible and should be adaptable to any type of emergency that may reasonably arise. ILDCs shall promptly report to the designated agency any emergency situation that renders the facility incapable of safeguarding classified equipment.

5.16 **Disclosure:**

5.16.1 General: ILDCs shall ensure that classified information is disclosed only to authorized persons.

5.16.2 Disclosure to Employees: ILDCs are authorized to disclose classified information to their authorized employees as necessary for the performance of tasks or services essential to the fulfilment of a classified contract or subcontract.

5.16.3 Disclosure to Subcontractors/ other persons/other ILDCs: ILDCs are authorized to disclose classified information to a subcontractor when access is necessary for the performance of tasks or services essential to the fulfilment of a prime contractor a subcontract. Prior authorization shall be obtained by the ILDC in writing from the Government Agency having classification jurisdiction over the information involved for this purpose.

5.16.4 Disclosure between Parent and Subsidiaries: Disclosure of classified information between a parent and its subsidiaries, or between subsidiaries, shall be accomplished in the same manner as prescribed in 5.16.3 for subcontractors.

5.16.5 Disclosure in an MFO: Disclosure of classified information between facilities of the MFO shall be accomplished in the same manner as prescribed in 5.16.2 for employees.

5.16.6 Disclosure of Classified Information in Connection with Litigation: ILDCs shall not disclose classified information to a legal advisor or consultant or representative or any other person acting in a legal capacity unless the disclosure is specifically authorized by the agency that has jurisdiction over the information. ILDCs shall not disclose classified information to any court except on specific instructions of the agency which has jurisdiction over the information.

5.16.7 Disclosure to the Public: ILDCs shall not disclose classified or unclassified information pertaining to a classified contract to the public without prior

review and clearance as specified in the Contract Security Classification Specification for the contract or as otherwise specified by the approving authority.

5.16.8 Non-disclosure agreement: Non-disclosure agreement may be put in place before sharing information with any outside agency.

5.17 **Down Grading, Disposal and Destruction of Classified Documents and Equipment:**

5.17.1 All organizations, departments, sections will carry out periodic destruction of documents (once in a year) to prevent their accumulation and consequent problems of accounting and security. Screening of documents for destruction should be done by a Board of Officers and the proceedings of such Board of should be approved by the Department Head prior to the destruction of the documents

5.17.2 Downgrading or Declassifying Classified Information. Information is downgraded or declassified based on the loss of sensitivity of the information due to the passage of time or on occurrence of a specific event. ILDCs downgrade or declassify information based on the guidance provided in a Contract Security Classification Specification or upon formal notification/ authorization.

5.17.2.1 An Officer will have no authority to downgrade / upgrade the security classification of a document received from other department without the concurrence of the originator.

5.17.3. Upgrading Action:When a notice is received to upgrade equipment to a higher level, the new markings shall be immediately entered on the equipment according to the notice to upgrade, and all the superseded markings shall be obliterated. The authority for and the date of the upgrading action shall be entered on the equipment.

5.17.4 Disposal: Classified documents will be examined from time to time with a view to reducing the number of such documents held. Accountable documents, if no longer required by holder, will be returned to the issuing authorities.

5.17.5 Destruction**:** TOP SECRET, SECRET or accountable CONFIDENTIAL documents will be shredded to small size without being able to be reconstituted and shall be destroyed by burning and a proper record be maintained under the supervision of authorised officer. Documents other than classified may be destroyed at the discretion of the head of the office concerned.

5.17.6 Other points on destruction:

a) Record of daily destruction of classified waste, indicating individual detailed for supervision and the time and place shall be maintained by the Sections, in order to pin point the responsibility in case of breach of security.

b) In no circumstances shall waste paper, drafts, spoiled forms, used carbon papers, unnecessary duplicates, stencils, blotting paper, impression of official seals and stamps relating to or used in connection with classified document be allowed to fall into the hands of unauthorized persons.

5.17.7 Record Rooms Following instructions will be applicable for security of classified documents stored in the record rooms: -

a) Isolated room shall be used for storing classified documents and equipment. They will not be kept in the room where other non-classified documents are stored and kept.
b) Proper fire fighting arrangements will be made to deal with outbreak of fire, suitable fireproof cupboards shall be made use of for storage of TOP SECRET, SECRET and CONFIDENTIAL documents.
c) Records/files/documents from Record Rooms will only be issued on a requisition, stating the purpose and duration for which the records are needed. The requisition should be signed by an officer. A record of the documents issued will be kept in a register.
d) Data regarding employees engaged in sensitive projects or given responsibility to handle sensitive information /materials /documents should be retained permanently by the ILDCs.

CHAPTER – 6 - Communication Security

6.1 General:

All communications are vulnerable to interception. Security of Communication is, therefore of paramount importance in an organization.

6.2 Telephones:

6.2.1 No form of telephonic conversation, including intercom PAX and hot lines, is secure. Every care has to be taken to prevent inadvertent leakage of classified information by discussing classified matters over the telephone. Following precautions shall be observed: -

(a) TOP SECRET, SECRET and CONFIDENTIAL information should not be passed or discussed on telephone.

(b) Before answering the phone or passing any official information on telephone, the person receiving the call should identify the caller beyond any reasonable doubt. In case of doubt, caller should be asked to give telephone no. and identity, which should be checked with the directory before calling back the caller.

(c) The management should carry out periodical sensitisation w.r.t Social Media Usage, Cyber best practices and handling calls/manning Exchange.

(d) Any attempt by the caller/ adversary to impersonate as government official seeking sensitive information should be blocked and officials should be wary of such calls from calls. Specifically, to prevent leaking of information through such calls, following procedure should be followed: -

- (i) Do not provide any information without establishing the identity of the caller.
- (ii) Take down the caller's contact number and seek time to revert back.
- (iii) If any suspicion arises during the call, cancel the call.
- (iv) Do not disclose any sensitive information over phone to anyone.
- (v) Don't be tricked into giving away confidential information.
- (vi) If any email is received from an operative of unfriendly countries, forward that email to CERT-IN for further necessary action.
- (vii) If the email attachment is opened by the user, immediately disconnect that PC from network and scan the network for the presence of malware.
- (viii) Any such calls or email shall be report to the CISO immediately

(e) To prevent misuse, telephones should be kept locked when the officer is away from his office.

(f) Cordless phones will not be used.

(g) If it comes to notice that an intruder has come on the line and some information has come to the knowledge of the listener, the same should be brought to the notice of senior officers and CCSO so that remedial measures can be taken.

(h) A thorough physical check of the PABX phones or instruments or boxes should be made periodically by the office of CCSO to ensure that these are not tampered with.

(i) All vulnerable points in the intercom system should be protected by wooden or metallic boxes with locking arrangement.

(j) Telephone conversation is totally unsafe; thus, if at all classified information has to be passed on phone proper secrecy device should be used.

(k) All telephones should be provided with a caller ID facility.

(l) Only authorized person be nominated for maintenance of PAX / outdoor plant, furthermore records of same be maintained.

6.3 **Cell or Mobile Phones / Data Cards / Voice Modems:**

6.3.1 Cellular or Mobile Phone / Data Cards / Voice Modems are highly insecure medium for communication purposes, since it works on UHF and VHF and is prone to interception by Frequency Modulation receivers. These gadgets can also be used as effective, unobtrusive listening devices for eavesdropping. Technology now exists where the eavesdropping function can be carried out even with they are in switched off mode and can be used to shoot and transmit still pictures or live videos. Therefore, cellular or mobile phones / Data Cards / Voice Modems including WLL phones are potent sources of breach of security of information. Also, no technology or device exists which can be fitted on them to make it interception proof.

6.3.2 GSM Monitoring system is a commercial off the shelf (COTS) equipment and is being manufactured by a large number of original equipment manufacturers (OEMs) across the world. Available equipment enables monitoring of Communication from briefcase sized equipment. A number of Indian vendors are marketing GSM monitoring systems. Due to their small size and portability, there is threat that inimical agencies may selectively employ such means/gadgets for interception of cellular communication from high density areas/ specific areas of activity.

6.3.3 The use of Cell phone shall be banned in areas/offices wherein classified work is in progress/documents are being worked upon. On special cases permission to carry mobile phones by critical staff, in these areas shall be recommended by the Head of department and granted by CCSO. Mobile phones are not permitted inside conference halls, operations rooms, at official briefings and at sensitive places even in off mode. This instruction is applicable to even those who have been permitted. Mobile phone with camera and other technical advance features including internet, GSM, etc. should not be allowed irrespective of ranks inside the office premises. No visitors will be permitted to carry mobiles inside the facility, the mobiles of visitors are to be deposited at the reception.

6.4 **FAX communications:**

FAX communications are also vulnerable to interception or leakage, e.g. a cross-connection. It is, therefore, necessary to identify the end party before transmitting a message. Papers which are not of classified or sensitive nature may be transmitted with the help of FAX in emergent cases. Under no circumstances such an option is exercised for transmitting classified documents. No classified message should be passed or received on Fax on auto mode.

6.4.1 While using Fax machines a record of the documents or papers faxed or received will be kept in a register. The record will include the following details: -

(a) Time of Fax sent or received.

(b) Title of document.

(c) Number of pages

(d) Sent to or received from.

(e) Designation of Officers or office where Fax is sent.

(f) Officer authorized to dispatch the Fax.

(g) No "Top Secret" message should be transmitted on FAX.

CHAPTER – 7 - Computer and Cyber Security (Information Systems Security)

7.1 General:

7.1.1 Information systems (IS) that are used to capture, create, store, process or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information, loss of data and integrity to ensure the availability of the data and system.

7.1.2 The organization must, at all times, be in strict compliance with the IT Act 2000, as amended in 2008 and as amended from time to time.

7.1.3 Protection requires a balanced approach in IS security features to include, but not limited to, administrative, operational, physical, computer, communications and personal controls. Protective measures commensurate with the classification of information, the threat and the operational requirement associated with environment of IS.

7.1.4 ILDC management should appoint / nominate Cyber Information Security Officer clearly defined with roles and responsibilities to carry out activities like development, implementation and evaluation of the facility IS program. To publish and promulgate IS security policy and procedures to address classified processing environment.

7.1.5 Threats to Computers security could emanate from internal sources such as subverted/disgruntled employees, as well from external sources such as the vendors of the Hardware/ Software, outsider maintenance staff or from intruders/hackers in the Cyber Space and hostile foreign countries /inimical agencies. Threats can manifest as Structured (automated methods of information gathering and attack - organised, determined and goal centric) or unstructured (network loitering, manual information gathering or attack and misuse by accident). Some of the Computer vulnerabilities that exist are as follows:-

(a) Physical theft of Hard disks, Computer Storage Media, Keyboards with memory facility, used Printer Cartridges, Laptops etc.
(b) Stealing /compromising data /information by remote access.
(c) Susceptibility to Ransomware and Denial of Service Attacks
(d) Susceptibility to Phishing, Smishing and Vishing Attacks
(e) Accidental/Intentional cross connection between the Organization Local Area Network and Internet.
(f) Spoofing by intruders.
(g) Defacing of various Websites by anonymous Hackers.

7.1.6 In addition to above, any advisory issued by the Government from time to time shall be strictly complied with.

7.2 **ISO 27001:**

7.2.1 The companies shall follow guidelines under ISO 27001. Appropriate controls shall be implemented to accommodate the guidelines given in this manual.

7.2.2 This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS).

7.2.3 This International Standard adopts a process approach for establishing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS.

7.2.4 The process approach for information security management presented in this International Standard encourages its users to emphasize the importance of:

a) Understanding an organization's information security requirements and the need to establish policy and objectives for information security;

b) Implementing and operating controls (administrative, technical and physical) to manage an organization's information security risks in the context of the organization's overall business risks;

c) Monitoring and reviewing the performance and effectiveness of the ISMS; and

d) Continual improvement based on objective measurement.

7.2.5 This International standard adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure all ISMS processes. PDCA provides a structured approach for organizations to achieve continual improvement.

7.2.6 Norms of ISO 27001 is the comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements. The compliance process subjects the system to appropriate verification that protection measures have been correctly implemented. The internal system shall review that all systems have the appropriate protection measures in place and validate that they provide the protection intended.

7.3 The information security policy must take into account the information systems deployed by the organization as well as by any sub-contractors, where such systems may have an impact of the confidentiality, integrity or availability of systems / data. This policy must be made based on a realistic vulnerability / threat and risk assessment by qualified information security experts. The policy must have sign off from the senior most management of the organisation. If the organization also holds Critical Information Infrastructure, the Policy must be made in consultation with NCIIPC. The policy must cover all information devices and, inter alia, include Implementation of Security Controls as released by NCIIPC / CERT-In e.g.

(a) Hardware / software inventory and controls

(b) Protection against malware

(c) User and Password management including for all users handling critical / sensitive information including sub-contractors.

(d) Revocation of privileges subsequent to termination of employees / contracts

(e) Safe and verified backup and restoration mechanisms. These must be tested on a regular basis.

(f) Configuration rules of Firewall, IDS/IPS, UTM, EDR/UEBA, SIEM/SOAR

(g) Industry 4.0 policy for safety of Cyber Physical and SCADA/ICS Systems.

(h) Disaster Recovery policy with focus on data security while assuring business continuity.

(i) (a) Restrict privileged accounts on the system to only those organisation-identities personnel who require this access compulsorily to carry out their allotted tasks which require access to controlled defence information

(b) Require that users (or roles) with privileged accounts use non-privileged accounts when accessing functions or information not related to allotted tasks which require access to controlled defence information

(j) (a) Prevent non-privileged users from executing privileged functions.

(b) Log the execution of privileges functions.

(k) Unsuccessful Logon Attempts

Limit the number of consecutive invalid logon attempts to an organisation-defined number and an organisation-defence time period.

(l) System use notification

Display a system use notification message with privacy and security notices consistent with applicable controlled defence information handling and processing rules before granting access to the system.

(m) Device Lock

(a)Prevent access to the systems by the following methods: –

i. Initiating a device lock after organisation-defined period of inactivity
ii. Requiring the user to initiate a device lock before leaving the system unattended
iii. Retain the device lock until the user re-establishes access using established identification and authorisation procedures.
iv. Conceal, via the device lock, information previously visible on the display with publicly viewable image.

7.3.1 Having implemented adequate measures to secure their information infrastructure, the CISO must also ensure that compensating controls and residual risk are enumerated and sign off obtained from management.

Review and Evaluation of Cyber Security Policy:

Cyber Security Policy of the Organisation shall be reviewed at least annually and updated in response to any changes that would affect the assumptions from the baseline risk assessment, such as significant security incidents, new vulnerabilities, new regulations or changes to the Organization's infrastructure.

The review shall include an assessment of the policy's effectiveness based upon:

-

(a) The nature and number and impact of recorded security incidents.

(b) Cost and impact of controls on business efficiency.

(c) Effects of changes to technology.

7.3.2 Some common Requirements are:

a) General User and Privileged users, their roles, responsibility and accountability should be clearly defined
b) Require that each IS privilege / general user sign an acknowledgement of responsibility to adhere to Information security guidelines.
c) Profiling of Information assets based on sensitivity of information by the Level of Concern for Confidentiality (C), System Availability (A) and Data integrity (I).The level of concern reflects the sensitivity of the information and the consequences of the loss of confidentiality, integrity or availability(CIA). Based on these matrices, need for protection levels and profiles in the form of security, audit, redundancy in the infrastructure, backup etc., shall be determined.
d) Procedures should be defined about unique identification of user, user id removal on termination, transfer; change in roles etc., re-use of user id and user id revalidation for the use of any centralised IS resource.
e) To maintain the CIA, control and audit logging mechanism along with monitoring system should be in place, for changes to data includes deterring, detecting and reporting of successful and unsuccessful attempts to change etc.Such monitoring system can be implemented by deploying solutions like Security incident and Event Management (SIEM), Security Orchestration Automation and Response (SOAR) and User and Entity Behaviour Analytics (UEBA).
f) Use of next generation technologies like Zero Trust Architecture will help in attack surface reduction. Also for granular level control Identity and Access Management (IAM) solutions are recommended.
g) Control and audit logs should be available in centralised systems/applications for Successive Logon Attempts, Multiple Logon Control, Session termination and User Inactivity etc. The logs retention period must be for a period of minimum 180 days.
h) Security should be ensured for inter connectivity of multiple LANs, when organisation has multiple Units/Offices across the geographical location, where interconnectivity may be WAN (Wide Area Network) using public networks.

i) When Public networks are used proven, secured WAN technologies should be used along with appropriate security at the gateway and suitable encryption during transmission.

j) Proper system should be in place to track, inventories, to carry out OS patches, IOS/Firmware updates and Configuration Management of information Systems.

k) All Internet facing Web sites /Applications, necessary protections at Network Layer and Application, like security during transmission, Application Security and Database security should be in place by using appropriate security components / measures. In addition, all these public facing applications and portal should be protected using Content Delivery Network (CDN) and Web Application Firewall (WAF). Also Single Sign On (SSO) with Multi Factor Authentication (MFA) must be enforced on all portals.

l) The Number of Internet Connections shall be controlled by CEO/ Head of Company as per the company policy.

m) Centralised Anti-Virus management solution should be in place for effective implementation of Anti-Virus solution.

n) System should be in place for internal incident management as well as for implementation of time to time necessary guidelines / measures from Computer Emergency Response Team – India (CERT-India)/ National Critical Information Infrastructure Protection Centre (NCIIPC); and should be able to detect any violations to existing policies and ensure updating IT infrastructure.

o) Phishing Attacks can be prevented by using Multi Factor Authentication (MFA). The MFA must be combined with anti-phishing technologies. These anti-phishing technologies encompass traditional methods such as Sender Policy Framework (SPF), Doman Keys Identified Mall (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC), alongside newer advancements like Authenticated Received Chain (ARC), Verified Mark Certificates (VMC), and Brand Indicators for Message Identification (BIMI) that collectively contribute to a comprehensive phishing prevention strategy.

p) Develop and maintain a current baseline configuration of the system. Review and update the baseline configuration of the system periodically and when system components are installed and modified.

q) In addition to above, some of the other guidelines which ILDCs need to follow are as follows -

(I) <u>Common Requirements:</u>

Types of cyber security incidents mandatorily to be reported to CERT-In:

(i) Targeted scanning/ probing of critical networks/systems.
(ii) Compromise of critical systems/ information.
(iii) Unauthorised access of IT systems/ data

(iv) Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
(v) Malicious code attacks such as spreading of Virus/Worm/Trojan/Bots/Spyware/Ransomware/Cryptominers.
(vi) Attack on servers such as Database, Mail, DNS and Network devicessuch as Routers.
(vii) Identity theft, spoofing and phishing attacks.
(viii) Denial of Service (DoS) and Distributed Denial of Service (DDoS)attacks.
(ix) Attacks on Critical infrastructure, SCADA and operational technologysystems and Wireless networks.
(x) Attacks on Application such as E-Governance, E-Commerce etc.
(xi) Data Breach.
(xii) Data Leak.
(xiii) Attacks on Internet of Things (loT) devices and associated systems,networks, software, servers.
(xiv) Attacks or incident affecting Digital Payment systems.
(xv) Attacks through Malicious Mobile Apps.
(xvi) Fake mobile Apps
(xvii) Unauthorised access to social media accounts.
(xviii) Attacks or malicious/ suspicious activities affecting Cloud computing systems/ servers/software/applications.
(xix) Attacks or malicious/suspicious activities affecting systems/ servers/networks/ software/ applications related to Big Data, Blockchain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones.
(xx) Attacks or malicious/suspicious activities affecting systems/servers/software/ applications related to Artificial Intelligence and Machine Learning.

(II) Configuration settings

(i) Establish document and implement the configuration settings for the system that reflect the most restrictive mode consistent with operational requirements. These configuration settings must be organisation-defined consistent with overarching requirement to protect, controlled defence information.
(ii) Identify document and approve any deviations from the establish configuration settings. Such deviations must be granted only as an exception after due deliberation be a collegiate.

(III) Configuration change control

(i) Define the type of changes to the system that are configuration-controlled.

(ii) Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security impacts.
(iii) Implement and document approved configuration-controlled changes to the system.

(IV) Impact Analyses

Analyse the security impact of changes to the system prior to the implementation.

(V) Access Restrictions for Change

Define, document, approve and enforce physical and logical restrictions associated with changes to the system.

(VI) Least functionality

(i) Configure the system to provide only mission-essential capabilities.
(ii) Prohibit or restrict use of the organisation-defined functions, ports, protocols, connections and services.
(iii) Review the system periodically to identify unnecessary or non-secure functions, ports, protocol, connections and services.
(iv) Disable or remove functions, port, protocols, connections and services that are unnecessary or non-secure.

(VII) Incident Response Plan and Handling

(i) Develop an incident response plan that provides the organisation with a roadmap for implementing its incident response capability
(ii) Implement an incident-handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication and recovery processes and procedures.
(iii) Update the incident response plan to address system and organisational changes or problems encountered during plan implementation, execution or testing phases.

(VIII) Incident Monitoring, Reporting and Response Assistance

(i) Track and document system security incidents.
(ii) Report suspected incidents to the organisational incident response capability within an organisation-defined time period.
(iii) Report incident information to CERT-In/NCIIPC as per timelines promulgated by these entities from time to time.
(iv) Provide an incident response support resource that offers advice and assistance to users of the systems for the handling and reporting of incidents.

(IX) Incident Response Testing

Test the effectiveness of the incident response capability periodically.

(X) Incident Response Testing

(i) Provide incident response training to system users consistent with assigned roles and responsibilities:
   a) Within an organisation-defined time-period of assuming an incident response role or responsibility and following occurrence of organisation-defined events.

(XI) Personnel Screening

(i) Screen individuals prior to the authorising access to the system.
(ii) Rescreen individuals in accordance with organisation-defined conditions

(XII) Personnel Termination and Transfer

(i) When individual employment is terminated –
   a) Disable system access within the shortest timeframe which is organisation-defined
   b) Terminate or revoke authenticators and credentials associated with the individual.
   c) Retrieve security-related system property from the terminated individual.

(ii) When individual is reassigned or transferred to other positions in the organisations –
   a) Review and confirm the ongoing operational need for current logical and physical access authorisation to the system and facility.
   b) Initiate information security-related transfer or reassignment actions within shortest timeframe that is organisation-defined.
   c) Modify access authorisation to correspond with any changes in operational need.

7.4 Enterprise Resource Planning (ERP):

Enterprise Resource Planning (ERP) should be implemented as system integrates internal and external management information across the entire organization, tracking of all processes, materials and personnel in the plant. ERP systems automate this activity with an integrated software application. The purpose of ERP is to facilitate the flow of information between all business functions inside the boundaries of the organization and manage the connections to outside stakeholders. There should be exhaustive guidelines, operating procedures issued for all aspects of plant functioning. Ownership of all processes and inventory held should be clearly defined with standby ownership.

7.5 Physical and Software Security:

7.5.1 Unless the physical security of a computer system is ensured, any attempt to protect its operations and data will be futile. Physical security and safeguard of hardware from damage, theft and unauthorized access and software and data from intentional, accidental or environmental corruption must be ensured at all costs.

7.5.2 Safeguarding the computer storage media, software, sensitive and proprietary data by:-

(i) Safekeeping of computer storage media, (CDs, magnetic tapes, hard disk, USB drives etc).
(ii) Shredding or secure disposal of console logs or printouts, used printer ribbons & carbons, damaged tapes and hard disks etc.
(iii) Protection of Switches/Routers and other connectivity devices.

7.5.3 Network racks should be situated away from easily accessible public spaces like the pantry, cafeteria, restrooms, waiting rooms, hallways etc. Also these devices should be properly locked and must be under continuous surveillance using cameras.

7.5.4 Adequate protection is required both for the operating system software and application software. In order to prevent unauthorized access to the data, passwords should be assigned at multiple levels i.e. first at the time of making the system operational, second at the time of logging with the authorized user's name, third at the time of running application software and so on, depending upon the type of data being handled. It is very essential that there should be a provision of 'Audit Trail' features to know which user had logged in and at what time.

a) Develop, approve and maintain a list of individuals with authorisation access to the physical location where the system resides.
b) Issue authorisation credentials for physical access.
c) Review the physical access list periodically.

7.5.5 Review individuals from the physical access list when access is no longer required.

7.5.6 Access Control for Mobile Devices.

a) Prevent access to the system by the following methods –
   (i) Initiating a device lock after organisation-defined period of inactivity.
   (ii) Requiring the user to initiate a device lock before leaving the system unattended.
b) Retain the device lock until the user re-establishes access using established identification and authorisation procedures.
c) Conceal, via the device lock, information previously visible on the display with publicly viewable image.

7.5.7 Remote Access

a) Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.
b) Authorise each type of remote system access prior to establishing such connections.
c) Route remote access to the system through authorised and managed access control points.

7.5.8 Authorise remote execution of privileged commands and remote access to security-relevant information.

1. Monitoring Physical Access
   a) Monitor physical access to the location where the system resides to detect and respond to physical security incidents
   b) Review physical access logs periodically.
2. Alternative Work Site
   a) Determine alternate work sites allowed for use by employees.
   b) Employ adequate physical requirements at alternate work sites at par with those employed at main work site.
3. Physical Access Control
   a) Control physical access at the location where the system resides by –
      i. Verifying individual physical access authorisations before granting access.
      ii. Controlling ingress and egress with physical access control systems/devices or guards.
   b) Maintain physical access audit logs for entry or exit points.
   c) Escort visitors and control visitor activity.
   d) Install secure keys, combinations and other physical access devices.
4. Access Control for Transmission and Output Devices.
   a) Control physical access to system distribution and transmission lines in organizational facilities. Control physical access to output devices to prevent unauthorized individual from obtaining access to controlled defence information.
5. Boundary Protection.
   a) Monitorand control communication at the external managed interfaces to the system and at key internal managed interfaces within the system.
   b) Implement subnet works for publicly accessible system components that are physically or logically separated from internal networks.
   c) Connect to external systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

7.6 Acquisition of Computer hardware and Software:

7.6.1 Computer hardware, which is proposed to be procured, should be of an open system or architecture and the user should be free to go in for 'Annual Maintenance Contract' with any party. The systems being procured should be the latest ones which can be upgraded at a later date.

7.6.2 If development of software application is outsourced, antecedents of the personnel/company developing the software should be verified. Where necessary, Non-Disclosure Agreements (NDA's) must be signed by the Contractor / sub-contractors. Further, for critical applications the vendor should be asked to provide source code for the application developed by him. Whenever feasible, dummy data should be used for testing the applications. This would prevent the vendor from accessing sensitive information.

7.6.3 The firms, which are offering AMCs, should be on boarded upon signing NDA and should be positively vetted by CISO (with help from Agencies of MHA/ Cyber Crime Cell of local police / MoD/ if so required) before they are allowed to take up Software & Hardware maintenance work. In case the same is not possible, an audit of the firm from security point of view should be carried out. While awarding contract for maintenance it should be ensured that too many engineers from the maintenance company are not allowed to work on the systems. It should also be ensured that when the service engineer undertakes the maintenance or repair job, a knowledgeable representative of the user invariably remains present throughout and ensures that no data or information from the computer is downloaded and taken out by the service engineer. Positive vetting of the firms offering AMCs will be as per the guidelines and processes issued by the Government from time to time.

7.6.4 The outsider maintenance Engineer should not be allowed to install his own keyboards and other accessories as an interim measure till repaired part is returned, as his accessory may have data capturing tools like key logger. When his accessory is taken back, it may have valuable data captured from the computer.

7.6.5 While installing the operating System, only the utilities /components required by the user should be installed/ enabled. Some of the utilities listed below which are enabled by default with the bundled software must either be disabled or configured on need basis.

a) Default Password.
b) Sample networking programme.
c) Files sharing tools.
d) Ports enabled by default.
e) Check for presence of any key logger software installed in any PC.
f) Where required CC EAL certification (Common Criteria-Evaluation Assurance Level) based on the protection profile required by the ILDC must be provided by the vendor.
g) Certain windows feature like Power Shell Script, Windows Management Instrumentation (WMI) code (WMIC), process dumps can be exploited by a threat actor for malicious purpose. It is suggested that same must be disabled and may be enabled as and when need arises and disabled again. Behaviour based detection rules should be implemented for the same.

7.7 **Miscellaneous Aspects:**

7.7.1 Each ILDC shall formulate a clearly defined Cyber Security Policy, based on which a third party cyber security audit shall be conducted. This auditor shall be selected by the ILDC from the list of certified Cyber Security Auditors as published by Computer Emergency Response Team – India) CERT-In, on their web site.

(i) The risk to secrecy of data due to the human factor should also not be underestimated. The following measures should be adopted in this regard:-

a) Adequate separation of duties and restriction of access in every office so that no single person can individually compromise the entire system or data.

b) Triennial character and antecedent verification of critically placed functionaries of the computer system handling sensitive information by CCSO through civil police.

c) Cyber Awareness and Evaluation Module should be an integral component of employee induction training. Also on a periodic basis, recurring cyber security awareness training and evaluation sessions must be conducted to keep all employees informed and vigilant regarding cyber security matters.

d) In-house sensitization and periodical briefing of concerned personnel of various departments regarding computer security.

e) Inclusion of talks on computer security in the training programmes on Departmental Security.

f) During the periodic security checks of the department, special emphasis should be laid on computer system security and any loopholes therein.

g) In case of annual maintenance contracts awarded to the vendor, the antecedents of their personnel providing service should at least be verified from the civil police.

h) All probationers of cyber security applied to the principle ILDC must equally carry forward to all contractors / sub-contractors employed in the project and they may also sign non-disclosure agreement.

i) The passwords/credentials of various applications must never be stored on devices (like in browsers/test files etc). Also access credentials should never be pasted / written on advice.

j) The IT Employees must be sensitized that sensitive information like IP Ranges; Passwords and Usernames etc must never be maintained in Personal Diaries.

k) Air-Gapped Systems should not be used for accessing Internet using Mobile Hotspots/USB Dongles.

l) Information in Shared System Resources prevents unauthorised and unintended information transfer via shared system resources.

m) Network communication – Deny by Default – Allow by Exception. Deny network communication traffic by default and allow network communication traffic by exception.

n) Transmission and Storage Confidentiality Implement cryptographic mechanism to prevent the unauthorised disclosure of controlled defence information during transmission and while in storage.

o) Network Disconnection
Terminate network connections associated with communications sessions at the end of the sessions or after period inactivity.

p) Cryptographic Key Establishment and Management.
Establish and manage cryptographic keys in the system in accordance with organisation-defined key establishment and management requirements.

q) Cryptographic Protection
Implement robust cryptography mechanism to protect the confidentiality of controlled defence information.

r) Collaborative Computing Devices and Applications
Prohibit remote activation of collaborative computing devices and applications. Provide and explicit indication of use to users physically present at the devices.

s) Supply Chain Risk Management Plan
Develop a plan for managing supply risks associated with the research, development, design, manufacturing, acquisition, delivery, integration, operations, maintenance and disposal of the system, system components or system devices which are related to or store or harness-controlled defence information. Review and update the supply chain risk management plan periodically. Protect the supply chain risk management plan for unauthorised disclosure.

t) Acquisition Strategies, Tools and Methods.
Develop and implement acquisition strategies, contract, tools and procurement methods to identify, protect against and mitigate supply chain risks.

u) The Software must be developed and build in secure environments. Those environments must be secured by the following actions, at a minimum –
Separating and protecting each environment involved in developing and building software. Regularly logging, monitoring and auditing trust relationships used for authorisation and access to any software development and build environments among components within each environment.

v) Enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software in a manner that minimises security risk.

w) Taking consistent and reasonable steps to document, as well as minimise use of inclusion of software products that create undue risk within the environments used to develop and build software.

x) Encrypting sensitive data, such as credentials, to the extent practicable and based on risk. Implementing defensive cyber security practices, including continuous monitoring of operations and alerts and, as necessary, responding to suspected and confirmed cyber incidents.

y) The software developer must make all efforts to maintain trusted source code supply chain by employing automated tools or comparable processes to address the security of internal code and third party components and manage related vulnerabilities as available from time-to-time. Use of trusted software/hardware components in facility handling/developing sensitive technology is mandatory.

z) The software developer must maintain provenance for internal code and third party components incorporated into the software as Software Bill of Material (SBOM) and supply the same to BUYER at the time of delivery of the software as well as each software update.

aa) The software developer must employ automated tools or comparable processes that check for security vulnerabilities.

7.7.2 Cataloguing of CDs/ External / Portable Hard Drive: The CDs (RW), Cartridge Tapes, External/Portable Hard Drives used should be serially numbered with name of the concerned written in indelible ink. A register should be maintained for taking it on charge and destroying those that become unserviceable, and periodical checks should be carried out. Supply of blank storage medium for use of the PC holders will be made only against written requisition duly signed, or countersigned, by an officer.

7.7.3 External / Portable Hard Drive: Use of External / Portable Hard Drive within Classified Zone/areas is not permitted. Only in rare and exceptional cases, officers, for whom specific permission has been granted by CCSO, can use External / Portable Hard Drive within the classified zones/areas. External / Portable Hard Drives will be issued only to such individuals who possess the permission by name and it will be in their personal charge. Procurement of External / Portable Hard Drive will be done centrally by the CCSO with written approval of the CEO/Chairman/CMD, who may delegate the powers to the Unit Head for issuing written approvals. However, the responsibility and accountability of the same shall still rest with the CEO. All instructions relating to classified documents contained in this Manual are equally applicable to External / Portable Hard Drives. Carriage of External / Portable Hard Drive inside/outside the office premises is not permitted.

Secondary storage Devices register will be maintained by the respective sections/departments. Internal physical check will be carried out within the concerned sections/departments every week and result indicated in

the register. Sections/departments will render a quarterly certificate to the CCSO regarding safe custody of the pen drives in their sections/departments. No visitor/employee will be permitted to use or carry personal pen drive / External / Portable Hard Drives within the classified area/zone. Loss of External / Portable Hard Drive will be reported to CCSO immediately, and investigations carried out simultaneously by the sections/departments, to ascertain the extent of loss of classified information and to pinpoint responsibility for the loss for initiating suitable action against the defaulters.

a) Prohibit the use of external systems in production environment unless the system are specifically authorised.
b) Establish the terms, conditions and security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorised individuals.
c) Permit authorised individuals to use an external system to access the organisational system or to process, store or transmit controlled defence information only after –
   (i) Verification of the implementation of security requirements on the external system as specified in the organisation's security plans.
   (ii) Retention of approved system connection or processing agreements with the organisational entity hosting the external system.
d) Restrict the use of organisation –
   Controlled portable storage devices by authorised individuals on external systems.

7.7.4 Laptops/Palmtop/Electronic Notebook: Carriage of Laptops/ Palmtops/ Electronic into or out of classified zone/area without permission from CCSO is not permitted. Following precautions should also be taken to ensure security of information: -

a) No personal Laptop/ Pen drive/ thumb drive/ hard disk/ palmtop/ Electronic Notebook and mobile phones with Blue tooth / Wireless Internet (4G/5G) should be permitted to be brought into the classified area/zone by the visitors or the employees.
b) In case a Laptop/Palmtop/Electronic notebook is required to be brought inside for a specific purpose, the Bluetooth/WI-FI feature, if present, should be disabled and the user/owner should be escorted till his exit to prevent any enabling during the visit.
c) Any laptop taken out for presentation should be checked for containing any unauthorised data/information. On return, it should be checked for any virus. Proper record of transport of data through Laptop should be kept. There should be provision to log all transactions, file transfers, read, write modifications etc.

7.7.5 Scanners: All scanners will remain in the physical custody of their owners and record of classified documents scanned should be kept.

7.7.6 Beacon and Siren must be integrated with the cameras used in Perimeter Intrusion Detection System (PIDS) as any camera can be tampered for

accessing in to the air-gapped camera network and can be used as pivoting point for further compromise.

7.7.7 Destruction and Weeding :

a) Damaged and unusable Cartridge Tapes/ CDs/ DVDs/ Pen Drives and other CSM should be broken and destroyed by burning or as applicable to the weeding out paper based files and an entry to this effect be made in the register. CCTV recordings should be password protected.
b) Bad / condemned hard disk should not be released even after it has been replaced by a new one. Such hard disks will be destroyed by following procedures as applicable to weeding out of classified files.
c) Destructions should be carried out by application of corrosive Chemicals (acid or abrasive substances, emery wheel or disk sander) to the recording surface, and by shredding, incineration, disintegration, pulverization and smelting etc.

7.7.8 **Cyber Security Audit:**

a) The CISO must supervise all computer security measures within his offices/ branches/section. The CISO shall not be a foreign citizen, or a Personof Indian Origin who is a Non-Resident Indian.
b) Cyber Security Audit must be carried out under the strict supervision of Cyber Information Security Officer (CISO).
c) Periodic security audit of the IT is liable to be carried out by designated Govt Agencies, from time to time, to ensure that the laid down guidelines are strictly followed. However, this does not in any way reduce the requirement of internal security audits conducted by the organisation.
d) Periodic Computer Security Awareness programme for the computer operator, users and administrators should be carried out to expose them to the latest developments in computer security and remind them of their responsibilities.
e) Creating own Cyber Security Infrastructure with staff to carry out Cyber Security audits and attend Cyber security incidents on day to day basis. Such security audits of the computer system and network devices be carried out by:
    i. Internal team every six months and report is sent to CEO.
    ii. CERT-IN empanelled auditors preferably by STQC (Standardization, Testing & Quality Certification) under Department of Information Technology once every year.
    iii. Comply with the Cyber Security audit observations in time bound manner.

7.8 **Guidelines for Computer Users or Operators:**

(a) DOs.

(i) Observe effective physical security procedures to restrict access to computer systems. Access to be given only to authorized persons.

(ii) Use hardware locks in the cabinets in which the computer system is housed.

(iii) The contents of cartridge tapes, CDs or Pen Drives are as good as written files. All physical and static protective measures and instructions laid down in this manual for document security will also apply to the use, control and custody of data CDs or Pen Drives. External storage media containing classified data will be marked and treated like other classified documents.

(iv) All classified documents should be stored in an encrypted form in PCs as well as external storage devices.

(v) Adopt effective physical access control procedures by incorporating proper identification and authentication mechanism like "Complex password' at different levels and 'Dynamic Log in' by verifying the user's magnetic strip cards, finger prints and voice recognition, depending upon the nature of sensitivity of the data. User password is the most important aspect whose Confidentiality must be zealously guarded. Further, a password should have the characteristics laid down in this chapter.

(vi) Audit trails are activated for keeping electronic record on the system regarding use of computer system by various users. Activities of a user be logged and appropriate audit trails be maintained on the system in electronic form.

(vii) Before deleting the sensitive files, overwrite the files with some junk data to prevent restoration of the sensitive data by any means. Keep the backup of operating system software and application software under safe custody. One backup copy should be kept in different location as a precaution against fire hazards.

(viii) Backup data should be periodically updated. Keep the software maintenance tool in your own custody. The periodic checking of backup inventory and testing of the ability to restore information validates that the overall backup process is working. This may be given to the engineer called to attend to the faults in the system as and when required.

(ix) External CD writers will be under the custody of officer only. CD writer will be used only in minimum and unavoidable files and data.

(x) Ensure safe custody of the Computer Storage Media such as cartridge tapes, Pen Drives, CDs etc.

(xi) Every new incoming storage media or software should be tested for Virus.

(xii) Always use original software purchased from the authorised vendors.

(xiii) Copying of data, deletion, modification, etc. from the disk should be done under proper authorisation and supervision of the office-in-charge.

(xiv) Use Screen saver password

(xv) Use exclusive computer for internet

(xvi) Software tools like device locks may be used to block unwanted storage devices, Ports and other external accessories.

(xvii) The movement or exchange of storage medias should be with the prior approval of the officer-in-charge of the office.

(xviii) In case the shift system is in vogue, there should be proper handing / taking over among the shift-in-charge.

(xix) (Damaged and unusable cartridges, tapes and CD(RW) and pen drives should be broken and destroyed and record to this effect should be maintained.

(xx) All the used printer ribbons and carbons should be destroyed by burning.

(xxi) Maintenance or rectification of faults in the computer system should be carried out under proper supervision. Keep an eye on the outside engineer attending to the fault in your computer system

(xxii) Use UPS units to prevent corruption of data and software.

(xxiii) Where feasible, all digital storage devices when permitted to be taken out will be password protected and prior permission of security office is obtained.

(xxiv) Some PCs have in-built physical locking system. The user should keep the computer locked when it is not in use and ensure safe custody of the operating and duplicate keys.

(xxv) Culture of one printer or more per PC should be curbed. Ensure centralized printing within section.

(xxvi) Network printers must be located in a secure place so that the documents being printed cannot be taken away by unauthorized personnel.

(xxvii) Internet PC as well as patches released by OEM should be periodically updated. Live updates for Anti-virus/Anti-spyware and portable storage media used on internet machine to be scanned for spyware, Trojan and another suspicious malware before being used on LAN.

(xxviii) While updating patches (using WSUS Server) an outbound quota limitation must be enforced to mitigate the risk of data exfiltration.

(xxix) Disable system accounts when –

a) The accounts have expired
b) The accounts have been inactive for an organisation – defined time period
c) The accounts are no longer associated with a user or individual
d) The accounts are in violation of organisational policy.
e) Significant risks associated with individuals are discovered.

(xxx) Notify organisational personnel or roles when -

a) Accounts are no longer required.
b) Users are terminated or transferred
c) System usage or need to know changes for an individual

(xxxi) Information in Shared System Resources.
Prevented unauthorised and unintended information transfer via shared system resources.

(b)<u>DON'Ts.</u>

(i) Don't let any unauthorized persons use your computer system.

(ii) Don't share your password with anyone, not even your colleagues.

(iii) Don't reveal the root password to any unauthorized person, particularly an outsider.

(iv) Don't connect the computer directly to the mains. Also, no heavy electric load drawing machines like plain paper copier, shredding machines, coolers etc. should be connected to the source of constant voltage supply to the computer.

(v) Do not connect your computer system storing classified data to internet.

(vi) Don't allow staff members to bring their own storage medias or software to run on the computer system of the department.

(vii) Don't use pirated or gifted copies of software as these may contain viruses and even facilitate intrusions into the system.

(viii) Don't play computer games. These could be the main carriers of computer viruses and an unsuspecting or easy media for an intruder to break into your computer system.

(ix) Don't panic if your system comes to a halt. Try to find out the cause and take precautions for future.

(x) Don't store TOP SECRET or SECRET information permanently in the hard disk of PC. Whenever TOP SECRET or SECRET information is processed on the PC, erase the information immediately from the disk after the processing is over. When CDs are used for working on TOP SECRET or SECRET information it should be handled in accordance with the instructions for handling TOP SECRET or SECRET documents. It will be the responsibility of the authorized officer under whose supervision the PC work is being carried out.

(xi) Don't carry CDs outside the office building. In case a data stored media has to be taken outside the office building, its movement will be with prior approval. A record of the movement indicating full details like date or time of its being taken out, name of the officer taking it out and purpose, date and its time of its return etc will be maintained.

(xii) Don't keep CDs in table drawers etc.

(xiii) Don't become a member of unofficial chat club or official chat club on official Internet.

(xiv) Don't Carry Pornographic CDs or VCDs or such like material in other storage devices.

(xv) Do not use pen drives, internal CD writer or combo drives unless specially authorized.

(xvi) Do not use/install freely available screen saver on internet as these may have encoded spyware/Trojan.

7.9 Instructions for Use of Internet within Classified Area/Zone:

Internet services are based on open architecture with minimal security features. They are also open to malicious attacks, hacking, virus activities and cyber-crimes. Unauthorized and unregulated use of internet can lead to compromise in security. Internet within the office/area/zone handling classified information can be installed in the office of an officer with prior approval from the CISO. Internet connectivity should be provided to the offices only on a stand-alone PC. The Internet PC should

not be used for office work. The Internet PC will have its own peripherals such as UPS, scanner, etc. which will not be shared with any other system under any circumstances. PC will be kept isolated from all other systems, especially LAN/Intranet. Connection of any other system with Internet line for any purpose, whatsoever, is strictly prohibited. No official or personal files will be stored on the hard disk of Internet PC. Personal media will never be used on Internet PC. No sensitive/ classified office work will be done in Internet computers.

7.9.1 All official work will be carried out on a system belonging to Air Gapped Network. Air Gapped Network will be isolated from the Internet at the physical layer. The air-gapped network's devices should meet following criteria:

(i) Must have a separate networking equipment, including switches and routers, accompanied by cables of a different colour to easily differentiate them from internet-related cables.
(ii) Specially designated desktop computer (referred as Entry-Exit system) must be used for moving data into/out of Air-gapped network.
(iii) Only officially recognised Thumb Drive/Pen Drive can be used on Entry-Exit system for data exchange. This Pen Drive will always remain in safe custody of CISO or any other officer designated by CISO. Every issue of Thumb Drive/ Pen Drive will be recorded.
(iv) Under no circumstances, the Entry-Exit system should be used for nefarious activities like connecting it to Internet using USB WiFi Dongles or Mobile Hotspots etc.
(v) Entry-Exit system is also part of Air-Gapped Network and should not be used for providing Remote Desktop Access/team Viewer Access to other air gapped systems.

7.9.2 The systems on the Air-Gapped network must meet following requirements:

(i) To enhance inventory tracking, systems within the Air-Gapped network should MAC bound to the hardware ports.
(ii) All USB ports must be blocked to disallow access to any Pen Drive/Thumb Drive/Hard Disk etc.
(iii) All Air-Gapped systems must have warning signs and Stickers Tags like USB Blocked / Air Gapped System etc.

7.9.3 Keeping in view the vulnerabilities involved in using internet in any sensitive / defence installation, apart from cyber security guidelines mentioned in the chapter, the following may be incorporated for security of the IT network(both internal & external) :-

(i) Instead of multiple internet connections, there should be limited internet gateways for accessing the internet from within the organisation. These limited internet connections must be closely monitored by the Information Security Operations Centre of the organization.
(ii) The SOC should include industry standard Security incident and Event Management (SIEM), Security Orchestration Automation and Response

(SOAR) and User and Entity Behaviour Analytics (UEBA) solutions for faster response time during attacks and timely detection and blocking of attacks.

(iii) All traffic through the organisational internet gateways must be screened to ensure that organizational data remains secure. Concerned personnel must be sensitized to the fact that their internet connections are provided to aid them in discharge of their duties and not for personal usage.

(iv) Communication through open e-mail should be avoided from disseminating information related to the equipment being used or quantity to be manufactured or its component details at any stage (from development, testing to deployment) to its joint partners (contractors /sub-contractors).

(v) If the joint venture involves collaboration of foreign firm(s) then, connectivity of their computers with contractor system needs to be examined from security angle.

(vi) All employees should be barred from using private email addresses (like Gmail, hotmail, yahoo, rediffmail etc.) for any form of official communications and emails from suppliers/contractors through private emails addressees should be barred, as far as possible. However, the employees should be discouraged to use official email id for registering into various non-official platforms like banking, insurance etc.

(vii) Social media usage policy should be defined and enforced on all employees. Unless specifically required for discharge of their duties, employees must be prohibited from accessing social media sites from their official systems. Employees should be discouraged from publishing information related to their work.

(viii) Server room/network room should have biometric access control systems with CCTV coverage in place

(ix) Enforce approved authorisations for controlling the flow of controlled defence information within the system and between connected systems.

7.10 **Cyber Posture Enhancement via integration with Defence CSOC:**

Industry entrusted with procurement orders/technologies developed by any Government agency of any such entity, privy to Defence related designs, plans, materials, documents, products, software, etc shall ingest necessary logs only (non-content) to Defence Cyber Security Operations Centre established by MoD for the purpose of centralized Log monitoring, analysis, anomaly detection and overall Cyber Security Posture Management.

CHAPTER – 8 – Subcontracting

8.1 General:

In case the ILDC outsource/ release or disclose classified information/ project to a sub-contractor all provisions of the Security Manual as per applicability shall be followed. Wherever/Whenever sharing of classified material/information is to take place, the same will be preceded by Non-Disclosure Agreement (NDA).It shall be the duty of CCSO to appraise the CEO / Head of Installation with regard to all the security provisions to be followed. The security parameters between the subcontractor and the ILDC shall be included in the contract with the following additional provisions:

(i) Out sourcing partner's personnel and facilities would also be covered under the Official Secrets Act, 1923, whenever the ILDC is handling classification material, document, information etc.

(ii) Persons working on such projects should be checked for character antecedents and police verification shall be obtained before inducting any person on such assignments.

(iii) All the relevant clauses of the Manual of Security are to be made applicable for the sub-contractor.

8.2 Terms and conditions related to classified information:

Terms and conditions relating to retention, handling and destruction of classified information/material received or generated under the subcontract shall be clearly indicated in the main contract between the subcontractor and the prime ILDC. If certain classified information/material received or generated under the subcontract is intended to be retained, then the subcontractor has to comply with the provisions of this manual and give an undertaking of the same to ILDC and concerned Government agencies.

8.3 Engagement of consultants/advisers:

ILDC should ensure that the background and the character & antecedents of the advisers/consultants are verified before hiring their services. ILDC would be responsible for verification of C&A of advisors /consultants. Engagement of consultants/advisers shall be subject to signing of NDA.

8.4 Audit Recommendations:

The ILDC shall receive the recommendations made by Audit Teams. The ILDCs shall make note of recommendations and take action as warranted as soon as possible but in any case not later than the timeline.

CHAPTER – 9 - International Security

9.1 Imports of Equipment/ Materials:

(i) Where Sensitive Equipment/ Materials is bought or otherwise acquired by the ILDC, it should be ensured the equipment is securely packed and sealed and transported. The packages will not have any markings to indicate that the Equipment is Top secret / Secret.

(ii) Top Secret and Secret Equipment/ Materials will not be shipped in Vessels / Flights which unload cargo in other countries or call at ports of unfriendly countries en-route.

(iii) Bills of lading or other documents will not indicate the classification of the Equipment. Separate bills of lading may be made out for small consignments which are delivered to the Master of the Ship for personal custody during transit. These documents will indicate the equipment in general terms, e.g. Instrument, PCB and so on, but will not give precise details.

(iv) Where possible, intimation will be sent to the consignee through official channels of the company. If time does not permit, intimation may be given through a coded / encrypted signal etc., describing the equipment in general terms and indicting the security measures to be adopted. Such consignments should be immediately removed from the Cargo area to the respective manufacturing Division / Unit or Factory.

(v) Consignments of classified equipment awaiting shipping will be suitably shrouded. If the size of the equipment does not permit this, it should be stored in such a way as to be out of sight of observers. These consignments will be adequately guarded to prevent pilferage or inspection by outsiders.

(vi) The Embarkation Firm / Agency abroad will inform the respective manufacturing Division / Unit or Factory of the dispatch of classified equipment. On receipt of such intimation and based on expected date of arrival of equipment, the desired level of security measures are to be adopted.

(vii) The Embarkation Firm / Agency will be responsible for enforcing the necessary security measures including provision of escort, if any, till the equipment is taken over by the receiving manufacturing Division / Unit or Factory. Where necessary, the consignee will detail an officer to go to the port of disembarkation to take over the Equipment. The receiving officer will cover the equipment or otherwise conceal it and, if necessary, unload and move it out of the port during night so that chances of leakage of information are minimized**.** Consignor shall be responsible to arrange security vetted carrier/transport agency till the receipt by consignee.

(viii) Single point contact (Security Co-ordinator) shall be designated for controlled movement of classified materials and documents from foreign source with whom collaborators can communicate for secured transaction of TOT documents/Materials.

9.2 Warning to Consignees:

Consignors of classified equipment will warn Consignees of the classification of the Equipment and the precautions to be taken. Escorts will be detailed during

movement of all classified equipment. Procedure followed for movement of classified documents would also be applicable to movement of sensitive equipment.

9.3 **Handing and Taking Over:**

Those concerned with Handing/ Taking over of classified equipment will ensure that they are fully aware of its classification and security measures to be adopted. Warnings as to the security measures necessary will be issued in writing. Top Secret and Secret Equipment will be Handed/ Taken over under the direct supervision of authorized senior officer only.

9.4 **NDA for transfer of classified information between two countries:**

The names of the Government Authority of each of the two countries empowered to authorise the release and to co-ordinate the safeguarding of Classified Information related to the Contract and the channels to be used for the transfer of the Classified Information between the Participants National Security Authority (NSA)/ Designated Security Authority (DSA)/ Competent Security Authority (CSA) and/or Contractors involved shall be governed by non-disclosure agreement.

9.5 **Movement:**

(i) Consignors of Top Secret and Secret Equipment will warn the consignee of the dispatch of equipment so that the latter is in a position to make adequate security arrangements to receive it. All such equipment will be suitably shrouded and accompanied by an escort to ensure that no unauthorized person gains an access to them surreptitiously.

(ii) When only portion of equipment is Top Secret or Secret and it is possible to conceal that portion, it is not necessary for the entire equipment to be covered up. Only the Top Secret / Secret portion(s) of such equipment should be covered.

(iii) If a portion of equipment is 'Top Secret' or 'Secret', the consigner would ensure that the whole equipment is covered before dispatch.

CHAPTER – 10 - Visits and Meetings

10.1 Visit of foreign Nationals:

10.1.1a) No foreigners would be allowed to visit the area/zone/manufacturing facility where the work related to MoD projects is going on without clearance of MoD. As per the MHA guidelines, prior security clearance is required for visits of foreigners to vital and sensitive installations in the country. The CEO / Head of the concerned ILDCs will have power to approve business visits of foreign nationals, those who are on appropriate type of visa to non-sensitive/non-strategic areas only of the manufacturing /R&D units of the Company and such visit shall be reported to Nodal Office, DDP after the visit within 24 hours through online portal of Vital Installation Information System (url: https://indianfrro.gov.in/viis/) preferably within two days but not later than fifteen days in any case. This will also be reported to Nodal Office, DDP in quarterly report. No foreigner shall be allowed to visit vital installation on the strength of tourist visa/e-tourist visa.

b) For the duration of the visit, the foreign nationals will be escorted by the security officer or officer designated by the company. A log of all the escorts assigned to the Foreigner or an Indian representing a foreign company/nation shall be maintained by IILDCs for atleast till the next external security audit.

c) No photography in the areas where work related to defence related projects will be permitted. It may also be ensured that viewing of contagious security areas does not occur.

d) After the visit, the names and particulars of the foreign nationals, the purpose, duration and site of the visit are to be communicated to the Internal Agencies of Ministry of Home Affairs quarterly. Instructions received from Department of Defence Productions, Ministry of Defence in this regard from time to time will be followed

10.1.2 In keeping with the above instructions, following procedure would be adopted for processing security clearance of Foreigners visiting the Company.

a) The Head of the Department / Division / Factory Office as the case may, will initiate the case for visit of foreigners, well in advance, giving the following particulars: -

i. Full name of the visitor.
ii. Nationality of the visitor.
iii. Date of birth.
iv. Parentage of the visitor.
v. Permanent and Present address of the visitor.
vi. Passport No with date and place of issue.
vii. Validity of Passport.

viii. Visa details (types, data & place of issue and duration of visa)
ix. Occupation and Name of the Firm / organization which the visitor is representing.
x. Specific purpose of the visit.
xi. If the foreigner has visited the establishment earlier, full details of the same is to be furnished.
xii. Details of escort being provided for conducting the tour of the Foreign National(s).
xiii. Address of Hotel/accommodation where the foreign visitor staying in India during the visit.
xiv. The address of the Indian company with which the foreigner is having partnership/alliance etc.
xv. Date & Time of visit
xvi. Area to be visited
xvii. Certificate that no classified document shall be shared with the foreign visitors.

b) The particulars of the foreigners will be filled in a proper format and processed through CEO/Head of ILDC as the case may be for approval. Purpose of the visits also needs to be mentioned in the format prescribed for this purpose. The particulars are also to be intimated to MHA and Nodal Office, DDP in the prescribed format as indicated in 10.1.2(a).

c) The approved copy will thereafter be forwarded to CCSO for preparing the Visitors Pass.

10.1.3 While conducting the visits of Foreigners, Instructions issued by the MHA/MoD from time to time should be followed.

10.1.4 In addition following points would also be adhered to:-

(a) The number of visits to non-sensitive areas/zones/offices shall be restricted to the barest essential and would be on need to know basis. Procedures to ensure that visitors are only given access to information consistent to their visit would be put in place by ILDC. The responsibility for determining need to know in connection with the visit shall rest with the individual who will disclose the information.

(b) If the visit to Manufacturing areas is considered necessary, the visitor should be allowed access to only these areas, which are relevant for the purpose of the visit.

(c) Notwithstanding the above guidelines, no foreign visitor should be allowed to manufacturing and development areas of Electronics Warfare and secure communications.

(d) The aforesaid guidelines should also apply to NRIs, Persons of Indian Origin, and Indian citizens representing foreign firms.

(e) No exposure as well as disclosure about activities undertaken at ILDC would be made to any foreign visitor without exclusive clearance from CEO/Head of ILDC. Such disclosures would be on minimum need basis.

10.2 **Meetings:**

Meetings would mean conference, seminar, symposium, exhibit, convention, training course or such gathering. Meeting with foreigners pertaining to MoD projects / classified information is not permitted without the approval of MoD.

10.2.1 ILDCs may conduct meetings with regard to Government Projects, with limited number of people who are connected with the project. However, all concerned officials will be governed under OSA, 1923. The information which is to be disseminated shall be cleared by the CEO. If ILDC wants to conduct meeting involving classified information, the same may be done with due authorization of CEO. However, it is the responsibility of the CEO to ensure that classified information is not leaked.

10.3 **Nomination of employees from ILDC to attend Classified Meetings:**

The CEO may authorize its nominated employee(s) to attend certain classified meetings pertaining to classified information / sensitive information. It is the responsibility of CEO for non-leakage of information.

CHAPTER – 11 – Training

11.1 **General:**

It shall be the responsibility of the ILDC to provide all employees with security training and briefing, commensurate with their roles and responsibilities while dealing with classified information. Towards this, the ILDC may obtain defensive security, threat awareness and other educational and training information from the nominated agency of Government of India, Ministry of Defence.

11.2 **Security Briefing:**

All employees should be briefed on security do's/don'ts on joining as a part of induction programme.The induction programme must include Cyber Awareness Capsule.

Prior to being granted access to classified information, an employee shall receive an initial security briefing that includes the following:

a. A threat awareness briefing.

b. A defensive security briefing.

c. An overview of the security classification system.

d. Employee reporting obligations and requirements.

e. Security procedures and duties applicable to the employee's job.

11.3 **Training:**

ILDC shall also be responsible for the training of CCSO & CISO and other members of his staff performing security duties, as promulgated from time to time by Ministry of Home Affairs. Training shall be based on the ILDC involvement with classified information and should be completed within One year of appointment as CCSO & CISO. Government may organize security briefings to the CCSO & CISO and other security staff as required from time to time.

11.4 **Refresher Training:**

The ILDC shall provide all the employees with some form of security education and training at least once a year, which shall aim at refreshing the training provided during the initial security briefing, update of security regulations and any new developments. ILDC shall maintain a record of all training conducted and employees' participation in them.

11.5 **Security Training of Vendors / Contractors and Casual Labourers:**

Security discipline needs to be imbibed among Vendors / Contractors and Casual Labourers for better efficiency of the overall Security system. This can be achieved by detailed briefing or small training capsule to contractors and on-the-job training to their casual labourers. A clause on termination of services / contract as the

case may be for breach of security of any kind must form part of the contract agreement between the ILDC and the Contractor/ Vendor.

11.6 **Training of Project Work Trainees:**

ILDC's may permit trainees to undergo training / undertake project work, however, all such trainees shall not be employed in any classified projects nor have any access to classified areas/zones/offices. In addition, all the students must be properly briefed about the sensitivity of the organization and conduct expected from them on Information Security. Police Verification including bonafide/Conduct certificates from respective college should accompany the sponsorship of Trainees before permitting the students / trainees to take up project work / training and proper identification badges to be issued to them. No trainee is permitted to carry sensitive data from the installation. Further, the Project Reports of these trainees must be completely vetted by the Head of the Department before certification and submission of the same to the respective College / University.

11.7 **Training on Cyber Security:**

IT Division shall ensure that all personnel be appropriately trained on the Organization's Information Security policies commensurate with their roles and responsibilities and be kept up-to-date on any additions or changes to the policies.

CHAPTER – 12 – Miscellaneous

12.1 **General:**

MoD will be the nodal agency for preparation, review and implementation of the manual. However, conducting inspection and audit would be the responsibility of **MHA /MoD**.MHA &MoD may take the assistance of other organizations like Agencies of MHA and MoD, DPSUs, NTRO etc. in the inspection or audit.

12.2 **Publicity and Photography:**

No photography would be permitted inside the Classified Zone/Area pertaining to MoD projects without the approval of MoD. Photography, when permitted for official purposes, will be done under proper supervision and both the photos, soft copy of photograph and their negatives shall be appropriately classified. In the case of Top Secret and Secret Equipment, permission for photography or publicity will be granted by General Manager / Chief Executive of the manufacturing Division / Unit or Factory, however, it will be done under controlled conditions by the official photographer. As far as possible only official agencies will be assigned for photography where authorized. Permission will not be necessary for official photography by the Factory / Division for compiling technical reports on equipment. Such reports and photographs will, however, be appropriately classified and safeguarded by them. The holder is, however, responsible to ensure that the equipment is not exposed to public view and that no one is afforded an opportunity to photograph it in full or in part.

12.3 **Trials / Demonstration:**

The Chief Executive of the manufacturing Division / Unit or Factory will enforce suitable security measures during trials / demonstration with the help of CCSO. When it is proposed to undertake demonstration involving Top Secret and Secret Equipment, full particulars of persons to be admitted to such demonstration will be approved by the Chief Executive. Special identity documents/passes will be issued to the invitees where necessary and a security officer appointed to enforce security measures.

12.4 **Rejects and Salvage:**

All Top Secret / Secret Equipment rejected during development, trial or manufacture will continue to bear its original security classification and receive appropriate security protection. If such equipment is no longer required, it will be dismantled and rendered unidentifiable. Such equipment will not be consigned to salvage unless it is downgraded to unclassified or shredded beyond recognition. All Hard disks pertaining to classified projects will, at no cost, be sent out for repair / recovery of data or salvage. Hard disks will always be removed before the CPU is sent to salvage. The hard disks will be destroyed under the supervision of Head of Security and certified to that effect. The disposal of non-sensitive scraps may be done M/s. MSTC.

12.5 **Disaster Management:**

The ILDC shall draw elaborate disaster management plan to minimize loss of life and property with an aim to handle the situation with utmost promptness and efficiency to safe guard the plant from major catastrophic incidents like Earth Quake, Bomb Blast, Floods, Terrorist Attack, etc., The ILDC shall also carry out frequent rehearsals, in any case, once in a year to ensure that in the event of any disaster, all functionaries can act effectively.

The disaster management plan should focus on data security while assuring business continuity. The BCP/DR backup sites (also referred as Secondary sites) should not be a source of data breach. Disaster Management Plan should be in line with the guidelines/instructions issued by the National Disaster Management Authority/State Disaster Management Authority.

12.6 **Internal Security Audit:**

The ILDC shall carry out internal security audit to ensure verification of compliance of security instructions contained in this manual. The Security Audits are required to be conducted to ascertain the level of compliance of security instruction and procedures specified in the security manual. The audit shall be done at least on a yearly basis. If ILDC is Multi Facility Organisation (MFO), audit shall be done annually in each facility: -

(a) Check compliance by all the establishments to realize the designed security objectives as enumerated in the security manual.

(b) Verify the effective implementation of the instructions and identify lapses, if any.

(c) Verify the efficacy of the existing Security & Fire Control System.

(d) To check that adequate safeguards exist against espionage, sabotage and subversion in a given environment where the installation is located.

(e) To check the general Security awareness amongst the Employees.

(f) To ascertain serviceability and operational worthiness of technical equipment such as CCTV, Electronic Barriers, Power Fence, Access Central Systems and Fire Fighting Equipment, etc.

12.7 **Action on Completion of Audit:**

On completion of audit, the audit observations contained in the audit report must be rectified by the auditee at the earliest and preventive action initiated after identifying the root cause of non-compliance to prevent its recurrence. Subsequent audit shall monitor the timely implementation of corrective / preventive action and its effectiveness. A report of the same shall also be submitted to MHA/and DDP, MoD.

12.8 **External Security Audit:**

In addition to the internal audit carried by the ILDC, External audit by agencies of MHA and MoD in consultation with DDP/MoD shall be carried out once

in two years. Government may also nominate any other agency to carry out security audit of ILDC on an annual basis, to ascertain compliance of security instructions contained in this security manual. Apart from this, the MHA/MoD/respective licensing authority shall be at liberty to visit any company which has been issued with a licence for private sector participation in defence under I(D&R) Act, 1951 & Arms Act, 1959, at its discretion, for a random security system assessment.

12.9 **Penalty for Non-compliance of security guidelines by ILDC:**

12.9.1 In the event of non-adherence of security guidelines by ILDC, action shall be taken against the ILDC and/or individual person(s) as per relevant Government regulations/provisions in various Acts, such as IPC, CrPC, I(D&R) Act, Arms Act, OSA, 1923 etc. The ILDCs are further liable for action against them in the event of any breach of security resulting into compromising national security and national interest under relevant provisions of Official Secrets Act, 1923. The penal action in case of violation of guidelines contained in this manual may also result in cancellation/suspension of Industrial License by the concerned licensing authority. In case of cancellation / suspension of industrial licence, completion of projects/procurement, fore-closures of the unit, the ILDC would be required to return all the classified information and materials in its possession to the rightful owner or Ministry of Defence as the case may be, within 24 hours of such cancellation of the licence.

12.9.2 In case of breach, violation, non-adherence to the provisions of Security Manual, penal provision including financial penalties and denial of various RFPs/technical details/ToTs other contracts by the Government agencies including Service Headquarters, DRDO, DPSUs, etc may be imposed.

12.9.3 For an entity holding license under Arms Act, 1959 (Arms Act) strict adherence to the terms and conditions of the license is mandatory. Any violation of these terms and conditions may lead to cancellation of license and prosecution under the Arms Act, 1959. The provisions of the Explosive Substances Act, 1908 will also be applicable in cases involving in the manufacture, possession, storage or transport of explosives.

12.10 **Alternate Power Source:**

An alternate power source is required to ensure that the system availability is maintained in the event of loss of primary power due to various reasons, including sabotage/subversion.

12.11 **Investigations of compromising emanations:**

Compromising emanations are unintentional intelligence-bearing signals that, if intercepted and analysed, will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment.

12.11.1 Countermeasures will be applied only in proportion to the threat of exploitation and the resulting damage to national security should the information be intercepted and analysed by a foreign intelligence

organization. It is the responsibility of the Agencies of MHA to share intelligence with DDP and DDP may decide further course of action including penal action against the company. The remedial measures on ILDC after prior approval of the Competent Authority will also be addressed.

12.11.2 The MHA & MoD are responsible for performing threat assessment and vulnerability studies when it is determined that classified information may be exposed during investigations / study. Investigations on theft /sabotage will be carried out by CCSO /local police.

12.11.3 ILDCs will assist the MHA & MoD in conducting threat and vulnerability surveys by providing the necessary information upon request:

12.12 **Retention of Classified Documents Generated Under IR&D Efforts:**

ILDCs may retain the classified documents that were generated in connection with their classified IR&D efforts for the duration of their facility is meeting the security manual requirements. Documents shall be clearly identified as "IR&D DOCUMENTS." ILDCs shall establish procedures for review of their IR&D documents on a recurring basis to reduce their classified inventory to the minimum.

12.13 **Classified Waste Management:**

Classified waste shall be destroyed as soon as practicable. This applies to all waste material containing classified information. Pending destruction, classified waste shall be safeguarded as required for the level of classified material involved. Receptacles utilized to accumulate classified waste shall be clearly identified as containing classified material.

12.14 **Waste Management:**

This shall include the scrap generated as well as the components rejected during the (Quality Assurance) QA evaluation, as individual the components may be useless but collectively and over time they could be assembled into a weapon. Comprehensive guidelines should be in place and be periodically reviewed, depending upon the work being executed at the plant with respect to environment, waste management, electronics waste disposal. The guidelines must include explicit procedures for the destruction of electronic devices at the end of their life cycle, especially emphasizing the secure wiping of sensitive data from storage devices to prevent potential data breaches.

12.14.1 Waste Management from health perspective: -Classification of waste will be done as chemical, hazardous, toxic and recyclable collection, transport, processing or disposal, managing and monitoring of waste materials. The term usually relates to materials produced by industrial activity, and the process is generally undertaken to reduce their effect on health, the environment or aesthetics. Waste management is a distinct practice from resource recovery which focuses on delaying the rate of consumption of natural resources. All wastes materials, whether they are solid, liquid, gaseous or radioactive fall within the ambit of waste management.

12.14.2 E-Waste:- Once the electronic device reaches its end of its life cycle, the data on the device must be destroyed by techniques like erasing, wing, and degaussing. Storage devices such as hard disks and flash drives should undergo destruction, and the CISO must issue a destruction certificate, co-signed by a board of officer, verifying the destruction process.

12.15 **Compliance statement:**

Compliance Statement	The company will give an undertaking that it complies with its own instructions/orders as well as all the above provisions as applicable
Internal Security Audit	The company will commit to an internal audit and give self-certification with regards to compliance with the mentioned provisions by 31st March every year to the DDP

12.15.1 In case of Multi Facility Organisation (MFO), the compliance reports will be compiled and forwarded by the Headquarters of the ILDCs.

*****

CATEGORY B

CHAPTER – 1 - General Provisions, Requirements and Responsibilities

1.1 **Scope:**

1.1.1 The Manual is applicable to all Licensee Companies engaged in the production of defence products and issued Industrial License by the Department for Promotion of Industry and Internal Trade (DPIIT), Ministry of Home Affairs (MHA), and Department of Commerce (DoC).

1.1.2 This Manual applies to and shall be used by all ILDCs to safeguard Government classified information and materials released to an ILDC, including, but not limited to, such information released during all phases of the contracting, licensing and grant process, bidding, negotiation, award, performance, and termination, or any product, assembly or component arising out of such classified information.

1.1.3 When an ILDC is executing a Govt Project, dealing with classified information, material, document, it will be the responsibility of CEO, who in consultation with CCSO will earmark the areas as classified/sensitive, depending upon the nature of work being carried out in such areas/zones.

1.2 **Authority:**

1.2.1 The implementation of the manual is the overall responsibility of the Chief Executive Officer (CEO) / Head of ILDCs.

1.2.2 Agencies of MHA and MoD are the designated agencies for inspecting and auditing ILDCs who require or will require access to, or will store classified information and materials covered by this Manual.

1.3 **Responsibility of the Management and Employees**:

1.3.1 It is the responsibility of management and every employee of the company to safeguard the security of all classified information and materials for which the access has been granted in course of duties or which comes into possession in any other way.

1.3.2 It is the duty of each employee of the company to immediately bring to the notice of his superior officer or the Company Chief Security Officer (CCSO), any breach of security regulations in general and/or in particular, any compromise on classified information or materials, either deliberately or inadvertently.

1.3.3 Every employee in the supervisory level is required to ensure, by frequent surprise checks, visits to office rooms and other places where his subordinates work or which they frequent and by all other means in his power, that the instructions laid down for the conduct of business and maintenance of security in company are fully understood and complied with by all of them. It will also be his duty to bring immediately to the notice of his superior officer, or to the officers responsible for security in his department, any instance of breach of security regulations by any member of the staff working under him or in that

department, or of any misconduct, of such a nature as would give rise to doubts about the staff member's integrity/ reliability from the security point of view. The CCSO will maintain the data of all such reported instances along with the Action Taken which will be made available to the external security audit team.

1.3.4 Whenever a new employee joins the company and/or the department, the superior officer of the employee will ensure that the new incumbent has read and understood the contents of the manual and shall take an undertaking in writing to this effect.

CHAPTER – 2 - Security Organization and Personnel Security

2.1 **Company Chief Security Officer (CCSO)**:

Each ILDC or its multi-location units shall appoint an Indian Citizen as the CCSO with adequate knowledge of security. The CCSO would ensure that security measures necessary for implementing applicable provisions of this Manual are in place and the manual is being implemented in the true spirit of the intention. Persons of Indian Origin and Non-Resident Indians shall be excluded from such appointments. Person with adverse remarks, if any, in his/her release certificate shall not be considered for appointment The security qualifications of CCSO will be as per Government guidelines issued from time to time. Further, the CCSO will be positively vetted by agencies of Government through Nodal Office, DDP before hiring and after every 3 years. The CCSO will be responsible for framing internal security policies, Internal Audit, Training, Review and updation of Security procedures, Up-gradation of Security Equipment etc., Liaison with other Departments / Organizations, Civil and Law Enforcement Authorities and Intelligence Agencies of Centre and State, etc. The CCSO may be assisted by additional staff based on requirement and size of the company and should report directly to CEO or Executive Head of the Company.

2.2 **Cyber Information Security Officer (CISO)**:

Each ILDC shall appoint/ nominate a Cyber Information Security Officer(CISO).The CISO will be positively vetted by agencies of Government through Nodal Office, DDP before hiring and after every 3 years. The function may be accomplished by one senior officer having necessary and sufficient knowledge on IT system of the organisation in addition to his/her job. In case of company with more than Rs 250 crore turnover, a dedicated CISO shall be appointed. The CISO will be responsible for framing and implementing a suitable Cyber Security policy, conduct of cyber security audit and cyber security training for the organization etc. He shall also be responsible for incident management, identification of the organizations Critical Information Infrastructure assets and interaction with NCIIPC/CERT-In/Nodal Office, DDP and other agencies of MHA and MoD, as the case may be. The CISO must be of sufficient seniority to report directly to senior most management of the organization to ensure functional independence. The CISO may be assisted by additional staff as per the requirement of ILDC. It is the responsibility of the CISO to ensure that the organizational cyber security policy is adequately framed, implemented and audited to ensure necessary and sufficient protection from cyber threats. The CISO shall also clearly identify residual risk subsequent to implementation of requisite cyber security mechanisms.

2.2.1 Following organizational structure for Cyber Security shall be followed in ILDCs :-

2.2.1.1 Duties of Management Tier:

The Management Tier, headed by the CEO/MD, assisted by CISO and CIOs, shall have the following roles and responsibilities:-

a) Responsible for taking executive decisions pertaining to ICT infrastructure for Organisation.
b) Decision making body for overall policy matters.
c) To take strategic decisions and evaluate opportunities in the field of Cyber Security and Cyber Defence, and countering cyber threats.
d) To ensure maintenance and enhancement of the overall cyber posture of the organisation.

2.2.1.2 Duties of Chief Information Security Officer:

a) Ensuring cyber security posture of the Organisation
b) Implementation of cyber security controls over entire network.
c) Cyber security and incident response.
d) Maintain awareness of emerging threats and vulnerabilities.
e) Implementation of Cyber Crisis Management plan.
f) Internal Information security audit of IT systems and controls
g) Maintaining and updating the threat landscape for the Organisation.
h) Ensuring review of the Cyber Security Policy by the designated expert agency to check for the adequacy and effectiveness of the existing policy in force.
i) Disseminate information security policies, procedures and guidelines to all concerned.
j) The CISO through Cyber Security Division is to ensure that the following activities are carried out at regular intervals:-
    (i) Internal Information Security Audit is carried out of all IT Assets on a yearly basis
    (ii) (Periodic assessment/ audits of third party service providers to assess risks to the Organisation.
    (iii) (Ensuring that clauses pertaining to Information Security are incorporated into contracts/ agreements/ MoUs with service providers.
    (iv) Ensuring that Incidents, especially repeat incidents are investigated and corrective action taken as identified through a comprehensive Root Cause Analysis (RCA).
    (v) Implementing automated and continuous monitoring of security incidents and breaches, and maintaining record of the same.

2.2.1.3 Duties of Information Security Officer (At Wing / Division / Sector level):

The ISO shall be responsible for the following:-

a) Training & awareness at Division/ Section level.
b) Information privacy at Division/ Section level.
c) Implementation of Cyber Crisis Management plan at Division/ Section level.
d) Information security audit of IT systems and controls at Division/Section level.

e) Ensure that every IT Asset under his/ her administrative control is assigned a custodian.
f) Ensure that an IT inventory file is maintained for the respective Division which will define the details of the IT Asset along with the custodian/ user.
g) Ensure that the changes in the ownership are logged in the IT Asset file. The format for collating the details of IT Assets.
h) Ensure that the IT Assets are not moved out of the respective division for which they were initially allocated without approval of the CISO. However, the same shall be properly documented.
i) Ensure that the policies as laid down in this Cyber Security Policy are disseminated across to all personnel within the division.
j) Ensure strict compliance with the laid down policies with respect to physical security of IT Assets.
k) Comply with the instructions/ guidelines laid down as a part of the Cyber Security Policy.
l) Act as the Nodal Officer for his/ her particular Wing/ Division/ Section as applicable for matters related to Cyber Security.

2.2.1.4 Duties of Cyber Security Division:

a) Cyber Security Audits of the Organisation.
b) Function as operations support and emergency response provider in case of Cyber Security incidents with the Organisation.
c) Handling cyber threats, vulnerability detection/ mitigation etc.
d) Advise IT division of the organisation for effective patch management of ICT infrastructure. Issue guidelines for timely dissemination of patches/Hot fixes/Service packs/Updates for IT assets.
e) Formulate and disseminate Cyber Security advisory on latest cyber security threats and trends.
f) Issue security advisories and instructions.
g) Ensure the cyber hygiene and compliance to Cyber Security policies of the Organisation's IT assets.
h) Carry out risk analysis and suggest mitigation measures/ enhancing security of the organisation.
i) Support in formulating Cyber Security policy and carrying out periodic review in consultation with ISO & CISO.
j) Organise periodic training and awareness campaigns for Personnel on Cyber Security.
k) Organise seminar/conference on cyber security to brainstorm/assess the current challenges/requirements of the Organisation.
l) Ensuring furnishing of all reports mandated by Security Manual to MHA/DDP//DPIIT/DoC/Nodal Office in DDP.

2.3 **Security Staff:**

The ILDC must employ security guards. These guards should preferably be from Defence Security Corps(DSC)/ Central Industrial Security Force (CISF)/

Director General Resettlement (DGR) empanelled agencies having Private Security Agencies Regulation Act (PSARA) License.

2.4 **Responsibilities and Duties of CCSO:**

a) To implement the security provisions as laid down in this Manual.
b) To clearly demarcate the areas as Sensitive/Classified area/zone/manufacturing facility where the work related to MoD Project is going on and ensures that necessary boards indicating such areas are displayed.
c) To keep himself fully conversant with all security instructions and ensure that the security instructions are fully understood by all employees and are implemented or complied with, within their respective sections and offices.
d) To be responsible for the proper conduct, discipline and performance of all the personnel in Security department.
e) To be responsible and ensure that fire service section is fully equipped and personnel are well trained. He shall take prompt action whenever necessity arises.
f) To be responsible for the duties of his subordinate staff and carry out any other lawful and reasonable orders issued to him by management.
g) To carry out periodic surprise checks and maintains a record of such checks.
h) To submit report to the CEO/Head of the sub units/division of the company indicating lapses noticed by him as and when it occurs.
i) To arrange regular programs to apprise the employees on security matters.
j) To maintain constant liaison with law enforcing agencies and nodal offices in Ministries.
k) To carry out improvement in the security system for the premises under his charge, as required, over and above the security manual.
l) To arrange Internal & External Security Audits
m) To carry out a comprehensive personnel risk assessment, short listing of suspects and keeping them on watch list in coordination with HR and Vigilance Department.

2.4.1 <u>When breach of security occurs, the main objectives shall be</u>: -

(a) To swiftly find out what has happened and modus operandi of the breach committed.

(b) To minimise the damage done.

(c) To investigate/ trace the culprit and report to CEO/ head of the company by fastest mode of communication.

(d) To prevent recurrence and suggest remedial measures.

(e) To report Cyber Attack/Data Breach to CISO**.**

2.4.2 If classified information or materials have been compromised/ lost/ found in wrong place, it is to be reported by concerned employee immediately in writing to the CCSO who shall take necessary action.

2.4.3 As and when cases of security violations are detected by the Security Staff, the same is to be reported to the CCSO on occurrence. These will be followed immediately by formal violation reports addressed to the head of the department who will thoroughly investigate the matter and furnish an action report within a week.

2.4.4 Enquires to have a tentative time frame by which it will be completed, in addition, progress report shall be submitted to the office of the Company Chief Security Officer till the case is finalized.

2.5 **Reporting Procedure:**

2.5.1 The ILDC shall, at the earliest, report in writing to the nearest Police Station, local office of agencies of MHA and the Nodal Office, DDP regarding any information or materials in regard to actual, possible or probable espionage, sabotage, terrorism, subversive activities or adverse information about any employee(s) in any of the ILDC locations immediately on occurrence. In addition, if the breach has led to data loss/compromise in cyber-security, the same will also be intimated to the Nodal Office, DDP at the earliest. Logs of all security violations/reporting shall be maintained by CCSO /CISO with the corrective actions taken in this regard as shown below -

S.No	Description of violation	Date and Time of incident	Date and Time of reporting to the authorities	Action Taken

2.5.2 The ILDC shall also report to the Nodal Office, DDP the following:-

a) Unauthorized receipt of classified material.
b) Any significant vulnerability identified in the equipment or material being manufactured.
c) Inability to safeguard classified material.
d) Report of loss or suspected compromise.

2.5.3 The ILDC shall forward to designated agency the reports as given below: -

S. No.	**Periodicity**	**Title of Report**	**Report to be rendered**
1	Quarterly	Loss /recovery/ unearthed Arms and Ammunition and Explosives – Annexure-VIII	Nodal Office, DDP
2	Immediately & Quarterly	Fire accidents & other incidents / accidents – Annexure-XII & Annexure-XIII	
3	Quarterly	Visits of foreign business visitors- Annexure-X	
4	Quarterly	Action taken report on, MoD/MHA agencies' visit-	

		Annexure-XI	
5	**Quarterly**	**Cyber Incidents-** Annexure-XII & Annexure-XIII	**Nodal Office, DDP**

Incident pertaining to theft, fire, espionage, loss of ammunition etc., will be reported to nearest police station and Nodal Office, DDP immediately on occurrence, over and above, the same will be reflected in quarterly report.

2.6 **Personnel Security:**

2.6.1 Every ILDC shall ensure that no security leakage occurs through any personnel due to any reason, including, but not limited to, the following: -

a) For personal gain.
b) For political affiliations.
c) Carelessness in talk and in handling documents.
d) In correspondence.
e) In communication.
f) Transmission of classified documents.
g) Conversations.
h) In case of any breach in the cyber security infrastructure of the ILDC, (National Critical Information Infrastructure Protection) NCIIP / (Computer Emergency Response Team- India) CERT-In/ shall be notified at earliest with a copy to Nodal Office, DDP. The ILDC shall ensure that all requisite information / assistance is provided by its personnel to support activities of NCIIP / CERT-In/Nodal Office, DDP /other agencies of MHA and MoD.

2.6.2 To ensure that there is no leakage of information it is necessary to observe the precautions given below: -

a) Character and antecedent verification through police, reference checks, previous employment verification has to be carried out for all persons before joining the ILDC
b) In case any adverse police report is received against an individual dealing with classified matters, on re-verification, generally after every three years, he or she shall be transferred out immediately. Persons employed on TOP SECRET work shall be subjected to prior positive vetting by Nodal Office, DDP, and also every two years thereafter. In case adverse police report pertains to national security, an enquiry shall be initiated by Plant Security Council**(**defined in para 3.7**)** under relevant law/act/internal guidelines, the individual shall not only be suspended but also barred from office access during the course of enquiry.
c) Only permanent employees shall be posted in TOP SECRET and in SECRET sections to deal with classified documents.
d) Police Verification shall be conducted i.r.o. all contractual / temporary employees /casual workers, before being engaged.

e) The employees of the company including those of the foreign collaborator, involved in design, development and production of Defence materials shall be cleared from security angle. The list of employees cleared from security angle and engaged by the licensee in design, development and production of defence materials shall be maintained by the licensee and furnished to Nodal Office, DDP every quarter. The licensee shall define the code of conduct of such persons.

f) All Officers should abide by the provisions laid down in the Official Secrets Act, 1923 and give a declaration to that effect.

2.6.3 It is the duty of every employee to bring to the notice of CCSO if they notice any suspicious behaviour of employees dealing with classified information like late staying in the office, making copies of document, frequent unauthorized absence, drunkenness and living beyond means etc.

2.6.4 Unconscious leakage due to carelessness or egoism often occurs at all levels, and even senior officers are not immune from this fault. It is the duty of every superior officer to make note of any such faults if any of his subordinates and suitably caution the officer against such lapses.

CHAPTER – 3 - Security of Premises and Physical Security Measures

3.1 **General:**

All Defence related installations automatically fall under category of 'Prohibited Place' under the Official Secrets Act, 1923. A display board to this effect shall be installed in trilingual at the main gate and around, also contemplating 'trespassers shall be prosecuted'.

3.2 **Physical Security Measures**:

Physical security means security in the form of safeguarding the installation which would comprise of providing adequate safeguards against an intruder coming from outside to damage the installation. This includes securing the perimeter walls, gates, lighting, access control system of entry, protection of vital stores and designating restricted areas.

3.3 **Layout of Premises**:

The installation must have perimeter as under

3.3.1 A 8 Ft wall with barbed wire fence / concertina coil.

3.3.2 Spot lights with Day & Night CCTV Cameras.

3.3.3 There should be lighting arrangement all along the perimeter wall to allow clear observation during hours of darkness.

3.3.4 To reinforce manual observation and to have data available for investigation, the perimeter should be covered by CCTV with recording facility for 90 days. The Guidelines issued by Ministry of Electronics and Information Technology (MeitY) on CCTVs from time to time shall be strictly adhere to.

3.3.5 There should be minimum number of gates. The material gate should be different from those meant for the employees.

3.3.6 Biometric Access Control system must be installed.

3.3.7 At the employee's gate, there should be provision for Door Frame Metal Detector, Hand Held Metal Detector, and separate frisking room for ladies.

3.3.8 The gates must be covered by CCTV.

3.3.9 A control room to monitor the CCTV's be established and manned round the clock.

3.3.10 The administrative area should be well demarcated from the manufacturing area.

3.3.11 Road barriers, speed breakers, boom barriers, Tyre busters etc., be employed at the gate.

3.3.12 Trolley Mirrors to be used for inspecting under carriage of vehicles.

3.3.13 All vulnerable areas/places, perimeter wall, gates, parking area and building/structures should be adequately illuminated.

3.3.14 Sitting of electric poles should not facilitate scaling of perimeter wall / fence by intruder.

3.4 Reception Office and Visitors:

3.4.1 Entry of visitors to classified area/zone/office shall be regulated through the Reception Office. The reception shall ascertain the purpose of visit and obtain the concurrence from the officer to be visited. A visitor management system be put in place for issue of photo passes to all visitors. Entry of the visitor in the classified area/zone/office would be authorised by CEO/Head of ILDC for official purpose only.

3.4.2 No visitor would be allowed to carry laptops, pen drives, mobile phones and any kind of storage devices or Bluetooth devices inside the premises. Entry of such items could be allowed only to non-classified area for the purpose of meetings that too on specific permission of CEO/CCSO of the installation.

3.4.3 Visitor's vehicle shall not be permitted to enter in the installation and would be parked at designated parking areas for visitors. If required, the visitors shall be taken to the designated classified area/zone/office in vehicles; specially used for such purposes by the concerned office/company or organisation.

3.4.4 The visitors will, at all times, be escorted during their visit to the classified area/zone/office and will not be left unattended or unescorted. The visitor shall not be allowed to leave the reception office without an escort.

3.4.5 Official visitors from Ministry of Defence, Government of India, MHA in possession of valid ID cards will also be issued with the visitor's ID card at the reception office; however, such visitors need not be escorted inside the classified area/zone/office.

3.4.6 No visitor shall be entertained after working hours. In exceptional circumstances where a visitor has to stay beyond the specified time, clearance of designated officer as decided by CCSO should be taken and security should be kept informed of the same.

3.4.7 Security Control room shall be situated near the factory main gate.

3.4.8 Medics: First Aid Room & Tie up with local Hospitals.

3.5 **Material Gate:**

Entry & exit of all material, raw, processes, garbage and scrap must take place only through the designated gate, which, as far as possible, should be divested from the employees. Provision of Weigh Bridge be made at the material gate

3.5.1 Communication: Gates are required to be connected to the security control room besides the office and residence of the security officer through a communication network that is dependable and operational around the clock.

Also, alternate means of communication in the form of radio telephony should be available at the gates/ watch towers to ensure uninterrupted communication.

3.6 **Watch Tower:**

The following points need to be kept in mind while sitting and constructing watch towers, if required based on criticality of the installation and the assessed threat perception:

i) Sitting: Watch towers should be sited tactically so that the area around is dominated with clear visibility towards both the adjacent towers. There should be no dead ground or blind spots between any two towers. In case of any dead ground, the area should be covered with artificial obstacles.

ii) Height: Depending on the height of the perimeter wall and the construction around and within the installation, the height of the watch tower from the ground should be at least 15' to 20' in order to provide a clear field of observation all around.

iii) Staircase: The stair case leading to the watch tower should be made in such way that the security personnel on duty do not find any difficulty in negotiating the same while carrying their weapons and other equipment.

iv) Sentry Post: The cubicle on the top of the watch tower should facilitate in the performance of watch duties of the sentry and also allow him to use his weapon effectively when the need arises:

(a) The walls should not be more than 4 feet.

(b) There should be protection from incoming harsh sunlight and rain.

(c) The size should permit the sentry adequate space for movement.

(d) In case windows are provided they should have wide angles for maximum observation.

(e) Lighting inside the post should be avoided to prevent outsiders from keeping a watch on the movement of the sentry and also facilitate a clear and effective observation of the area during hours of darkness / poor visibility.

v) Vision Devices: Day and night vision devices may be provided to the sentries based on the criticality of the installation and the assessed threat perception. Watch Towers may be equipped with dragon lights, Walkie-Talkie sets/intercoms and High mast light/revolving flash lights etc.

3.7 **Setting up of Plant Security Council:**

A Council to be constituted under the chairmanship of Head of Unit with CCSO as member Secretary, CISO as a permanent member and other divisional/section heads as members. The Council shall meet quarterly and review the existing security requirements/arrangements and take corrective actions. In case of Multi Facility Organisation, Headquarters security representative will also be included as a member in the quarterly reviews. The Record of the proceedings shall be maintained by the company.

The council may also bring to the notice of Local Police/Nodal Office, DDP any cases pertaining to security violation, theft/pilferage, espionage, sabotage, terrorism, subversion activities or adverse information about any employee.

3.8 **Identity Badges, Entry Passes for personnel /vehicle and Parking of Vehicles**:

Entry into Classified zone/area/offices would be regulated on the basis of photo Identity cards issued by the CCSO. The Identity Badge should have following details:

a) Company logo

b) Name and photograph of the employee

c) Staff Number and pass number

d) Signature of issuing authority

e) Blood group

f) Date of issue and validity

g) Signature of employee

h) Address of Unit

3.8.1 These ID cards are to be returned to CCSO on the date of expiry of their validity or when no longer required. The identity badges should be reissued once in 5 years so that latest photo is reflected on the badge. The Security Department should keep relevant account of badges issued. All employees shall follow the following instructions: -

a) Every person, irrespective of designation, rank and status will display his or her Identity Card or any other identity document issued by the CCSO for verification by the security personnel on duty at all times while inside classified area/zone/office.
b) Impersonation of the authorised holder of identity card or its alteration, destruction or transfer to another person would be a punishable under relevant laws.
c) In case any individual found within the classified area/zone/office is not able to produce his or her identity card or pass, he or she will be brought to the office of the CCSO for further necessary action.

3.8.2 Other than the Identity cards for the permanent employees working in the classified area/zone/office, the CCSO may also issue following Identity documents: -

a) Temporary Photo Identity Card To be issued to personnel of the company or organisation who are working in the classified area/zone/office on temporary basis or for a short duration.
b) Visitor Pass. A list of officers who are authorised to receive visitors as per the Company rolls shall be available at reception. Passes would be issued using Visitor Management System by the reception/security office

on production of a valid identity photo document by the visitor (like passport, services ID card, driver's license, PAN card, Voters I card). The pass should be returned by the visitor at the gate on completion of the visit and endorsement of time and signature by the officer visited upon is to be checked. Online system should be in place for min 1-year retention and tracking of visitor details along with the photo for future analysis / investigations required if any.

c) Labour Pass Labour pass with photo would be issued by the office of CCSO for casual labourers who are working for a specific period/term. These passes should be issued to labourers whose character and antecedents have been verified by the police.

d) Token labourer Tokens should be issued on daily basis for labourers employed for constructions / other duties. The contractor employing such labourers should be accountable & responsible for such casual labourers for the duration of working inside the plant. To this effect, an undertaking may be obtained from the contractor.

3.8.3 Vehicle Stickers: Vehicle stickers would be issued by the CCSO to employees who are on permanent basis and who have a valid photo ID card issued by the CCSO for parking in designated area outside the installation.

3.8.4 Loss of Identity Cards: Loss of ID card should be reported immediately to the CCSO along with an investigation report from the concerned section/office. CCSO may thereafter take further necessary action as per the policy of the company/office/organization. A database of stolen/lost ID cards will also be maintained with proper and regular Cyber audit of the computers used in the issuance of ID cards.

3.8.5 All sections shall maintain a list showing name, designation, identity card number, local resident address and permanent home address contact number of the employees working in area/zone/office handling classified information.

3.8.6 The ID card, vehicle sticker and any other documents issued to an employee would be withdrawn and submitted to the CCSO prior to dismissal, suspension or transfer of the employee.

3.9 **Keys of the Organization:**

3.9.1 Keys to the offices rooms/areas/zones holding classified information should be kept in a secured designated placed at the office of CCSO. The access to the secured designated place will be strictly limited. The keys can be drawn or deposited by an employee who has been authorised to do so by the head of department/officer in charge of the section or office. While authorising employees to draw the keys, it would be ensured that rotation system is followed and casual labourer is not detailed for opening and closing duties. In case of loss of keys, the matter shall be reported to the CCSO. Key registers shall be maintained for record.

3.9.2 Prior to submitting the keys, the nominated person shall ensure that all the windows are closed and window blinds and curtains are open to detect any unauthorized movement / fire.

3.9.3 A Team under CCSO should carry out random checks of the rooms after office hours to find security lapses, if any, on the part of the occupants of the rooms after they leave the premises.

3.10 **Late Sitting in Office:** Staff may sit in their office in the classified rooms/areas/zones under supervision of an officer. In case any staff is required to work on Holidays, or beyond stipulated working hours, a letter authorising him to do so would be sent to the CCSO by the departmental head. However, work classified as TOP SECRET and SECRET can only be performed under the supervision of an Officer. The person so authorised shall also be responsible for drawing and submitting of the room keys.

3.11 **Photography:** Photography/Videography on ground or aerial (through drones/UAVs) wherein any work related projects/ manufacturing of MoD is being carried out will not be permitted without the approval of MoD. Warning sign boards to this effect shall also be displayed at the main gate as well as inside the premises at vantage points. The guidelines of Ministry of Civil Aviation on Drone/ Drone threats issued from time to time shall be strictly adhere to.

3.12 **Carriage of Weapons:** Carriage of weapons, other than by the staff of CCSO would be strictly prohibited inside the Classified Zone/Area. Permission may be accorded to official security guards of visiting personnel, after obtaining specific prior permission of the CCSO. A kote is to be made near the office of CCSO where weapons can be stored and only authorised supervisor cadre is allowed to operate.

3.13 **Carriage of Liquor:** Carriage and consumption of all kinds of liquor(including beer, wine and all alcoholic drinks) would be strictly prohibited inside the plant.

3.14 **Security Measures for Sensitive / Secure / Storage Areas for Classified Equipment:**

The storage area may be declared as Vital Point with the following safeguards:-

(a) Additional Boundary Wall and Power Fence to prevent any intrusion, if required.

(b) Access control for authorised personnel through photo identity and/or proximity/smart/biometric card based systems.

(c) Frisking and Baggage screening of employees of persons moving in/ out of the Vital Point shall be enforced.

(d) Banning electronic gadgets, cameras, storage devices inside the Vital Points shall be enforced. Carrying of Smart phones high-end mobileswith camerasand other features also to be banned.

(e) Patrolling in and around the Vital Points including night patrolling by Guards and Dog squads if required shall be carried out. Night patrolling

should be mandatorily provisioned at staggered intervals covering the entire perimeter along with vital points.

(f) CCTV surveillance must be provided at entry / exit of Vital Points and other sensitive locations inside the factory. Recording of all CCTV footage should be kept for 90 days.

(g) A two key system may be used for stores holding sensitive hardware wherein two authorised persons, one from Security and the other from stores / user Department, may be detailed.

(h) Suitable Fire-fighting and Emergency / Disaster management measures to be instituted.

(i) Proper foolproof access control to be established.

(j) ILDC should ensure that adequate fire-fighting mechanism is in place so as to ensure that no untoward incidents happen in the premises due to fire.

3.15 **Building Security:**

It shall be ensured that the buildings are constructed at a distance from the compound wall so that there is no intrusion from outsiders. Wherever possible no construction zone of 50 ft from compound wall may be maintained.

3.16 **Emergency response/contingency plan:**

In the event of emergencies like accidents, terror attacks, strikes, etc. the following procedure is to be followed:

(a) Activation of control room with immediate intimation to police and local authorities and a team of other officers, disaster management mechanism to be activated for taking charge of the situation.

(b) Display of contact details along with telephone numbers of the higher officials.

(c) Display of contact details of local police, special branch, hospitals, bomb disposal team and local authorities in conspicuous places within premises of ILDC besides at security control rooms.

(d) Emergency exits/ route plan to be identified.

(e) The above actions should be in accordance with the Disaster Management Plan as per the guidelines/instructions issued by the National Disaster Management Authority/State Disaster Management Authority.

CHAPTER – 4 - Material Security

4.1 Incoming and Outgoing Material:

No railway car, truck or other vehicle conveying crates, boxes, machinery, repair parts, fuel or other material should be admitted to the plant without first being examined and thoroughly searched by a guard for concealed explosives, contraband items, incendiary devices or other hazardous items. No material should be allowed to go out of the factory area without a proper pass from an authority authorized for the purpose. Such authority should be restricted to a few officers only and their specimen signatures should be available at the gate for easy and quick identification. Computerized Material Management System (CMMS) for returnable/non-returnable goods may be installed for generating gate pass and data backup.

4.2 Inward Material Register:

Entry will be made in the register in respect of all materials that come into the plant, either brought by the contractors as sample, or brought by the stores officers as supplies/samples, for which inward materials gate pass has been issued by the security gate officers. Samples and such other materials taken back should be crossed out after the party has returned the inward materials gate pass.

4.3 Material Gate Pass Register:

This register shows materials that went out of the factory under an authorized gate pass. The time and nature of materials sent out and brought back shall be recorded by the gate staff. The time and nature of materials sent out shall the gate staff showing that the item is brought back. The time of return however should be noted. A specimen signature book showing the signature of the officer authorized to sign passes should also be maintained.

4.4 Material Gate Pass:

A model material gate pass procedure is given below. The ILDC should, as far as possible, evolve a proper gate pass procedure to suit the conditions prevailing in the respective divisions and get it issued under the signature of the competent authority for compliance: -

4.4.1 Description of material gate pass:

There will be two types of material gate passes, viz.,

(a) Non-returnable material gate pass; and

(b) Returnable gate passes.

4.4.2 A non- returnable gate pass should be issued for the materials, which are taken out of the factory on permanent basis or for materials issued to sub-contractors etc.

4.4.3 A returnable gate pass will be issued for materials, which are sent out of the factory on returnable basis. Returnable gate pass will be issued only to such materials, which will come back in the same form without undergoing any change. For finished goods and items against customer order, gate pass will be issued only by the stores.

4.5 **Authority:**

The CEO/Head of the Organisation will authorise a limited number of Officers who will be authorised to sign the material gate passes. The specimen signatures of authorised officers signing the material gate pass will be made available at the security gates.

4.6 **Gate Pass Specification:**

The concerned officer of the security department in charge of the guard room should take the following action: -

(a) Verify the signature in gate pass with the specimen.

(b) Check the materials as per the gate pass.

(c) Affix security outward seal and attest his signatures on the gate pass.

4.7 **Returnable Material Register:**

Control SL. Nos. Should be given to the gate passes for taking out returnable materials A 'RETURNABLE MATERIAL REGISTER' should be maintained by the officer in charge. Proper entries should be maintained giving the reference numbers of the gate pass, authority for sending out materials.

4.8 **Material sent out register:**

It is the responsibility of the department concerned to account for the materials sent out. Proper register should be maintained giving the reference number of the gate pass, authority for sending out materials.

4.9 **Abnormal Delays:**

The material sent out on returnable basis should be brought back within the stipulated period mentioned in the gate pass. Cases where there is abnormal delay will be brought to the notice of the concerned departmental head by CCSO for taking suitable action. All abnormal delays will be documented with specific reasons.

4.10 **Issue of Gate Passes:**

Gate pass should be issued to all materials including stationary items taken out of the gate.

4.11 **Transfer of classified information:**

When drawing in CDs/any electronic form are exchanged with subcontractors/ vendors in case outsourcing activity involving technology transfer of classified

projects or indigenous classified projects for manufacturing components, it should be sent in sealed cover with material gate pass signed by authorized personnel.The CCSO will authorise a person for supervising the movement of such information. Sealing & dispatch should be done appropriate to the classification of projects. The subcontractor/vendor who has been given any classified project or information would also be bound by the provisions under "Official Secrets Act, 1923".

4.12 **Items brought by customers/suppliers as samples or for demonstration:**

Items brought by customers/suppliers as samples or for demonstration /tryout /rectification /repairs etc. should be allowed 'INWARD GATE PASS' by 'Security in-charge' at gates. The materials will be allowed to be taken out on the same gate pass after making proper entry in the office copy of the INWARD GATE PASS book. This procedure will be applicable to materials brought as samples. In case any electronic items(s) is/are brought inside by the customers or suppliers as samples or for demonstration/try out/rectification/repairs etc, it/they shall be authenticated through the CISO.

4.13 **Bulk Materials:**

For bulk materials brought by contractors for their work, a proper gate pass should be issued for taking out the balance materials giving reference of the INWARD GATE PASS issued by the security department.

4.14 **Secret Documents:**

The officers of the civil engineering department, purchase department and technical department should ensure that graded official documents of any nature including blue print should not be sent out without gate pass. A broad outline of instructions on handling of classified documents and safe guarding against the exchange of information is given at chapter-5.

4.15 **Material brought on cash purchase Basis:**

Certain materials are purchased on cash purchase basis. Once a gate entry is made for such materials the materials should also be taken out only on material gate pass. This is accounting for control purpose.

4.16 **Repair hand tools:**

Hand tools by plumber, electricians and mechanics of transport department who attend to repair will be taken out after making proper entries in the register maintained at the guard room.

4.17 **Use of ERP/IFS:**

A system may be evolved for recording & tracking of materials using ERP/IFS.

4.18 **Transportation of Sensitive and Classified Materials:**

a) There shall be empanelment of only security vetted transporter/carriers and drivers verified through local police for transportation of classified material/sensitive goods.
b) In order to avoid any sabotage en-route it should be ensured that the vehicles carrying explosives and classified materials are escorted by armed guards.
c) Secrecy should be maintained about the transportation plans/date/route etc.
d) Constant communication should be maintained while transporting explosives and classified materials.
e) It is the responsibility of the company to hand over classified material/finished product to the rightful owner, i.e. purchaser.
f) Superintendent of police of the districts falling on way should be kept informed about transportation of explosive and classified materials. Consignor as well as consignee would keep the Superintendent of Police of the district falling on way between the place of consigner and the place of consignee informed.
g) When classified Equipment is sent by road in India, the vehicles will, as far as possible, be harboured during the night in Military unit en-route. The information for such an arrangement has to be forwarded to MoD well in advance of the planned movement, to arrange for the necessary security clearance with the military authorities concerned. In absence of Military units they will harbour within civil police station. Where neither of the two courses is possible, the dispatching authority will approach the civil authorities through their higher formation, for affording security protection and other assistance to the convoy en-route. The superintendent of police of the district falling on the way between the place of consignor and the place of consignees should to be informed. GPS tracking devices on the equipment / vehicles to continuously monitor the movement of classified materials / equipment may be installed.

CHAPTER – 5 - Handling of Documents and Equipment

5.1 Security Classification of Documents and Equipment:

5.1.1 Aims & objective of Document / equipment Security: To prevent a spy or an enemy agent from access to classified information/ equipment, to help CCSO in investigations into cases of leakage and spying and to implement the theory of security based on the principle of need to know, need to take and need to retain. Besides, classified document should be kept in such a secure place, where only authorized officials should have access.

5.1.2 Matters related to suspicious cases of leakages of classified information/theft should immediately be informed to CCSO and head of the company for a thorough investigation, taking serious view of such security lapses and breaches, dealing appropriately against delinquent official / person. However, outcome of investigations should be reported to CCSO and head of the company, for taking preventive and remedial measures for strengthening the security system.

5.1.3 Classification of Documents and Equipment: A clearly laid out Data Classification policy shall be put in place by ILDC. Absence of policy and its implementation shall be treated as a violation of this Manual. Documents and equipment shall be classified as follows: -

a) **TOP SECRET.** "TOP SECRET" shall be applied to information and equipment, the unauthorized disclosure of which could be expected to cause exceptionally grave damage to the National Security or national Interest. This category is reserved for the nation's closest SECRETs and is to be used with great reserve.

b) **SECRET**. "SECRET" shall be applied to information and equipment, the unauthorized disclosure of which could be expected to cause serious damage to the National Security or National Interests or cause serious embarrassment to the Government in its functioning. This classification should be used for highly important matters and is the highest classification normally used.

c) **CONFIDENTIAL**. "CONFIDENTIAL" shall be applied to information and equipment, the unauthorized disclosure of which could be expected to cause damage to National Security or could be prejudicial to the National Interests or would embarrass the Government in its functioning.

d) **RESTRICTED**. "Restricted" shall be applied to information and equipment which is essentially meant for official use only and which should not be published or communicated, to anyone except for official purpose.

e) **UNCLASSIFIED**. The designation UNCLASSIFIED is used to identify information and equipment that does not require a security classification.

Note: Documents or equipment not covered by any of the above categories shall be regarded as unclassified.

5.2 **Guidelines on Classification**

5.2.1 A document should be given a classification which it really deserves. Over classification or under classification can be detrimental.

5.2.2 If a document or equipment bearing higher security classification is added to a file, document or material, the file/document/ material itself will be upgraded to that classification.

5.2.3 The document or equipment as a whole shall bear the highest security grading that any particular part of it may deserve. The grading of a file or of a group of physically connected documents or materials must be that of the higher graded document/ material therein.

5.2.4 Officers authorized to classify: The originator of the document will be authorized to classify the document / upgrade / downgrade the same. It is the responsibility of the originator that care is taken of such documents so that the same do not fall in the wrong hands. The overall responsibility of safeguarding classified documents will be of the CEO/ head of the company who shall take all necessary precautions / audits / review mechanisms as deemed fit. The level of officer in a company to initiate/handle classification of classified documents (Top Secret, Secret, Confidential & Restricted), should be designated by the CEO/Head of the Company.

5.3 **Marking of Classified Documents and Equipment**:

The classified documents and equipment shall be prepared and marked as per the guidelines described below, as applicable, in the following manner:

5.3.1 All documents including Files, folders, binders, envelopes, and other items containing classified documents, noting of the file containing classified matter will have the security classification printed, stamped or typed in bold capital letters on the top and bottom centre of each page of the document. Any insertions, such as maps, or illustrations of an individually classified nature will also be similarly marked.

5.3.2 File covers containing TOP SECRET documents will be marked with a diagonal Red Cross of one cm in width thickness extending from corner to corner on both the front and back covers.

(a) A separate record of all TOP SECRET case files will be maintained in a register of TOP SECRET documents and docketed by the authorized officer. He should also carefully monitor movement of such files.

(b) Even part files, if opened in relation to any classified document, will have the same security classification and will also be properly docketed.

5.3.3 SECRET files covers should carry a red vertical line in the centre.

5.3.4 TOP SECRET, SECRET, CONFIDENTIAL OR RESTRICTED drawings or tracings are to be marked in such a manner that the marking will be reproduced along with the main text whenever copies are made there from.

5.3.5 TOP SECRET, SECRET OR CONFIDENTIAL maps and charts are to be marked under or near the scale. For marking by stamp, red endorsing ink pads are to be used.

5.3.6 TOP SECRET documents should, wherever feasible, be printed or written on coloured paper, so that they may be easily recognized.

5.3.7 Marking for ILDC Developed Information and Equipment - Any information or materials arising in any manner out of classified information released to an ILDC shall be treated at the same classification level as was attached to the original information or material released.

5.4 **Accounting of Classified Documents and Equipment:**

5.4.1 Reference Number: Classified documents and equipment shall be given code or other reference number, which will be used in correspondence to avoid reference to their titles and subject matter.

5.4.2 Copy numbers or Receipts or making of Spare Copies. The following important aspects shall be kept in view in this regard: -

a) When more than one copy of TOP SECRET document is made, they shall be given copy numbers and each page shall be serially numbered.
b) The transmission of TOP SECRET and SECRET documents shall be covered by a receipt system. The sender shall enclose a receipt for completion and return to the sender by the addressee.
c) If the receipt for a classified document does not reach the issuing authority within seven days, the issuing authority shall ascertain whether the document has in fact been received, if not the same to be reported to CCSO.
d) Letters or documents including appendices, if any, shall have continuous page numbers. The total number of pages of a TOP SECRET or SECRET letter or document will be indicated in words below the security classification on the top centre of the front page.
e) The Typist besides noting down his initials at the foot of each classified paper typed by him/her, should also note the number of copies made.
f) Whenever a TOP SECRET document is required for preparation of additional copies for simultaneous examination, the same may be made after obtaining order in writing from the CEO/ Head of the ILDC. It is, however very essential that the originator be informed along with its distribution.

5.5 **List of Documents, Checks and Annual Accounting:**

5.5.1 All personnel who are holding classified documents and materials shall check all accountable classified documents and materials, and render certificate of safe custody on 31st December of each year to the next Superior officer. A copy of the certificate will be sent to the CCSO.

5.5.2 Two security inspections and verification shall be carried out, one by the Officer in charge of the section/wing/department/unit and another by the

CCSO during the calendar year. A physical verification of all the classified files and materials shall be carried out during these inspections.

5.5.3 During the checking or inspections, the officers shall recommend destruction of classified papers and materials, wherever required.

5.5.4 A separate Diary and Dispatch book shall be maintained for TOP SECRET and other classified correspondence.

5.5.5 While making cyclostyled copies of SECRET or CONFIDENTIAL documents, a register indicating the number of copies, their copy numbers and to whom issued, would be maintained. The copy shall be made in a controlled environment under supervision.

5.5.6 End of Day Security Checks

a) ILDCs that store classified material shall establish a system of security checks at the close of each working day.

b) ILDCs that operate multiple work shifts shall perform the security checks at the end of the last working shift.

5.6 **Care and Custody of Classified Documents and Equipment /Responsibility of Holders**:

ILDC authorized to store classified documents and equipment shall establish and maintain a system to deter and detect unauthorized intrusion or removal of classified documents and equipment from their facility. Personnel who have a legitimate need to remove or transport classified material should be provided with appropriate authorization for passing through designated entry/exit points.

5.6.1 All categories of classified documents and equipment will be regarded as under the personal charge of the individual to whom the same is issued as recorded and by whom a receipt has been given.

5.6.2 Other Classified Documents and Equipment will be regarded as under the charge of the person to whom the custody of these documents and materials has been entrusted by the Head of the office concerned.

5.6.3 Individuals in charge of Classified Documents and Materials are responsible for their safe custody and their disclosure is limited to only those required to know. The concept of need to know to be followed.

5.6.4 Proper handing /taking over of all documents to be carried out whenever an individual is transferred or superannuating.

5.6.5 In case any employee transferred from one classified section to other section, an undertaking should be obtained from the employee that No information regarding the functional aspects of the section, cases or reference of any cases will be discussed / disclosed by him / her.

5.6.6 The holders of classified documents will carry out periodic checks.

5.6.7 Classified documents will not be studied in the presence of a person who is not entitled to see them or left exposed during the absence of the authorized holder.

5.6.8 When an individual is the sole occupant of a room and during working hours leaves the room for a short period/lunch hour, he must ensure that all TOP SECRET documents are locked in safes or cupboards.

5.6.9 The last two officials/late hour duty officers leaving the office will ensure that almirahs, drawer of tables containing classified documents inside the room / office are properly locked and that no document / paper has been left inside / on table, floor of the room and also in waste paper basket. They will deposit the sealed key to the Caretaker with proper entries.

5.6.10 No single official will open the almirah containing classified document in the office while joining the office in the morning.

5.6.11 The following instructions will always be strictly observed: -

(a) When it is necessary to open a safe, it will be opened for the shortest possible time and locked immediately.

(b) Keys, receptacles containing classified documents will be invariably carried by the person responsible for the receptacle.

(c) Duplicate keys should be kept in a sealed packet which will be in the custody of a nominated officer. A yearly report regarding this should be sent to the CCSO. The duplicate keys will not be withdrawn in normal circumstances and shall be withdrawn with the approval of CCSO only. The keys can be drawn or deposited by an employee who has been authorised to do so by the head of department/officer in charge of the section or office. While authorising employees to draw the keys, it would be ensured that rotation system is followed and casual labourer is not detailed for opening and closing duties. In case of loss of keys the matter shall be reported to the CCSO. Separate duplicate key registers shall be maintained for record.

(d) In case of loss of a key, the matter should be immediately reported to CCSO and concerned lock should be changed. Even if the key is recovered subsequently, it should be regarded as compromised and a fresh lock and key should be issued with proper record.

(e) Keys should, where possible, be passed from hand to hand only. Should it be necessary to transmit a key by post, it will be made up into a package so that the contents cannot be recognized, and will be handled according to the highest category of document contained in the safe.

(f) The company security staff must check employees / staff carrying briefcase, purses at exit/entry to see that no official takes out/in any classified paper without written authority from the Competent Authority.

(g) All almirahs containing classified documents will have a cross marking on it and it shall be written as “to be removed first in case of fire”.

5.7 **Notebooks of PAs:**

5.7.1 Note-books after utilization of PAs should be returned to the officer under whom he works who will keep it in his personal custody and destroy it after the expiry of three months from the date of the last entry in the note book.

5.7.2 The Short-hand note books should remain in the custody of the officer. After typing out the dictation, the PA should return it to the officer. In no case will it be kept in the locker provided to the PA for storing stationery etc.

5.7.3 Any notebook, disc, tape, film, cassette laptop, PCs etc. which has been used to record classified material, should be treated as a classified document and should be kept in the custody of the officer. Classified work done on Laptops, PCs will not be stored in the hard disk or CDs and zip drives etc. If used, these will be handled as per the security classification of data contained therein.

5.8 **Segregation and Care of SECRET Section:** Any branch/ department or sections dealing with classified documents (i.e. Top Secret, Secret, Confidential and Restricted) must segregate its SECRET sections from the non-SECRET sections. There must be adequate provision of steel safes for the custody of classified documents in SECRET sections. Doors of rooms of these sections shall be provided with security locks of proper make and quality in addition to the existing inset locks. Non adherence to this Provision shall be viewed as violation and shall entail punitive action.

5.9 **Security Arrangements for SECRET Section:** The window or the skylight of the SECRET section should be fitted with wire netting or Iron bars and, if it is accessible from outside, it should, in addition, be fitted with strong wire meshing. Lighting arrangements both inside a section dealing with classified documents and in the corridors approaching it, should be adequate.

5.10 **Guarding - Provision for Lighting:** There must be provision of adequate guards both by day and by night to prevent the entry of unauthorized persons. The officer in charge of such a section shall ensure that only authorized persons have legitimate access to his section. If a paper is brought by a person not authorized to enter the SECRET Section, arrangements should be made for such paper being taken into the section without the person concerned being allowed access to the room.

5.11 **Duplicating Work:** Offices or Branches or Sections using Xerox and Photostats Machines etc., shall keep a record of all classified duplicating work done in their respective offices. The supervision of duplicating work will be done in accordance with the following: -

(a) Whenever any TOP SECRET letters or documents are required to be photocopied or cyclostyled, it would be done under the personal supervision of the custodian of the TOP SECRET documents.

(b) Xeroxing a classified document of Top-Secret nature should be facilitated through a requisition slip duly signed by a designated officer by the CEO/ Head of the Company, with proper record maintenance at Reprography section. Similarly, in case of Xeroxing confidential document, requisition slips shall be signed by a senior officer authorized by the CEO/ Head of the Company.

5.12 **Reprographic Equipment:** The reprographic equipment shall be under the personal custody of an officer. It shall be located in his room and he shall be personally responsible for the custody, operation and accounting of the documents reproduced. Any change of the officer or change of location of equipment should immediately be reported to the CCSO, whose personnel shall make periodic checks to verify the system of the accounting. The machine should always be kept under lock, while not in use.

5.13 **Opening and Diarizing of Classified Documents:**

(a)Opening

(i) On receipt of TOP SECRET documents the inner cover will be handed over by the opening personnel to the Officers. All TOP SECRET covers will be opened by the addressee or in his absence by the officer officiating for him.

(ii) SECRET or CONFIDENTIAL documents will be opened either by the addressee or a person so authorised by him.

(b) Diarizing

(i) The diarizing of all TOP SECRET documents shall be carried out either by the officer to whom it is addressed or by his personal staff so authorised by him. The diarizing of SCERET documents may be entrusted to the lower level at the discretion of the concerned officer. The responsibility of the safe custody of the documents will, however, rest with the officer concerned

(ii) The diarizing of CONFIDENTIAL documents may be carried out by selected nominated office staff.

5.14 **Transmission of Classified Documents:**

(a)Preparation of Envelopes:

(i) TOP SECRET, SECRET and CONFIDENTIAL documents will be sent in two envelopes. To assist the recipient in verifying that there has been no tampering in transit, the inner envelope will invariably be a new one. The outer envelope will bear only the address, and will not be marked with the security classification of the contents. The inner envelop will be marked with the appropriate security classification, and if TOP SECRET, it will also be marked "to be opened personally by or officer officiating" (the holder of an appointment or the name of the individual being stated).

(ii) In respect of TOP SECRET and SECRET documents, the dispatcher shall sign the inner cover at two prominent places (e.g. joint-line or the flap), with his name, date and time of dispatch clearly written. The time of dispatch would also be indicated in the dispatch register. The receiver shall scrutinize

such covers carefully to ensure that no undue time has been taken in receipt and shall clearly indicate the time of receipt in the register of the receipts.

(iii) In every case, where single envelope is used, the appropriate classification of the enclosed document will be marked on the envelope, except when restricted documents are dispatched by civil post and they may be sent in single envelope.

(iv) Care will be taken to ensure that envelopes are not of poor quality and are not overloaded. If the documents to be included are likely to be too heavy for an envelope, they shall be made into a parcel, or the envelope will be tied with a string. Cloth-lined envelopes, if available, may be used.

(v) Classified material shall be handled with similar care and attention to record keeping.

(b) Sealing of Envelopes

(i) Inner envelopes of TOP SECRET, SECRET and CONFIDENTIAL documents shall be wax sealed. Special Seals shall be used to seal TOP SECRET documents.

(ii) The closing and sealing of "TOP SECRET" inner covers will be done under the personal supervision of the officers. The inner cover of the top secret documents will be sealed only by top secret seal bearing a number issued by the CCSO. The closing and sealing of SECRET and CONFIDENTIAL inner covers shall be carried out by or under the supervision of Section Officer or Personal Assistant or equivalent.

(iii) All departmental seals issued to different branches/groups/ units must be numbered and a list must be maintained by the issuing authority showing person to whom it has been issued. All such persons will be responsible for the security of these seals.

(iv) In case of any loss of such seal, matter should immediately be reported to the CCSO and authority concern for necessary action on their parts. Besides, other seals of the same series should be treated as compromised. Later, a new series of seal with different shape and design should be issued as early as possible.

(c)Movement of Classified Documents

(i) For movement of classified paper within office, a box, may be of steel or of thick leather / Rexene/ canvas provided it has a proper locking arrangement and cannot be easily cut/pierced/ opened/ tampered, need to be used. Under no circumstances should classified documents be carried loose in the hands of the messengers/ orderlies.

(ii) A messenger carrying secret covers should not leave them unattended at any time till they are delivered.

(iii) Within the Same Block or Building: TOP SECRET files or documents shall be taken only by the officer entrusted to deal with them. In rare cases, if a document is to be conveyed through another Officer authorized to handle the document, it shall be put in a single sealed envelope and then carried. SECRET files or documents shall be taken by hand by a person authorised

by CEO/ Head of ILDC. CONFIDENTIAL files or documents may be transmitted through any member of the staff entrusted to deal with it.

(iv) Movement of Classified Documents Within the Same Station: Movement of TOP SECRET documents between one block to another within the station, shall be through an authorized courier and not through peons or registry. If the carriage involves movement in public area Journey shall be undertaken only in an authorized transport. Wherever feasible, a second person shall also be nominated to accompany the courier.

(v) The responsibility of the safe custody and handling of the TOP SECRET document will be that of the recipient officer.

(vi) SECRET or CONFIDENTIAL: Officers may carry classified documents, other than TOP SECRET in locked brief cases. In case, brief cases are not available, these may be carried in a single sealed envelope. The documents too bulky to be carried in a brief case may be carried in locked and sealed canvas bag or boxes by messengers accompanying the officers.

(vii) If employees (other than officers) are required to carry classified mail, it shall be carried in a locked box or bag, the operating key of which shall be with the originator and the duplicate with the addressee. In the event of more number of addressees, a special box with multiple keys will be used, one key of which shall be with the originator and the rest (one each) with individual addressees. Such keys will not be handed over to the person carrying the box.

(viii) All classified mail inside the Mail Box or Bag shall be kept in a sealed cover. While doing so, it will be ensured that classification of the letter is not mentioned on the outer cover.

(ix) Section / Unit Officers must ensure that no mail is left undelivered with the person carrying them particularly on Fridays or on days preceding closed holidays.

(x) Similar care shall be taken in the movement of classified equipment.

(d) Carrying Classified Documents or Equipment to Residence or Outside Office: Carrying of classified documents and equipment to residence of officers is prohibited. All Top Secret papers should be dealt with in office only.

(i) Officers are generally prohibited to carry any Top Secret paper to their residence. When it is necessary to send a Top Secret paper to CEO/ authorized senior officer at his residence after office hours, the dispatching officer should obtain his specific instructions that it may be sent to his residence and that he would be ready to receive the document at his residence.

(ii) The dispatching officer must ensure that the box in which Top Secret document is sent, is locked and fastened to the vehicle in which the messenger is carrying it.

(iii) When an officer having authority to do so carries any Top secret document to his residence, he must take the documents only in securely locked bag/box, the key of which must be in his possession. The bag/box must be kept all along in his personal custody till he reaches his residence where

also this must be placed in a secure place to which no outsider may have access.

(iv) Whenever an officer requires a Top Secret document for meetings /discussions, etc. either at the place of his posting or at a place other than the place of posting and Top Secret documents have to be taken out of the office, the following procedure shall be followed:

Only Officers authorized by CEO/ Head of the Company will be permitted in special circumstances for taking top secret documents out of the building to facilitate official meetings with explicit approval of CEO / Head of the Company.

(e) Transmission of Classified Documents to Outstations within India: Classified documents will be dispatched through civil postal service subject to the under mentioned instructions:-

(i) TOP SECRET. TOP SECRET documents will only be sent by special couriers. In no circumstances will they be transmitted by civil post. TOP SECRET mail, however, will not be dispatched by "AIR DESPATCH SERVICE." unless accompanied by special couriers.

(ii) SECRET or CONFIDENTIAL. Documents can be sent by Registered Civil Post and marked "Registered AD" post on the outer envelope of documents.

(iii) RESTRICTED. Document may be sent by civil post, and it is left to the discretion of the originator to decide whether or not registration is necessary.

(f) Transmission of Classified Documents to Foreign Countries: Transmission of classified documents is prohibited in any form, either electronic/ fax or otherwise, to any foreign country.

(g) Circulation and Carriage of Documents/Papers Containing Sensitive Information for Official Interdepartmental and Other Meetings. Utmost care will be taken to ensure security of classified information required to be circulated for Inter-departmental and Other Meetings. Following additional precautions will be taken: -

(i) Need to know principle will be strictly applied while circulating sensitive information.

(ii) No extra copies of papers etc. will be prepared.

(iii) Security classification commensurate with the contents will be assigned to the papers/documents required to be circulated.

(iv) The papers/documents if required to be sent in advance will be sent by name and acknowledgement/receipt obtained. The document/ paper will be handed over to the addressee and not their personal staff.

(v) The paper/documents should be retrieved by concerned office after the meetings and accounted for.

(vi) Only authorized officers will carry such papers/documents for the meeting. These documents will not be carried to residence except where permitted.

5.15 **Emergency Procedures**: ILDCs shall develop procedures for safeguarding classified equipment in emergency situations. The procedures shall be as simple and practical as possible and should be adaptable to any type of emergency that may reasonably arise. ILDCs shall promptly report to the designated agency any emergency situation that renders the facility incapable of safeguarding classified equipment.

5.16 **Disclosure:**

5.16.1 General: ILDCs shall ensure that classified information is disclosed only to authorized persons.

5.16.2 Disclosure to Employees**:** ILDCs are authorized to disclose classified information to their authorized employees as necessary for the performance of tasks or services essential to the fulfilment of a classified contract or subcontract.

5.16.3 Disclosure to Subcontractors/ other persons/other ILDCs: ILDCs are authorized to disclose classified information to a subcontractor when access is necessary for the performance of tasks or services essential to the fulfilment of a prime contract or a subcontract. Prior authorization shall be obtained by the ILDC in writing from the Government Agency having classification jurisdiction over the information involved for this purpose.

5.16.4 Disclosure between Parent and Subsidiaries: Disclosure of classified information between a parent and its subsidiaries, or between subsidiaries, shall be accomplished in the same manner as prescribed in 5.16.3 for subcontractors.

5.16.5 Disclosure in an MFO: Disclosure of classified information between facilities of the MFO shall be accomplished in the same manner as prescribed in 5.16.2 for employees.

5.16.6 Disclosure of Classified Information in Connection with Litigation: ILDCs shall not disclose classified information to a legal advisor or consultant or representative or any other person acting in a legal capacity unless the disclosure is specifically authorized by the agency that has jurisdiction over the information. ILDCs shall not disclose classified information to any court except on specific instructions of the agency which has jurisdiction over the information.

5.16.7 Disclosure to the Public: ILDCs shall not disclose classified or unclassified information pertaining to a classified contract to the public without prior review and clearance as specified in the Contract Security Classification Specification for the contract or as otherwise specified by the approving authority.

5.16.8 Non-disclosure agreement: Non-disclosure agreement may be put in place before sharing information with any outside agency.

5.17 **Down Grading, Disposal and Destruction of Classified Documents and Equipment:**

5.17.1 All organizations, departments, sections will carry out periodic destruction of documents (once in a year) to prevent their accumulation and consequent problems of accounting and security. Screening of documents for destruction should be done by a Board of Officers and the proceedings of such Board of should be approved by the Department Head prior to the destruction of the documents

5.17.2 Downgrading or Declassifying Classified Information. Information is downgraded or declassified based on the loss of sensitivity of the information due to the passage of time or on occurrence of a specific event. ILDCs downgrade or declassify information based on the guidance provided in a Contract Security Classification Specification or upon formal notification/ authorization.

5.17.2.1 An Officer will have no authority to downgrade / upgrade the security classification of a document received from other department without the concurrence of the originator.

5.17.3. Upgrading Action: When a notice is received to upgrade equipment to a higher level, the new markings shall be immediately entered on the equipment according to the notice to upgrade, and all the superseded markings shall be obliterated. The authority for and the date of the upgrading action shall be entered on the equipment.

5.17.4 Disposal: Classified documents will be examined from time to time with a view to reducing the number of such documents held. Accountable documents, if no longer required by holder, will be returned to the issuing authorities.

5.17.5 Destruction: TOP SECRET, SECRET or accountable CONFIDENTIAL documents will be shredded to small size without being able to be reconstituted and shall be destroyed by burning and a proper record be maintained under the supervision of authorised officer. Documents other than classified may be destroyed at the discretion of the head of the office concerned.

5.17.6 Other points on destruction:

a) Record of daily destruction of classified waste, indicating individual detailed for supervision and the time and place shall be maintained by the Sections, in order to pin point the responsibility in case of breach of security.
b) In no circumstances shall waste paper, drafts, spoiled forms, used carbon papers, unnecessary duplicates, stencils, blotting paper, impression of official seals and stamps relating to or used in connection with classified document be allowed to fall into the hands of unauthorized persons.

5.17.7 Record Rooms Following instructions will be applicable for security of classified documents stored in the record rooms: -

a) Isolated room shall be used for storing classified documents and equipment. They will not be kept in the room where other non-classified documents are stored and kept.

b) Proper fire-fighting arrangements will be made to deal with outbreak of fire, suitable fireproof cupboards shall be made use of for storage of TOP SECRET, SECRET and CONFIDENTIAL documents.

c) Records/files/documents from Record Rooms will only be issued on a requisition, stating the purpose and duration for which the records are needed. The requisition should be signed by an officer. A record of the documents issued will be kept in a register.

d) Data regarding employees engaged in sensitive projects or given responsibility to handle sensitive information /materials /documents should be retained permanently by the ILDCs.

CHAPTER – 6 - Communication Security

6.1 General:

All communications are vulnerable to interception. Security of Communication is, therefore of paramount importance in an organization.

6.2 Telephones:

6.2.1 No form of telephonic conversation, including intercom PAX and hot lines, is secure. Every care has to be taken to prevent inadvertent leakage of classified information by discussing classified matters over the telephone. Following precautions shall be observed: -

(a) TOP SECRET, SECRET and CONFIDENTIAL information should not be passed or discussed on telephone.

(b) Before answering the phone or passing any official information on telephone, the person receiving the call should identify the caller beyond any reasonable doubt. In case of doubt, caller should be asked to give telephone no. and identity, which should be checked with the directory before calling back the caller.

(c) The management should carry out periodical sensitisation w.r.t Social Media Usage, Cyber best practices and handling calls/manning Exchange.

(d) Any attempt by the caller/ adversary to impersonate as government official seeking sensitive information should be blocked and officials should be wary of such calls from calls. Specifically, to prevent leaking of information through such calls, following procedure should be followed: -

(i) Do not provide any information without establishing the identity of the caller.

(ii) Take down the caller's contact number and seek time to revert back.

(iii) If any suspicion arises during the call, cancel the call.

(iv) Do not disclose any sensitive information over phone to anyone.

(v) Don't be tricked into giving away confidential information.

(vi) If any email is received from an operative of unfriendly countries, forward that email to CERT-IN for further necessary action.

(vii) If the email attachment is opened by the user, immediately disconnect that PC from network and scan the network for the presence of malware.

(viii) Any such calls or email shall be report to the CISO immediately

(e) To prevent misuse, telephones should be kept locked when the officer is away from his office.

(f) Cordless phones will not be used.

(g) If it comes to notice that an intruder has come on the line and some information has come to the knowledge of the listener, the same should be brought to the notice of senior officers and CCSO so that remedial measures can be taken.

(h) A thorough physical check of the PABX phones or instruments or boxes should be made periodically by the office of CCSO to ensure that these are not tampered with.
(i) All vulnerable points in the intercom system should be protected by wooden or metallic boxes with locking arrangement.
(j) Telephone conversation is totally unsafe; thus, if at all classified information has to be passed on phone, proper secrecy device should be used.
(k) All telephones should be provided with a caller ID facility.
(l) Only authorized person be nominated for maintenance of PAX / outdoor plant, furthermore records of same be maintained.

6.3 **Cell or Mobile Phones / Data Cards / Voice Modems:**

6.3.1 Cellular or Mobile Phone / Data Cards / Voice Modems are highly insecure medium for communication purposes, since it works on UHF and VHF and is prone to interception by Frequency Modulation receivers. These gadgets can also be used as effective, unobtrusive listening devices for eavesdropping. Technology now exists where the eavesdropping function can be carried out even with they are in switched off mode and can be used to shoot and transmit still pictures or live videos. Therefore, cellular or mobile phones / Data Cards / Voice Modems including WLL phones are potent sources of breach of security of information. Also, no technology or device exists which can be fitted on them to make it interception proof.

6.3.2 GSM Monitoring system is a commercial off the shelf (COTS) equipment and is being manufactured by a large number of original equipment manufacturers (OEMs) across the world. Available equipment enables monitoring of Communication from briefcase sized equipment. A number of Indian vendors are marketing GSM monitoring systems. Due to their small size and portability, there is threat that inimical agencies may selectively employ such means/gadgets for interception of cellular communication from high density areas/ specific areas of activity.

6.3.3 The use of Cell phone shall be banned in areas/offices wherein classified work is in progress/documents are being worked upon. On special cases permission to carry mobile phones by critical staff, in these areas shall be recommended by the Head of department and granted by CCSO. Mobile phones are not permitted inside conference halls, operations rooms, at official briefings and at sensitive places even in off mode. This instruction is applicable to even those who have been permitted. Mobile phone with camera and other technical advance features including internet, GSM, etc should not be allowed irrespective of ranks inside the office premises. No visitors will be permitted to carry mobiles inside the facility, the mobiles of visitors is to be deposited at the reception.

6.4 **FAX communications:**

FAX communications are also vulnerable to interception or leakage, e.g. a cross-connection. It is, therefore, necessary to identify the end party before transmitting a message. Papers which are not of classified or sensitive nature may be transmitted with the help of FAX in emergent cases. Under no circumstances such an option is exercised for transmitting classified documents. No classified message should be passed or received on Fax on auto mode.

6.4.1 While using Fax machines a record of the documents or papers faxed or received will be kept in a register. The record will include the following details: -

a) Time of Fax sent or received.
b) Title of document.
c) Number of pages
d) Sent to or received from.
e) Designation of Officers or office where Fax is sent.
f) Officer authorized to dispatch the Fax.
g) No “Top Secret” message should be transmitted on FAX.

CHAPTER – 7 - Computer and Cyber Security (Information Systems Security)

7.1 General:

7.1.1 Information systems (IS) that are used to capture, create, store, process or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information, loss of data and integrity to ensure the availability of the data and system.

7.1.2 The organization must, at all times, be in strict compliance with the IT Act 2000, as amended in 2008 and as amended from time to time.

7.1.3 Protection requires a balanced approach in IS security features to include, but not limited to, administrative, operational, physical, computer, communications and personal controls. Protective measures commensurate with the classification of information, the threat and the operational requirement associated with environment of IS.

7.1.4 ILDC management should appoint / nominate Cyber Information Security Officer clearly defined with roles and responsibilities to carry out activities like development, implementation and evaluation of the facility IS program. To publish and promulgate IS security policy and procedures to address classified processing environment.

7.1.5 Threats to Computers security could emanate from internal sources such as subverted/disgruntled employees, as well from external sources such as the vendors of the Hardware/ Software, outsider maintenance staff or from intruders/hackers in the Cyber Space and hostile foreign countries /inimical agencies. Threats can manifest as Structured (automated methods of information gathering and attack - organised, determined and goal centric) or unstructured (network loitering, manual information gathering or attack and misuse by accident). Some of the Computer vulnerabilities that exist are as follows: -

(a) Physical theft of Hard disks, Computer Storage Media, Keyboards with memory facility, used Printer Cartridges, Laptops etc.
(b) Stealing /compromising data /information by remote access.
(c) Susceptibility to Ransomware and Denial of Service Attacks
(d) Susceptibility to Phishing, Smishing and Vishing Attacks
(e) Accidental/Intentional cross connection between the Organization Local Area Network and Internet.
(f) Spoofing by intruders.
(g) Defacing of various Websites by anonymous Hackers.

7.1.6 In addition to above, any advisory issued by the Government from time to time shall be strictly complied with.

7.2 **ISO 27001:**

7.2.1 The companies shall follow guidelines under ISO 27001. Appropriate controls shall be implemented to accommodate the guidelines given in this manual.

7.2.2 This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS).

7.2.3 This International Standard adopts a process approach for establishing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS.

7.2.4 The process approach for information security management presented in this International Standard encourages its users to emphasize the importance of:

(i) Understanding an organization's information security requirements and the need to establish policy and objectives for information security;
(ii) Implementing and operating controls (administrative, technical and physical) to manage an organization's information security risks in the context of the organization's overall business risks;
(iii) Monitoring and reviewing the performance and effectiveness of the ISMS; and
(iv) Continual improvement based on objective measurement.

7.2.5 This International standard adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure all ISMS processes. PDCA provides a structured approach for organizations to achieve continual improvement.

7.2.6 Norms of ISO 27001 is the comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements. The compliance process subjects the system to appropriate verification that protection measures have been correctly implemented. The internal system shall review that all systems have the appropriate protection measures in place and validate that they provide the protection intended.

7.3 **Common Requirements:**

The information security policy should take into account the information systems deployed by the organization as well as by any sub-contractors, where such systems may have an impact of the confidentiality, integrity or availability of systems / data. This policy should be made based on a realistic vulnerability / threat and risk assessment by qualified information security experts. The policy must have sign off from the senior most management of the organisation. If the organization also holds Critical Information Infrastructure, the Policy must be made in consultation with NCIIPC. The policy must cover all information devices and, inter alia, include Implementation of Security Controls as released by NCIIPC / CERT-In e.g.

(a) Hardware / software inventory and controls

(b) Protection against malware

(c) User and Password management including for all users handling critical / sensitive information including sub contractors.

(d) Revocation of privileges subsequent to termination of employees / contracts

(e) Safe and verified backup and restoration mechanisms. These must be tested on a regular basis.

(f) Configuration rules of Firewall, IDS/IPS, UTM, EDR/UEBA, SIEM/SOAR

(g) Industry 4.0 policy for safety of Cyber Physical and SCADA/ICS Systems.

(h) Disaster Recovery policy with focus on data security while assuring business continuity.

(i) (a) Restrict privileged accounts on the system to only those organisation-identities personnel who require this access compulsorily to carry out their allotted tasks which require access to controlled defence information

(b) Require that users (or roles) with privileged accounts use non-privileged accounts when accessing functions or information not related to allotted tasks which require access to controlled defence information

(j) (a) Prevent non-privileged users from executing privileged functions.

(b) Log the execution of privileges functions.

(k) Unsuccessful Logon Attempts:

Limit the number of consecutive invalid logon attempts to an organisation-defined number and an organisation-defence time period.

(l) System use notification:

Display a system use notification message with privacy and security notices consistent with applicable controlled defence information handling and processing rules before granting access to the system.

(m) Device Lock:

(a) Prevent access to the systems by the following methods –

(i) Initiating a device lock after organisation-defined period of inactivity

(ii) Requiring the user to initiate a device lock before leaving the system unattended

(iii) Retain the device lock until the user re-establishes access using established identification and authorisation procedures.

(iv) Conceal, via the device lock, information previously visible on the display with publicly viewable image.

7.3.1 Having implemented adequate measures to secure their information infrastructure, the CISO should also ensure that compensating controls and residual risk are enumerated and sign off obtained from management.

Review and Evaluation of Cyber Security Policy

Cyber Security Policy of the Organisation shall be reviewed at least annually and updated in response to any changes that would affect the assumptions from the baseline risk assessment, such as significant security incidents, new vulnerabilities, new regulations or changes to the Organization's infrastructure.

The review shall include an assessment of the policy's effectiveness based upon:

-

(a) The nature and number and impact of recorded security incidents.

(b) Cost and impact of controls on business efficiency.

(c) Effects of changes to technology.

7.3.2 Some common Requirements are:

a) General User and Privileged users, their roles, responsibility and accountability should be clearly defined
b) Require that each IS privilege / general user sign an acknowledgement of responsibility to adhere to Information security guidelines.
c) Profiling of Information assets based on sensitivity of information by the Level of Concern for Confidentiality (C), System Availability (A) and Data integrity (I).The level of concern reflects the sensitivity of the information and the consequences of the loss of confidentiality, integrity or availability (CIA). Based on these matrices, need for protection levels and profiles in the form of security, audit, redundancy in the infrastructure, backup etc., shall be determined.
d) Procedures should be defined about unique identification of user, user id removal on termination, transfer; change in roles etc., re-use of user id and user id revalidation for the use of any centralised IS resource.
e) To maintain the CIA, control and audit logging mechanism along with monitoring system should be in place, for changes to data includes deterring, detecting and reporting of successful and unsuccessful attempts to change etc.Such monitoring system can be implemented by deploying solutions like Security incident and Event Management (SIEM), Security Orchestration Automation and Response (SOAR) and User and Entity Behaviours Analytics (UEBA).
f) Use of next generation technologies like Zero Trust Architecture will help in attack surface reduction. Also for granular level control Identity and Access Management (IAM) solutions are recommended.
g) Control and audit logs should be available in centralised systems/applications for Successive Logon Attempts, Multiple Logon Control, Session termination and User Inactivity etc. The logs retention period must be for a period of minimum 180 days.

h) Security should be ensured for inter connectivity of multiple LANs, when organisation has multiple Units/Offices across the geographical location, where interconnectivity may be WAN (Wide Area Network) using public networks.

i) When Public networks are used proven, secured WAN technologies should be used along with appropriate security at the gateway and suitable encryption during transmission.

j) Proper system should be in place to track, inventories, to carry out OS patches, IOS/Firmware updates and Configuration Management of information Systems.

k) All Internet facing Web sites /Applications, necessary protections at Network Layer and Application, like security during transmission, Application Security and Database security should be in place by using appropriate security components / measures. In addition, all these public facing applications and portal should be protected using Content Delivery Network (CDN) and Web Application Firewall (WAF). Also Single Sign On (SSO) with Multi Factor Authentication (MFA) must be enforced on all portals.

l) The Number of Internet Connections shall be controlled by CEO/ Head of Company as per the company policy.

m) Centralised Anti-Virus management solution should be in place for effective implementation of Anti-Virus solution.

n) System should be in place for internal incident management as well as for implementation of time to time necessary guidelines / measures from Computer Emergency Response Team – India (CERT-India)/ National Critical Information Infrastructure Protection Centre (NCIIPC); and should be able to detect any violations to existing policies and ensure updating IT infrastructure.

o) Phishing Attacks can be prevented by using Multi Factor Authentication (MFA). The MFA must be combined with anti-phishing technologies. These anti-phishing technologies encompass traditional methods such as Sender Policy Framework (SPF), Doman Keys Identified Mall (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC), alongside newer advancements like Authenticated Received Chain (ARC), Verified Mark Certificates (VMC), and Brand Indicators for Message Identification (BIMI) that collectively contribute to a comprehensive phishing prevention strategy.

p) Develop and maintain a current baseline configuration of the system. Review and update the baseline configuration of the system periodically and when system components are installed and modified.

q) In addition to above, some of the other guidelines which ILDCs need to follow are as follows -

(I) <u>Common Requirements:</u>

Types of cyber security incidents mandatorily to be reported to CERT-In.

(i) Targeted scanning/ probing of critical networks/systems.
(ii) Compromise of critical systems/ information.
(iii) Unauthorised access of IT systems/ data
(iv) Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
(v) Malicious code attacks such as spreading of Virus/Worm/Trojan/Bots/Spyware/Ransomware/Cryptominers.
(vi) Attack on servers such as Database, Mail, DNS and Network devices such as Routers.
(vii) Identity theft, spoofing and phishing attacks.
(viii) Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
(ix) Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks.
(x) Attacks on Application such as E-Governance, E-Commerce etc.
(xi) Data Breach.
(xii) Data Leak.
(xiii) Attacks on Internet of Things (loT) devices and associated systems, networks, software, servers.
(xiv) Attacks or incident affecting Digital Payment systems.
(xv) Attacks through Malicious mobile Apps.
(xvi) Fake mobile Apps
(xvii) Unauthorised access to social media accounts.
(xviii) Attacks or malicious/ suspicious activities affecting Cloud computing systems/ servers/software/applications.
(xix) Attacks or malicious/suspicious activities affecting systems/ servers/networks/ software/ applications related to Big Data, Blockchain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones.
(xx) Attacks or malicious/suspicious activities affecting systems/servers/software/ applications related to Artificial Intelligence and Machine Learning.

(II) Configuration settings:

(a) Establish document and implement the configuration settings for the system that reflect the most restrictive mode consistent with operational requirements. These configuration settings must be organisation-defined consistent with overarching requirement to protect, controlled defence information.
(b) Identify document and approve any deviations from the establish configuration settings. Such deviations must be granted only as an exception after due deliberation be a collegiate.

(III) Configuration change control:

(a) Define the type of changes to the system that are configuration-controlled.
(b) Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security impacts.
(c) Implement and document approved configuration-controlled changes to the system.

(IV) Impact Analyses

Analyse the security impact of changes to the system prior to the implementation.

(V) Access Restrictions for Change

Define, document, approve and enforce physical and logical restrictions associated with changes to the system.

(VI) Least functionality

(a) Configure the system to provide only mission-essential capabilities.
(b) Prohibit or restrict use of the organisation-defined functions, ports, protocols, connections and services.
(c) Review the system periodically to identify unnecessary or non-secure functions, ports, protocol, connections and services.
(d) Disable or remove functions, port, protocols, connections and services that are unnecessary or non-secure.

(VII) Incident Response Plan and Handling

(a) Develop an incident response plan that provides the organisation with a roadmap for implementing its incident response capability
(b) Implement an incident-handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication and recovery processes and procedures.
(c) Update the incident response plan to address system and organisational changes or problems encountered during plan implementation, execution or testing phases.

(VIII) Incident Monitoring, Reporting and Response Assistance

(a) Track and document system security incidents.
(b) Report suspected incidents to the organisational incident response capability within an organisation-defined time period.
(c) Report incident information to CERT-In/NCIIPC as per timelines promulgated by these entities from time to time.

(d) Provide an incident response support resource that offers advice and assistance to users of the systems for the handling and reporting of incidents.

(IX) Incident Response Testing

Test the effectiveness of the incident response capability periodically.

(X) Incident Response Testing

(a) Provide incident response training to system users consistent with assigned roles and responsibilities:
   (i) Within an organisation-defined time-period of assuming an incident response role or responsibility and following occurrence of organisation-defined events.

(XI) Personnel Screening

a) Screen individuals prior to the authorising access to the system.
b) Rescreen individuals in accordance with organisation-defined conditions

(XII) Personnel Termination and Transfer

a) When individual employment is terminated –
   (i) Disable system access within the shortest timeframe which is organisation-defined
   (ii) Terminate or revoke authenticators and credentials associated with the individual.
   (iii) Retrieve security-related system property from the terminated individual.
b) When individual is reassigned or transferred to other positions in the organisations –
   (i) Review and confirm the ongoing operational need for current logical and physical access authorisation to the system and facility.
   (ii) Initiate information security-related transfer or reassignment actions within shortest timeframe that is organisation-defined.
   (iii) Modify access authorisation to correspond with any changes in operational need.

7.4 Enterprise Resource Planning (ERP):

Enterprise Resource Planning (ERP) may be implemented as system integrates internal and external management information across the entire organization, tracking of all processes, materials and personnel in the plant. ERP systems automate this activity with an integrated software application. The purpose of ERP is to facilitate the flow of information between all business functions inside the boundaries of the organization and manage the connections to outside stakeholders. There should be

exhaustive guidelines, operating procedures issued for all aspects of plant functioning. Ownership of all processes and inventory held should be clearly defined with standby ownership.

7.5 **Physical and Software Security:**

7.5.1 Unless the physical security of a computer system is ensured, any attempt to protect its operations and data will be futile. Physical security and safeguard of hardware from damage, theft and unauthorized access and software and data from intentional, accidental or environmental corruption must be ensured at all costs.

7.5.2 Safeguarding the computer storage media, software, sensitive and proprietary data by:-

(i) Safekeeping of computer storage media, (CDs, magnetic tapes, hard disk, USB drives etc).
(ii) Shredding or secure disposal of console logs or printouts, used printer ribbons & carbons, damaged tapes and hard disks etc.
(iii) Protection of Switches/Routers and other connectivity devices.

7.5.3 Network racks should be situated away from easily accessible public spaces like the pantry, cafeteria, restrooms, waiting rooms, hallways etc. Also these devices should be properly locked and must be under continuous surveillance using cameras.

7.5.4 Adequate protection is required both for the operating system software and application software. In order to prevent unauthorized access to the data, passwords should be assigned at multiple levels i.e. first at the time of making the system operational, second at the time of logging with the authorized user's name, third at the time of running application software and so on, depending upon the type of data being handled. It is very essential that there should be a provision of 'Audit Trail' features to know which user had logged in and at what time.

a) Develop, approve and maintain a list of individuals with authorisation access to the physical location where the system resides.
b) Issue authorisation credentials for physical access.
c) Review the physical access list periodically.

7.5.5 Review individuals from the physical access list when access is no longer required.

7.5.6 Access Control for Mobile Devices.

(a) Prevent access to the system by the following methods –
(i) Initiating a device lock after organisation-defined period of inactivity.
(ii) Requiring the user to initiate a device lock before leaving the system unattended.
(b) Retain the device lock until the user re-establishes access using established identification and authorisation procedures.

(c) Conceal, via the device lock, information previously visible on the display with publicly viewable image.

7.5.7 Remote Access

(a) Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.
(b) Authorise each type of remote system access prior to establishing such connections.
(c) Route remote access to the system through authorised and managed access control points.

7.5.8 Authorise remote execution of privileged commands and remote access to security-relevant information.

1. Monitoring Physical Access
   a) Monitor physical access to the location where the system resides to detect and respond to physical security incidents
   b) Review physical access logs periodically.
2. Alternative Work Site
   a) Determine alternate work sites allowed for use by employees.
   b) Employ adequate physical requirements at alternate work sites at par with those employed at main work site.

3. Physical Access Control
   a) Control physical access at the location where the system resides by –
      i. Verifying individual physical access authorisations before granting access.
      ii. Controlling ingress and egress with physical access control systems/devices or guards.
   b) Maintain physical access audit logs for entry or exit points.
   c) Escort visitors and control visitor activity.
   d) Install secure keys, combinations and other physical access devices.
4. AccessControl for Transmission and Output Devices.
   a) Control physical access to system distribution and transmission lines in organizational facilities. Control physical access to output devices to prevent unauthorized individual from obtaining access to controlled defence information.
5. Boundary Protection.
   a) Monitor and control communication at the external managed interfaces to the system and at key internal managed interfaces within the system.
   b) Implement subnet works for publicly accessible system components that are physically or logically separated from internal networks.
   c) Connect to external systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

7.6 Acquisition of Computer hardware and Software

7.6.1 Computer hardware, which is proposed to be procured, should be of an open system or architecture and the user should be free to go in for 'Annual Maintenance Contract' with any party. The systems being procured should be the latest ones which can be upgraded at a later date.

7.6.2 If development of software application is outsourced, antecedents of the personnel/company developing the software should be verified. Where necessary, Non-Disclosure Agreements (NDA's) must be signed by the Contractor / sub-contractors. Further, for critical applications the vendor should be asked to provide source code for the application developed by him. Whenever feasible, dummy data should be used for testing the applications. This would prevent the vendor from accessing sensitive information.

7.6.3 The firms, which are offering AMCs, should be on boarded upon signing NDA and should be positively vetted by CISO (with help from Agencies of MHA/ Cyber Crime Cell of local police / MoD/ if so required) before they are allowed to take up Software & Hardware maintenance work. In case the same is not possible, an audit of the firm from security point of view should be carried out. While awarding contract for maintenance it should be ensured that too many engineers from the maintenance company are not allowed to work on the systems. It should also be ensured that when the service engineer undertakes the maintenance or repair job, a knowledgeable representative of the user invariably remains present throughout and ensures that no data or information from the computer is downloaded and taken out by the service engineer. Positive vetting of the firms offering AMCs will be as per the guidelines and processes issued by the Government from time to time.

7.6.4 The outsider maintenance Engineer should not be allowed to install his own keyboards and other accessories as an interim measure till repaired part is returned, as his accessory may have data capturing tools like key logger. When his accessory is taken back, it may have valuable data captured from the computer.

7.6.5 While installing the operating System, only the utilities /components required by the user should be installed/ enabled. Some of the utilities listed below which are enabled by default with the bundled software must either be disabled or configured on need basis.

a) Default Password.
b) Sample networking programme.
c) Files sharing tools.
d) Ports enabled by default.
e) Check for presence of any key logger software installed in any PC.
f) Where required CC EAL certification (Common Criteria-Evaluation Assurance Level) based on the protection profile required by the ILDC must be provided by the vendor.

g) Certain windows feature like Power Shell Script, Windows Management Instrumentation (WMI) code (WMIC), process dumps can be exploited by a threat actor for malicious purpose. It is suggested that same must be disabled and may be enabled as and when need arises and disabled again. Behaviour based detection rules should be implemented for the same.

7.7 Miscellaneous Aspects:

7.7.1 Each ILDC should formulate a clearly defined Cyber Security Policy, based on which a third party cyber security audit shall be conducted. This auditor shall be selected by the ILDC from the list of certified Cyber Security Auditors as published by Computer Emergency Response Team – India) CERT-In, on their web site.

i) The risk to secrecy of data due to the human factor should also not be underestimated. The following measures should be adopted in this regard: -

a) Adequate separation of duties and restriction of access in every office so that no single person can individually compromise the entire system or data.
b) Triennial character and antecedents verification of critically placed functionaries of the computer system handling sensitive information by CCSO through civil police.
c) Cyber Awareness and Evaluation Module should be an integral component of employee induction training. Also on a periodic basis, recurring cyber security awareness training and evaluation sessions must be conducted to keep all employees informed and vigilant regarding cyber security matters.
d) In-house sensitization and periodical briefing of concerned personnel of various departments regarding computer security.
e) Inclusion of talks on computer security in the training programmes on Departmental Security.
f) During the periodic security checks of the department, special emphasis should be laid on computer system security and any loopholes therein.
g) In case of annual maintenance contracts awarded to the vendor, the antecedents of their personnel providing service should at least be verified from the civil police.
h) All probationers of cyber security applied to the principle ILDC must equally carry forward to all contractors / sub-contractors employed in the project and they may also sign non disclosure agreement.
i) The passwords/credentials of various applications must never be stored on devices (like in browsers/test files etc). Also access credentials should never be pasted / written on advice**.**
j) The IT Employees must be sensitized that sensitive information like IP Ranges; Passwords and Usernames etc must never be maintained in Personal Diaries.

k) Air-Gapped Systems should not be used for accessing Internet using Mobile Hotspots/USB Dongles.

l) Information in Shared System Resources prevent unauthorised and unintended information transfer via shared system resources.

m) Network communication – Deny by Default – Allow by Exception. Deny network communication traffic by default and allow network communication traffic by exception.

n) Transmission and Storage Confidentiality Implement cryptographic mechanism to prevent the unauthorised disclosure of controlled defence information during transmission and while in storage.

o) Network Disconnection
Terminate network connections associated with communications sessions at the end of the sessions or after period inactivity.

p) Cryptographic Key Establishment and Management.
Establish and manage cryptographic keys in the system in accordance with organisation-defined key establishment and management requirements.

q) Cryptographic Protection
Implement robust cryptography mechanism to protect the confidentiality of controlled defence information.

r) Collaborative Computing Devices and Applications
Prohibit remote activation of collaborative computing devices and applications. Provide and explicit indication of use to users physically present at the devices.

s) Supply Chain Risk Management Plan
Develop a plan for managing supply risks associated with the research, development, design, manufacturing, acquisition, delivery, integration, operations, maintenance and disposal of the system, system components or system devices which are related to or store or harness-controlled defence information. Review and update the supply chain risk management plan periodically. Protect the supply chain risk management plan for unauthorised disclosure.

t) Acquisition Strategies, Tools and Methods.
Develop and implement acquisition strategies, contract, tools and procurement methods to identify, protect against and mitigate supply chain risks

u) The Software must be developed and build in secure environments. Those environments must be secured by the following actions, at a minimum –
Separating and protecting each environment involved in developing and building software. Regularly logging, monitoring and auditing trust relationships used for authorisation and access to any software development and build environments among components within each environment.

v) Enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software in a manner that minimises security risk.

w) Taking consistent and reasonable steps to document, as well as minimise use of inclusion of software products that create undue risk within the environments used to develop and build software.

x) Encrypting sensitive data, such as credentials, to the extent practicable and based on risk. Implementing defensive cyber security practices, including continuous monitoring of operations and alerts and, as necessary, responding to suspected and confirmed cyber incidents.

y) The software developer must make all efforts to maintain trusted source code supply chain by employing automated tools or comparable processes to address the security of internal code and third party components and manage related vulnerabilities as available from time-to-time. Use of trusted software/hardware components in facility handling/developing sensitive technology is mandatory

z) The software developer must maintain provenance for internal code and third party components incorporated into the software as Software Bill of Material (SBOM) and supply the same to BUYER at the time of delivery of the software as well as each software update.

aa) The software developer must employ automated tools or comparable processes that check for security vulnerabilities.

7.7.2 Cataloguing of CDs/ External / Portable Hard Drive: The CDs (RW), Cartridge Tapes, External/Portable Hard Drives used should be serially numbered with name of the concerned written in indelible ink. A register should be maintained for taking it on charge and destroying those that become unserviceable, and periodical checks should be carried out. Supply of blank storage medium for use of the PC holders will be made only against written requisition duly signed, or countersigned, by an officer.

7.7.3 External / Portable Hard Drive: Use of External / Portable Hard Drive within Classified Zone/areas is not permitted. Only in rare and exceptional cases, officers, for whom specific permission has been granted by CCSO, can use External / Portable Hard Drive within the classified zones/areas. External / Portable Hard Drives will be issued only to such individuals who possess the permission by name and it will be in their personal charge. Procurement of External / Portable Hard Drive will be done centrally by the CCSO with written approval of the CEO/Chairman/CMD, who may delegate the powers to the Unit Head for issuing written approvals. However, the responsibility and accountability of the same shall still rest with the CEO. All instructions relating to classified documents contained in this Manual are equally applicable to External / Portable Hard Drives. Carriage of External / Portable Hard Drive inside/outside the office premises is not permitted.

Secondary storage Devices register will be maintained by the respective sections/departments. Internal physical check will be carried out within the concerned sections/departments every week and result indicated in the register.

Sections/departments will render a quarterly certificate to the CCSO regarding safe custody of the pen drives in their sections/departments. No visitor/employee will be permitted to use or carry personal pen drive / External / Portable Hard Drives within the classified area/zone. Loss of External / Portable Hard Drive will be reported to CCSO immediately, and investigations carried out simultaneously by the sections/departments, to ascertain the extent of loss of classified information and to pinpoint responsibility for the loss for initiating suitable action against the defaulters.

a) Prohibit the use of external systems in production environment unless the system are specifically authorised.
b) Establish the terms, conditions and security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorised individuals.
c) Permit authorised individuals to use an external system to access the organisational system or to process, store or transmit controlled defence information only after –
   (i) Verification of the implementation of security requirements on the external system as specified in the organisation's security plans.
   (ii) Retention of approved system connection or processing agreements with the organisational entity hosting the external system.
d) Restrict the use of organisation –

   Controlled portable storage devices by authorised individuals on external systems.

7.7.4 Laptops/Palmtop/Electronic Notebook: Carriage of Laptops/ Palmtops/ Electronic into or out of classified zone/area without permission from CCSO is not permitted. Following precautions should also be taken to ensure security of information: -

(a) No personal Laptop/ Pen drive/ thumb drive/ hard disk/ palmtop/ Electronic Notebook and mobile phones with Blue tooth / Wireless Internet (4G/5G) should be permitted to be brought into the classified area/zone by the visitors or the employees.

(b) In case a Laptop/Palmtop/Electronic notebook is required to be brought inside for a specific purpose, the Bluetooth/WI-FI feature, if present, should be disabled and the user/owner should be escorted till his exit to prevent any enabling during the visit.

(c) Any laptop taken out for presentation should be checked for containing any unauthorised data/information. On return, it should be checked for any virus. Proper record of transport of data through Laptop should be kept. There should be provision to log all transactions, file transfers, read, write modifications etc.

7.7.5 Scanners. All scanners will remain in the physical custody of their owners and record of classified documents scanned should be kept.

7.7.6 Beacon and Siren must be integrated with the cameras used in Perimeter Intrusion Detection System (PIDS) as any camera can be tampered for accessing in to the air-gapped camera network and can be used as pivoting point for further compromise.

7.7.7 Destruction and Weeding:

a) Damaged and unusable Cartridge Tapes/ CDs/ DVDs/ Pen Drives and other CSM should be broken and destroyed by burning or as applicable to the weeding out paper based files and an entry to this effect be made in the register. CCTV recordings should be password protected.
b) Bad / condemned hard disk should not be released even after it has been replaced by a new one. Such hard disks will be destroyed by following procedures as applicable to weeding out of classified files.
c) Destructions should be carried out by application of corrosive Chemicals (acid or abrasive substances, emery wheel or disk sander) to the recording surface, and by shredding, incineration, disintegration, pulverization and smelting etc.

7.7.8 Cyber Security Audit:

a) The CISO must supervise all computer security measures within his offices/ branches/section. The CISO shall not be a foreign citizen, or a Personof Indian Origin who is a Non-Resident Indian.
b) Cyber Security Audit must be carried out under the strict supervision of Cyber Information Security Officer (CISO).
c) Periodic security audit of the IT is liable to be carried out by designated Govt Agencies, from time to time, to ensure that the laid down guidelines are strictly followed. However, this does not in any way reduce the requirement of internal security audits conducted by the organisation.
d) Periodic Computer Security Awareness programme for the computer operator, users and administrators should be carried out to expose them to the latest developments in computer security and remind them of their responsibilities.
e) Creating own Cyber Security Infrastructure with staff to carry out Cyber Security audits and attend Cyber security incidents on day to day basis. Such security audits of the computer system and network devices be carried out by:
   i. Internal team every six months and report is sent to CEO.
   ii. CERT-IN empanelled auditors preferably by STQC (Standardization, Testing & Quality Certification) under Department of Information Technology once every year.
   iii. Comply with the Cyber Security audit observations in time bound manner**.**

7.8 **Guidelines for Computer Users or Operators:**

(a) DOs.

(i) Observe effective physical security procedures to restrict access to computer systems. Access to be given only to authorized persons.
(ii) Use hardware locks in the cabinets in which the computer system is housed.

(iii) The contents of cartridge tapes, CDs or Pen Drives are as good as written files. All physical and static protective measures and instructions laid down in this manual for document security will also apply to the use, control and custody of data CDs or Pen Drives. External storage media containing classified data will be marked and treated like other classified documents.

(iv) All classified documents should be stored in an encrypted form in PCs as well as external storage devices.

(v) Adopt effective physical access control procedures by incorporating proper identification and authentication mechanism like "Complex password' at different levels and 'Dynamic Log in' by verifying the user's magnetic strip cards, finger prints and voice recognition, depending upon the nature of sensitivity of the data. User password is the most important aspect whose Confidentiality must be zealously guarded. Further, a password should have the characteristics laid down in this chapter.

(vi) Audit trails are activated for keeping electronic record on the system regarding use of computer system by various users. Activities of a user be logged and appropriate audit trails be maintained on the system in electronic form.

(vii) Before deleting the sensitive files, overwrite the files with some junk data to prevent restoration of the sensitive data by any means. Keep the backup of operating system software and application software under safe custody. One backup copy should be kept in different location as a precaution against fire hazards.

(viii) Backup data should be periodically updated. Keep the software maintenance tool in your own custody. The periodic checking of backup inventory and testing of the ability to restore information validates that the overall backup process is working. This may be given to the engineer called to attend to the faults in the system as and when required.

(ix) External CD writers will be under the custody of officer only. CD writer will be used only in minimum and unavoidable files and data.

(x) Ensure safe custody of the Computer Storage Media such as cartridge tapes, Pen Drives, CDs etc.

(xi) Every new incoming storage media or software should be tested for Virus.

(xii) Always use original software purchased from the authorised vendors.

(xiii) Copying of data, deletion, modification, etc. from the disk should be done under proper authorisation and supervision of the office-in-charge.

(xiv) Use Screen saver password

(xv) Use exclusive computer for internet

(xvi) Software tools like device locks may be used to block unwanted storage devices, Ports and other external accessories.

(xvii) The movement or exchange of storage medias should be with the prior approval of the officer-in-charge of the office.

(xviii) In case the shift system is in vogue, there should be proper handing / taking over among the shift-in-charge.

(xix) Damaged and unusable cartridges, tapes and CD(RW) and pen drives should be broken and destroyed and record to this effect should be maintained.

(xx) All the used printer ribbons and carbons should be destroyed by burning.

(xxi) Maintenance or rectification of faults in the computer system should be carried out under proper supervision. Keep an eye on the outside engineer attending to the fault in your computer system

(xxii) Use UPS units to prevent corruption of data and software.

(xxiii) Where feasible, all digital storage devices when permitted to be taken out, will be password protected and prior permission of security office is obtained.

(xxiv) Some PCs have in-built physical locking system. The user should keep the computer locked when it is not in use and ensure safe custody of the operating and duplicate keys.

(xxv) Culture of one printer or more per PC should be curbed. Ensure centralized printing within section.

(xxvi) Network printers must be located in a secure place so that the documents being printed cannot be taken away by unauthorized personnel.

(xxvii) Internet PC as well as patches released by OEM should be periodically updated. Live updates for Anti-virus/Anti-spyware and portable storage media used on internet machine to be scanned for spyware, Trojan and another suspicious malware before being used on LAN.

(xxviii) While updating patches (using WSUS Server) an outbound quota limitation must be enforced to mitigate the risk of data exfiltration.

(xxix) Disable system accounts when –

a) The accounts have expired
b) The accounts have been inactive for an organisation – defined time period
c) The accounts are no longer associated with a user or individual
d) The accounts are in violation of organisational policy.
e) Significant risks associated with individuals are discovered.

(xxx) Notify organisational personnel or roles when -

a) Accounts are no longer required.
b) Users are terminated or transferred
c) System usage or need to know changes for an individual

(xxxi) Information in Shared System Resources.

Prevented unauthorised and unintended information transfer via shared system resources.

(b) <u>DON'Ts</u>.

i. Don't let any unauthorized persons use your computer system.
ii. Don't share your password with anyone, not even your colleagues.
iii. Don't reveal the root password to any unauthorized person, particularly an outsider.

iv. Don't connect the computer directly to the mains. Also, no heavy electric load drawing machines like plain paper copier, shredding machines, coolers etc. should be connected to the source of constant voltage supply to the computer.

v. Do not connect your computer system storing classified data to internet.

vi. Don't allow staff members to bring their own storage medias or software to run on the computer system of the department.

vii. Don't use pirated or gifted copies of software as these may contain viruses and even facilitate intrusions into the system.

viii. Don't play computer games. These could be the main carriers of computer viruses and an unsuspecting or easy media for an intruder to break into your computer system.

ix. Don't panic if your system comes to a halt. Try to find out the cause and take precautions for future.

x. Don't store TOP SECRET or SECRET information permanently in the hard disk of PC. Whenever TOP SECRET or SECRET information is processed on the PC, erase the information immediately from the disk after the processing is over. When CDs are used for working on TOP SECRET or SECRET information it should be handled in accordance with the instructions for handling TOP SECRET or SECRET documents. It will be the responsibility of the authorized officer under whose supervision the PC work is being carried out.

xi. Don't carry CDs outside the office building. In case a data stored media has to be taken outside the office building, its movement will be with prior approval. A record of the movement indicating full details like date or time of its being taken out, name of the officer taking it out and purpose, date and its time of its return etc will be maintained.

xii. Don't keep CDs in table drawers etc.

xiii. Don't become a member of unofficial chat club or official chat club on official Internet.

xiv. Don't Carry Pornographic CDs or VCDs or such like material in other storage devices.

xv. Do not use pen drives, internal CD writer or combo drives unless specially authorized.

xvi. Do not use/install freely available screen saver on internet as these may have encoded spyware/Trojan.

7.9 Instructions for Use of Internet within Classified Area/Zone:

Internet services are based on open architecture with minimal security features. They are also open to malicious attacks, hacking, virus activities and cyber-crimes. Unauthorized and unregulated use of internet can lead to compromise in security. Internet within the office/area/zone handling classified information can be installed in the office of an officer with prior approval from the CISO. Internet connectivity should be provided to the offices only on a stand-alone PC. The Internet PC should not be used for office work. The Internet PC will have its own peripherals such as UPS, scanner, etc which will not be shared with any other system under any

circumstances. PC will be kept isolated from all other systems, especially LAN/Intranet. Connection of any other system with Internet line for any purpose, whatsoever, is strictly prohibited. No official or personal files will be stored on the hard disk of Internet PC. Personal media will never be used on Internet PC. No sensitive/ classified office work will be done in Internet computers.

7.9.1 All official work will be carried out on a system belonging to Air Gapped Network. Air Gapped Network will be isolated from the Internet at the physical layer. The air-gapped network's devices should meet following criteria:

(i) Must have a separate networking equipment, including switches and routers, accompanied by cables of a different colour to easily differentiate them from internet-related cables.
(ii) Specially designated desktop computer (referred as Entry-Exit system) must be used for moving data into/out of Air-gapped network.
(iii) Only officially recognised Thumb Drive/Pen Drive can be used on Entry-Exit system for data exchange. This Pen Drive will always remain in safe custody of CISO or any other officer designated by CISO. Every issue of Thumb Drive/ Pen Drive will be recorded.
(iv) Under no circumstances, the Entry-Exit system should be used for nefarious activities like connecting it to Internet using USB WiFi Dongles or Mobile Hotspots etc.
(v) Entry-Exit system is also part of Air-Gapped Network and should not be used for providing Remote Desktop Access/team Viewer Access to other air gapped systems.

7.9.2 The systems on the Air-Gapped network must meet following requirements:

(i) To enhance inventory tracking, systems within the Air-Gapped network should MAC bound to the hardware ports.
(ii) All USB ports must be blocked to disallow access to any Pen Drive/Thumb Drive/Hard Disk etc.
(iii) All Air-Gapped systems must have warning signs and Stickers Tags like USB Blocked / Air Gapped System etc.

7.9.3 Keeping in view the vulnerabilities involved in using internet in any sensitive / defence installation, apart from cyber security guidelines mentioned in the chapter, the following may be incorporated for security of the IT network(both internal & external) :-

i. Instead of multiple internet connections, there should be limited internet gateways for accessing the internet from within the organisation. These limited internet connections must be closely monitored by the Information Security Operations Centre of the organization.
ii. The SOC should include industry standard Security incident and Event Management (SIEM), Security Orchestration Automation and Response (SOAR) and User and Entity Behaviour Analytics (UEBA) solutions for faster response time during attacks and timely detection and blocking of attacks.

iii. All traffic through the organisational internet gateways must be screened to ensure that organizational data remains secure. Concerned personnel must be sensitized to the fact that their internet connections are provided to aid them in discharge of their duties and not for personal usage.

iv. Communication through open e-mail should be avoided from disseminating information related to the equipment being used or quantity to be manufactured or its component details at any stage (from development, testing to deployment) to its joint partners (contractors /sub-contractors).

v. If the joint venture involves collaboration of foreign firm(s) then, connectivity of their computers with contractor system needs to be examined from security angle.

vi. All employees should be barred from using private email addresses (like Gmail, hotmail, yahoo, rediffmail etc.) for any form of official communications and emails from suppliers/contractors through private emails addressees should be barred, as far as possible. However, the employees should be discouraged to use official email id for registering into various non-official platforms like banking, insurance etc.

vii. Social media usage policy should be defined and enforced on all employees. Unless specifically required for discharge of their duties, employees must be prohibited from accessing social media sites from their official systems. Employees should be discouraged from publishing information related to their work.

viii. Server room/network room should have biometric access control systems with CCTV coverage in place

ix. Enforce approved authorisations for controlling the flow of controlled defence information within the system and between connected systems.

7.10 **Cyber Posture Enhancement via integration with Defence CSOC:**

Industry entrusted with procurement orders/technologies developed by any Government agency of any such entity, privy to Defence related designs, plans, materials, documents, products, software, etc shall ingest necessary logs only (non-content) to Defence Cyber Security Operations Centre established by MoD for the purpose of centralized Log monitoring, analysis, anomaly detection and overall Cyber Security Posture Management.

CHAPTER – 8 - Subcontracting

8.1 General:

In case the ILDC outsource/ release or disclose classified information/ project to a sub-contractor all provisions of the Security Manual as per applicability shall be followed. It shall be the duty of CCSO to appraise the CEO / Head of Installation with regard to all the security provisions to be followed. Wherever/Whenever sharing of classified material/information is to take place, the same will be preceded by Non-Disclosure Agreement (NDA). The security parameters between the subcontractor and the ILDC shall be included in the contract with the following additional provisions:

(a) Out sourcing partners personnel and facilities would also be covered under the Official Secrets Act, 1923, whenever the ILDC is handling classification material, document, information etc.

(b) Persons working on such projects should be checked for character antecedents and police verification shall be obtained before inducting any person on such assignments.

(c) All the relevant clauses of the Manual of Security are to be made applicable for the sub-contractor.

8.2 Terms and conditions related to classic information:

Terms and conditions relating to retention, handling and destruction of classified information/material received or generated under the subcontract shall be clearly indicated in the main contract between the subcontractor and the prime ILDC. If certain classified information/material received or generated under the subcontract is intended to be retained, then the subcontractor has to comply with the provisions of this manual and give an undertaking of the same to ILDC and concerned Government agencies.

8.3 Engagement of consultants/advisers:

ILDC should ensure that the background and the character & antecedents of the advisers/consultants are verified before hiring their services. ILDC would be responsible for verification of C&A of advisors /consultants. Engagement of consultants/advisers shall be subject to signing of NDA.

8.4 Audit Recommendations:

The ILDC shall receive the recommendations made by Audit Teams. The ILDCs shall make note of recommendations and take action as warranted as soon as possible but in any case not later than the timeline.

CHAPTER – 9 - International Security

9.1 Imports of Equipment/ Materials:

a) Where Sensitive Equipment/ Materials is bought or otherwise acquired by the ILDC, it should be ensured the equipment is securely packed and sealed and transported. The packages will not have any markings to indicate that the Equipment is Top secret / Secret.

b) Top Secret and Secret Equipment/ Materials will not be shipped in Vessels / Flights which unload cargo in other countries or call at ports of unfriendly countries en-route.

c) Bills of lading or other documents will not indicate the classification of the Equipment. Separate bills of lading may be made out for small consignments which are delivered to the Master of the Ship for personal custody during transit. These documents will indicate the equipment in general terms, e.g. Instrument, PCB and so on, but will not give precise details.

d) Where possible, intimation will be sent to the consignee through official channels of the company. If time does not permit, intimation may be given through a coded / encrypted signal etc., describing the equipment in general terms and indicting the security measures to be adopted. Such consignments should be immediately removed from the Cargo area to the respective manufacturing Division / Unit or Factory.

e) Consignments of classified equipment awaiting shipping will be suitably shrouded. If the size of the equipment does not permit this, it should be stored in such a way as to be out of sight of observers. These consignments will be adequately guarded to prevent pilferage or inspection by outsiders.

f) The Embarkation Firm / Agency abroad will inform the respective manufacturing Division / Unit or Factory of the dispatch of classified equipment. On receipt of such intimation and based on expected date of arrival of equipment, the desired level of security measures are to be adopted.

g) The Embarkation Firm / Agency will be responsible for enforcing the necessary security measures including provision of escort, if any, till the equipment is taken over by the receiving manufacturing Division / Unit or Factory. Where necessary, the consignee will detail an officer to go to the port of disembarkation to take over the Equipment. The receiving officer will cover the equipment or otherwise conceal it and, if necessary, unload and move it out of the port during night so that chances of leakage of information are minimized**.** Consignor's responsibility to arrange security vetted carrier/transport agency till the receipt by consignee needs to be included.

h) Single point contact (Security Co-ordinator) shall be designated for controlled movement of classified materials and documents from foreign source with whom collaborators can communicate for secured transaction of TOT documents/Materials.

9.2 Warning to Consignees:

Consignors of classified equipment will warn Consignees of the classification of the Equipment and the precautions to be taken. Escorts will be detailed during movement of all classified equipment. Procedure followed for movement of classified documents would also be applicable to movement of sensitive equipment.

9.3 **Handing and Taking Over:**

Those concerned with Handing/ Taking over of classified equipment will ensure that they are fully aware of its classification and security measures to be adopted. Warnings as to the security measures necessary will be issued in writing. Top Secret and Secret Equipment will be Handed/ Taken over under the direct supervision of authorized senior officer only.

9.4 **NDA for transfer of classified information between two countries:**

The names of the Government Authority of each of the two countries empowered to authorise the release and to co-ordinate the safeguarding of Classified Information related to the Contract and the channels to be used for the transfer of the Classified Information between the Participants National Security Authority (NSA)/ Designated Security Authority (DSA)/ Competent Security Authority (CSA) and/or Contractors involved shall be governed by non-disclosure agreement.

9.5 **Movement:**

a) Consignors of Top Secret and Secret Equipment will warn the consignee of the dispatch of equipment so that the latter is in a position to make adequate security arrangements to receive it. All such equipment will be suitably shrouded and accompanied by an escort to ensure that no unauthorized person gains an access to them surreptitiously.
b) When only portion of equipment is Top Secret or Secret and it is possible to conceal that portion, it is not necessary for the entire equipment to be covered up. Only the Top Secret / Secret portion(s) of such equipment should be covered.
c) If a portion of equipment is ‘Top Secret’ or ‘Secret’, the consigner would ensure that the whole equipment is covered before dispatch.

CHAPTER – 10 - Visits and Meetings

10.1 Visit of foreign Nationals:

10.1.1a) No foreigners would be allowed to visit the area/zone/manufacturing facility where the work related to MoD projects is going on without clearance of MoD. As per the MHA guidelines, prior security clearance is required for visits of foreigners to vital and sensitive installations in the country. The CEO / Head of the concerned ILDCs will have power to approve business visits of foreign nationals those who are on appropriate type of visa to non-sensitive/non-strategic areas only of the manufacturing /R&D units of the Company and such visit shall be reported to Nodal Office after the visit within 24 hours through online portal of Vital Installation Information System (url: https://indianfrro.gov.in/viis/)preferably within two days but not later than fifteen days in any case. This will also be reported to /Nodal Office,in quarterly report. No foreigner shall be allowed to visit vital installation on the strength of tourist visa/e-tourist visa.

b) For the duration of the visit, the foreign nationals will be escorted by the security officer or officer designated by the company. A log of all the escorts assigned to the Foreigner or an Indian representing a foreign company/nation shall be maintained by IILDCs for atleast till the next external security audit.

c) No photography in the areas where work related to defence related projects will be permitted. It may also be ensured that viewing of contagious security areas does not occur.

d) After the visit, the names and particulars of the foreign nationals, the purpose, duration and site of the visit are to be communicated to the Internal Agencies of Ministry of Home Affairs quarterly. Instructions received from Dept of Defence Productions, Ministry of Defence in this regard from time to time will be followed.

10.1.2 In keeping with the above instructions, following procedure would be adopted for processing security clearance of Foreigners visiting the Company.

(a) The Head of the Department / Division / Factory Office as the case may, will initiate the case for visit of foreigners, well in advance, giving the following particulars:-

(i) Full name of the visitor.
(ii) Nationality of the visitor.
(iii) Date of birth.
(iv) Parentage of the visitor.
(v) Permanent and Present address of the visitor.
(vi) Passport No with date and place of issue.
(vii) Validity of Passport.

(viii) Visa details (types, data & place of issue and duration of visa)
(ix) Occupation and Name of the Firm / organization which the visitor is representing.
(x) Specific purpose of the visit.
(xi) If the foreigner has visited the establishment earlier, full details of the same is to be furnished.
(xii) Details of escort being provided for conducting the tour of the Foreign National(s).
(xiii) Address of Hotel/accommodation where the foreign visitor staying in India during the visit.
(xiv) The address of the Indian company with which the foreigner is having partnership/alliance etc.
(xv) Date & Time of visit
(xvi) Area to be visited
(xvii) Certificate that no classified document shall be shared with the foreign visitors.

(b) The particulars of the foreigners will be filled in a proper format and processed through CEO/Head of ILDC as the case may be for approval. Purpose of the visits also needs to be mentioned in the format prescribed for this purpose. The particulars are also to be intimated to MHA, Nodal Office, DDP in the prescribed format as indicated in 10.1.2(a).

(c) The approved copy will thereafter be forwarded to CCSO for preparing the Visitors Pass.

10.1.3 While conducting the visits of Foreigners, Instructions issued by the MHA/MoD from time to time should be followed.

10.1.4 In addition following points would also be adhered to:-

(a) The number of visits to non-sensitive areas/zones/offices shall be restricted to the barest essential and would be on need to know basis. Procedures to ensure that visitors are only given access to information consistent to their visit would be put in place by ILDC. The responsibility for determining need to know in connection with the visit shall rest with the individual who will disclose the information.

(b) If the visit to Manufacturing areas is considered necessary, the visitor should be allowed access to only these areas, which are relevant for the purpose of the visit.

(c) Notwithstanding the above guidelines, no foreign visitor should be allowed to manufacturing and development areas of Electronics Warfare and secure communications.

(d) The aforesaid guidelines should also apply to NRIs, Persons of Indian Origin, and Indian citizens representing foreign firms.

(e) No exposure as well as disclosure about activities undertaken at ILDC would be made to any foreign visitor without exclusive clearance from CEO/Head of ILDC. Such disclosures would be on minimum need basis.

10.2 **Meetings:**

Meetings would mean conference, seminar, symposium, exhibit, convention, training course or such gathering. Meeting with foreigners pertaining to MoD projects / classified information is not permitted without the approval of MoD.

10.2.1 ILDCs may conduct meetings with regard to Government Projects, with limited number of people who are connected with the project. However, all concerned officials will be governed under OSA, 1923. The information which is to be disseminated shall be cleared by the CEO. If ILDC wants to conduct meeting involving classified information, the same may be done with due authorization of CEO. However, it is the responsibility of the CEO to ensure that classified information is not leaked.

10.3 **Nomination of employees from ILDCs to attend Classified Meetings:**

The CEO may authorize its nominated employee(s) to attend certain classified meetings pertaining to classified information / sensitive information. It is the responsibility of CEO for non-leakage of information.

CHAPTER – 11 - Training

11.1 **General:**

It shall be the responsibility of the ILDC to provide all employees with security training and briefing, commensurate with their roles and responsibilities while dealing with classified information. Towards this, the ILDC may obtain defensive security, threat awareness and other educational and training information from the nominated agency of Government of India, Ministry of Defence.

11.2 **Security Briefing:**

All employees should be briefed on security do's/don'ts on joining as a part of induction programme. The induction programme must include Cyber Awareness Capsule

Prior to being granted access to classified information, an employee shall receive an initial security briefing that includes the following:

a. A threat awareness briefing.

b. A defensive security briefing.

c. An overview of the security classification system.

d. Employee reporting obligations and requirements.

e. Security procedures and duties applicable to the employee's job.

11.3 **Training:**

ILDC shall also be responsible for the training of CCSO &CISO and other members of his staff performing security duties, as promulgated from time to time by Ministry of Home Affairs. Training shall be based on the ILDC involvement with classified information and should be completed within One year of appointment as CCSO & CISO. Government may organize security briefings to the CCSO & CISO and other security staff as required from time to time.

11.4 **Refresher Training:**

The ILDC shall provide all the employees with some form of security education and training at least once a year, which shall aim at refreshing the training provided during the initial security briefing, update of security regulations and any new developments. ILDC shall maintain a record of all training conducted and employees' participation in them.

11.5 **Security Training of Vendors / Contractors and Casual Labourers:**

Security discipline needs to be imbibed among Vendors / Contractors and Casual Labourers for better efficiency of the overall Security system. This can be achieved by detailed briefing or small training capsule to contractors and on-the-job training to their casual labourers. A clause on termination of services / contract as the

case may be for breach of security of any kind must form part of the contract agreement between the ILDC and the Contractor/ Vendor.

11.6 **Training of Project Work Trainees:**

ILDC's may permit trainees to undergo training / undertake project work, however, all such trainees shall not be employed in any classified projects nor have any access to classified areas/zones/offices. In addition, all the students must be properly briefed about the sensitivity of the organization and conduct expected from them on Information Security. Police Verification including Bonafide /Conduct certificates from respective college should accompany the sponsorship of Trainees before permitting the students / trainees to take up project work / training and proper identification badges to be issued to them. No trainee is permitted to carry sensitive data from the installation. Further, the Project Reports of these trainees must be completely vetted by the Head of the Department before certification and submission of the same to the respective College / University.

11.7 **Training on Cyber Security:**

IT Division shall ensure that all personnel be appropriately trained on the Organization's Information Security policies commensurate with their roles and responsibilities and be kept up-to-date on any additions or changes to the policies.

CHAPTER – 12 – Miscellaneous

12.1 General:

MoD will be the nodal agency for preparation, review and implementation of the manual. However, conducting inspection and audit would be the responsibility of **/MHA /MoD**. MHA and MoDmay take the assistance of other organizations like DPSUs, NTRO etc. in the inspection or audit.

12.2 Publicity and Photography:

No photography would be permitted inside the Classified Zone/Area pertaining to MoD projects without the approval of MoD. Photography, when permitted for official purposes, will be done under proper supervision and both the photos, soft copy of photograph and their negatives shall be appropriately classified. In the case of Top Secret and Secret Equipment, permission for photography or publicity will be granted by General Manager / Chief Executive of the manufacturing Division / Unit or Factory, however, it will be done under controlled conditions by the official photographer. As far as possible only official agencies will be assigned for photography where authorized. Permission will not be necessary for official photography by the Factory / Division for compiling technical reports on equipment. Such reports and photographs will, however, be appropriately classified and safeguarded by them. The holder is, however, responsible to ensure that the equipment is not exposed to public view and that no one is afforded an opportunity to photograph it in full or in part.

12.3 Trials and Demonstration:

The Chief Executive of the manufacturing Division / Unit or Factory will enforce suitable security measures during trials / demonstration with the help of CCSO. When it is proposed to undertake demonstration involving Top Secret and Secret Equipment, full particulars of persons to be admitted to such demonstration will be approved by the Chief Executive. Special identity documents/passes will be issued to the invitees where necessary and a security officer appointed to enforce security measures.

12.4 Rejects and Salvage:

All Top Secret / Secret Equipment rejected during development, trial or manufacture will continue to bear its original security classification and receive appropriate security protection. If such equipment is no longer required, it will be dismantled and rendered unidentifiable. Such equipment will not be consigned to salvage unless it is downgraded to unclassified or shredded beyond recognition. All Hard disks pertaining to classified projects will, at no cost, be sent out for repair / recovery of data or salvage. Hard disks will always be removed before the CPU is sent to salvage. The hard disks will be destroyed under the supervision of Head of Security and certified to that effect. The disposal of non-sensitive scraps may be done M/s. MSTC.

12.5 **Disaster Management**:

The ILDC shall draw elaborate disaster management plan to minimize loss of life and property with an aim to handle the situation with utmost promptness and efficiency to safe guard the plant from major catastrophic incidents like Earth Quake, Bomb Blast, Floods, Terrorist Attack, etc., The ILDC shall also carry out frequent rehearsals, in any case, once in a year to ensure that in the event of any disaster, all functionaries can act effectively.

The disaster management plan should focus on data security while assuring business continuity. The BCP/DR backup sites (also referred as Secondary sites) should not be a source of data breach. Disaster Management Plan should be in line with the guidelines/instructions issued by the National Disaster Management Authority/State Disaster Management Authority.

12.6 **Internal Security Audit:**

The ILDC shall carry out internal security audit to ensure verification of compliance of security instructions contained in this manual. The Security Audits are required to be conducted to ascertain the level of compliance of security instruction and procedures specified in the security manual. The audit shall be done at least on a yearly basis. If ILDC is Multi Facility Organisation (MFO), audit shall be done annually in each facility: -

a) Check compliance by all the establishments to realize the designed security objectives as enumerated in the security manual.
b) Verify the effective implementation of the instructions and identify lapses, if any.
c) Verify the efficacy of the existing Security & Fire Control System.
d) To check that adequate safeguards exist against espionage, sabotage and subversion in a given environment where the installation is located.
e) To check the general Security awareness amongst the Employees.
f) To ascertain serviceability and operational worthiness of technical equipment such as CCTV, Electronic Barriers, Power Fence, Access Central Systems and Fire Fighting Equipment, etc.

12.7 **Action on Completion of Audit:**

On completion of audit, the audit observations contained in the audit report must be rectified by the auditee at the earliest and preventive action initiated after identifying the root cause of non-compliance to prevent its recurrence. Subsequent audit shall monitor the timely implementation of corrective / preventive action and its effectiveness. A report of the same shall also be submitted to MHAand DDP, MoD.

12.8 **External Security Audit:**

In addition to the internal audit carried by the ILDC, External audit by agencies of MHA and MoD in consultation with DDP/MoD shall be carried out once in two years. Government may also nominate any other agency to carry out security audit of ILDC on an annual basis, to ascertain compliance of security instructions contained in this security manual. Apart from this, the MHA/MoD/respective

licensing authority shall be at liberty to visit any company which has been issued with a licence for private sector participation in defence under I(D&R) Act, 1951 & Arms Act, 1959, at its discretion, for a random security system assessment.

12.9 **Penalty for Non-compliance of security guidelines by ILDC:**

12.9.1 In the event of non-adherence of security guidelines by ILDC, action shall be taken against the ILDC and/or individual person(s) as per relevant Government regulations/provisions in various Acts, such as IPC, CrPC, I(D&R) Act, Arms Act, OSA, 1923 etc. The ILDCs are further liable for action against them in the event of any breach of security resulting into compromising national security and national interest under relevant provisions of Official Secrets Act, 1923. The penal action in case of violation of guidelines contained in this manual may also result in cancellation/suspension of Industrial License by the concerned licensing authority. In case of cancellation / suspension of industrial licence, completion of projects/procurement, fore-closures of the unit, the ILDC would be required to return all the classified information and materials in its possession to the rightful owner or Ministry of Defence as the case may be, within 24 hours of such cancellation of the licence.

12.9.2 In case of breach, violation, non-adherence to the provisions of Security Manual, penal provision including financial penalties and denial of various RFPs/technical details/ToTs other contracts by the Government agencies including Service Headquarters, DRDO, DPSUs, etc. may be imposed.

12.9.3 For an entity holding license under Arms Act, 1959 (Arms Act) strict adherence to the terms and conditions of the license is mandatory. Any violation of these terms and conditions may lead to cancellation of license and prosecution under the Arms Act, 1959. The provisions of the Explosive Substances Act, 1908 will also be applicable in cases involving in the manufacture, possession, storage or transport of explosives.

12.10 **Alternate Power Source:**

An alternate power source is required to ensure that the system availability is maintained in the event of loss of primary power due to various reasons, including sabotage/subversion.

12.11 **Investigations of compromising emanations:**

Compromising emanations are unintentional intelligence-bearing signals that, if intercepted and analyzed, will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment.

12.11.1 Countermeasures will be applied only in proportion to the threat of exploitation and the resulting damage to national security should the information be intercepted and analyzed by a foreign intelligence organization. It is the responsibility of the agencies of MHA to share intelligence with DDP and DDP may decide further course of action

including penal action against the company. The remedial measures on ILDC after prior approval of the Competent Authority will also be addressed.

12.11.2 The MHA & MoD are responsible for performing threat assessment and vulnerability studies when it is determined that classified information may be exposed during investigations / study. Investigations on theft /sabotage will be carried out by CCSO /local police.

12.11.3 ILDCs will assist the agencies of MHA & MoD in conducting threat and vulnerability surveys by providing the necessary information upon request:

12.12 **Retention of Classified Documents Generated Under IR&D Efforts:**

ILDCs may retain the classified documents that were generated in connection with their classified IR&D efforts for the duration of their facility is meeting the security manual requirements. Documents shall be clearly identified as "IR&D DOCUMENTS." ILDCs shall establish procedures for review of their IR&D documents on a recurring basis to reduce their classified inventory to the minimum.

12.13 **Classified Waste Management:**

Classified waste shall be destroyed as soon as practicable. This applies to all waste material containing classified information. Pending destruction, classified waste shall be safeguarded as required for the level of classified material involved. Receptacles utilized to accumulate classified waste shall be clearly identified as containing classified material.

12.14 **Waste Management:**

This shall include the scrap generated as well as the components rejected during the (Quality Assurance) QA evaluation, as individual the components may be useless but collectively and over time they could be assembled into a weapon. Comprehensive guidelines should be in place and be periodically reviewed, depending upon the work being executed at the plant with respect to environment, waste management, electronics waste disposal. The guidelines must include explicit procedures for the destruction of electronic devices at the end of their life cycle, especially emphasizing the secure wiping of sensitive data from storage devices to prevent potential data breaches.

12.14.1 Waste Management from health perspective its the classification of waste as chemical, hazardous, toxic and recyclable collection, transport, processing or disposal, managing and monitoring of waste materials. The term usually relates to materials produced by industrial activity, and the process is generally undertaken to reduce their effect on health, the environment or aesthetics. Waste management is a distinct practice from resource recovery which focuses on delaying the rate of consumption of natural resources. All wastes materials, whether they are solid, liquid, gaseous or radioactive fall within the ambit of waste management.

12.14.2 E-Waste: Once the electronic device reaches its end of its life cycle, the data on the device must be destroyed by techniques like erasing, wing, and

degaussing. Storage devices such as hard disks and flash drives should undergo destruction, and the CISO must issue a destruction certificate, co-signed by a board of officer, verifying the destruction process.

12.15 **Compliance statement:**

Compliance Statement	The company will give an undertaking that it complies with its own instructions/orders as well as all the above provisions as applicable
Internal Security Audit	The company will commit to an internal audit and give self-certification with regards to compliance with the mentioned provisions by 31st March every year to the DDP

12.15.1 In case of Multi Facility Organisation (MFO), the compliance reports will be compiled and forwarded by the Headquarters of the ILDCs.

*****

APPENDIX

Compliances to be followed by ILDCs

Annexure No.	Reporting mechanism post issue of license	Compliance frequency	Compliance date*	Reporting to
1	Report on Progress made till commencement.	Half yearly or till commencement	30th September 31st March or till commencement	Nodal Office, DDP, concerned licensing authority***
2	Intimation/information of commencement of production	Once	Before start of Production	Nodal Office, DDP, concerned licensing authority
3	Information of Production data/Sales data	Quarterly	30th June 30th September 31st December 31st March	Nodal Office, DDP, concerned licensing authority
4	Undertaking to MHA/MoD/DPIIT to comply with provisions of Security Manual	Immediately and on half yearly	Immediately and on 30th September 31st March	Nodal Office, DDP, concerned licensing authority
5	Self-certification on compliance to internal security Audit	31st March	31st March	DDP, concerned licensing authority
6	Annual Cyber Security Audit in case of classified information, if any	Annually	31st March	MoD & Nodal Office, DDP
7	Internal Inspection Reports of Manufacturing Facilities	Half yearly	30th September and 31st March	DDP
8	Report on Loss/recovery/unearthed Arms & Ammunition and Explosives	Quarterly	30th June 30th September 31st December 31st March	Nodal Office, DDP, Local Police

9	Report to /MHA/DDP on compliance with observations of Internal and External Audit	Quarterly & within 15 days of visit	30th June 30th September 31st December 31st March	Nodal Office, DDP
10	Report on Visit of foreign business visitors	Immediately and on Quarterly basis	Immediately 30th June 30th September 31st December 31st March	Nodal Office, DDP,
11	Action taken report to Nodal Office, DDP	Half yearly	30th June 30th September 31st December 31st March	Nodal Office, DDP
12 & 13	Report on incidents such as Fire, Theft, Sabotage, Espionage, Cyber Accidents, strike, terror activities, adverse information about employees unauthorized receipt of classified materials, report of loss or suspected compromise	Immediately(with in 24 hours) and on quarterly basis	Immediately 30th June 30th September 31st December 31st March	Local Police,MHA, Nodal Office, DDP
14	Report to MHA on list of employees cleared from security angle	Annually	30th June 30th September 31st December 31st March	Nodal Office, DDP
15	Report of inflow of foreign investment	Annually	30th June 30th September 31st December 31st March	Nodal Office, DDP

**Report to be submitted within 7 days of end of Quarter/Half year/Financial year*

*** In case, ILDC does not have any information to report, a Nil report shall be sent to concerned licensing authorities*

****Licensing authorities are Ministry of Home Affairs (MHA), Department for Promotion of Industry & Internal Trade (DPIIT) and Department of Commerce (DoC)*

Annexure - I

1. Name and Address of the Industrial Undertaking_____ State_____

2. Location of Factory_____State

3. If any extension has been granted then

   (i) Letter of Extension No._____Date_____
   (ii) Date upto which extension granted_____

4. Whether lease land expiry Yes / No _____

5.1 Status of progress:

Proposed Investment	Actual Investment

5.2 Status of progress:

Physical Progress	Status
	1.
	2.
	3.
	4.
	5.

6. Date of commencement as indicated in the DPR (furnished in the license application)_____

7. Likely date of commencement Year Quarter

8. Additional Information, If any,

_____

Place:

Date:

_____

[Signature]

_____

Name (Block Letters)

_____

(CEO/MD)

Annexure-II

INTIMATION/INFORMATION OF COMMENCEMENT OF PRODUCTION

Number Year

1. Reference Number CIL/DIL
   (Strike whichever is not applicable)
2.

Actual Date of Commencement (Item wise)*	Name of Item(s)	Date							
1.									
3.									
4.									
5.									
6.									
7.									

3. Actual Investment

(Amount in Rupees)

a	Land (for rented premises, Capitalised value of the same to be indicated)									
b	Building									
c	Plant & Machinery									
	(i)	Indigenous								
	(ii)	Imported								
		(a)	CIF Value							
		(b)	Landed Cost							
	(iii)	Total [(i)+(ii)+(iii)]								

4. Employment
   (a) Supervisory _____
   (b) Non-Supervisory _____

5. Any other information (you may indicate difficulties, if any faced during implementation of the project).

Place:

Date: _____ [Signature]

_____ Name (Block Letters)

_____ (CEO/MD)

* *i. Each item under the issued license is to be mentioned.*
ii. Each successive report should also mention items mentioned in the previous form.

Annexure-III

INFORMATION OF PRODUCTION DATA/SALES DATA

Date-

(i) Details of Industrial License :
(ii) Period of reporting :
(iii) Items for' which license granted :
(iv) Status of commencement of Commercial Production :

(v) Production data :

S.No.	Item	Licensed Quantity (if applicable)	Quantity Produced	Value	Import content (%)
1					
2					
3					
4					

(vi) Sale data: (please tick the appropriate box and furnish details of the entities)

S.No.	Item	Quantity	Value (in INR)	Entity to whom sold	
				Domestic (organisation)	Export (countries)
1					
2					
3					
4					

(vii) Stock in hand/Balance Stock

S.No	Item	Quantity
1		
2		
3		
4		

Place :

Date: [Signature]

Name (Block Letters)

(CEO/MD)

Annexure-IV

No._____

To

D(DIP) Section,

Department of Defence Production,

Ministry of Defence

Subject: Self certification on compliance to Security Manual for Licensed Defence Indsutries

In regard to Industrial License No_____ issued to M/s _____, I _____ hereby declare that our company is complying with the provisions mentioned in the Security Manual for Licensed Defence Industries prepared by Ministry of Defence, Department of Defence Production.

Encl: If required

Place:

_____

Date: [Signature]

_____

Name (Block Letters)

_____

(CEO/MD)

Annexure-V

No._____

To,

D(DIP) Section,

Department of Defence Production,

Ministry of Defence

Subject: Self certification on compliance to Internal Security Audit.

In regard to Industrial License No_____ issued to M/s _____, I _____ hereby declare that the Internal Audit as mandated by the Security Manual for LDIs have been conducted and the observations/Recommendations have been complied with.

Place:

Date:

_____
[Signature]

_____
Name (Block Letters)

_____
(CEO/MD)

Annexure-VI

Annual Cyber Security Audit in case of classified information, if any

S.No	Observations of Annual Cyber Security Audit	Action Taken	Stage of Progress	Probable Date of completion	Remarks, if any

Annexure-VII

Internal Inspection Reports of Manufacturing facilities

S.No	Observations of Internal Reports	Action Taken	Stage of Progress	Probable Date of completion	Remarks, if any

Annexure-VIII

Report on Loss/recovery/unearthed Arms & Ammunition and Explosives

S.No	Date & Place of Incident	Whether reported to concerned authorities	Cause of Incident	Loss/Value	Corrective Measures taken	Remarks, if any

Annexure-IX

Report to MHA/DDP on compliance with observations of Internal and External Audit:

For Internal Audit:

S.No	Observations of Internal Audit	Action Taken	Stage of Progress	Probable Date of completion	Remarks, if any

For External Audit:

S.No	Observations of Agencies of MHA	Action Taken	Stage of Progress	Probable Date of completion	Remarks, if any

Annexure-X

Report on visit of Foreign Business visitors:

S.No	Name & Address	Nationality	Passport/Visa Details	Area Visited	Purpose of Visit	Duration of Visit

Annexure-XI

Action taken report to Nodal Office, DDP (Half yearly):

S.No	Observations/Recommendations	Action taken	Probable date of Completion	Remarks, if any

Annexure-XII

Report on Fire, Theft, Sabotage, Espionage, Cyber Accidents, strike, terror activities, adverse information about employees unauthorized receipt of classified materials, report of loss or suspected compromise (Immediately):

S.No	Date & Place of Incident	Brief of Incident	Loss	Remarks, if any

Annexure-XIII

Report on Fire, Theft, Sabotage, Espionage, Cyber Accidents, strike, terror activities, adverse information about employees unauthorized receipt of classified materials, report of loss or suspected compromise (Quarterly):

S.No	Date & Place of Incident	Cause of Incident	Loss	Corrective Measures taken	Remarks, if any

Annexure-XIV

Report to MHA on list of employees cleared from Security angle (Quarterly):

S.No	Name & Address	Employee ID	Aadhaar Details	Designation

Annexure-XV

Name of the Company	
License No.	
Particulars of the concerned	**Name** **Email** **Contact**
FDI Route (Government/Automatic) **(In Case of Government Route, Approval No and date)**	

Contd../…

Details of Foreign Investors

S. No.	Name of Foreign Investor	Percentage Shareholding	Country	Nature of Investment (FDI, FII, FPI, QFI etc.)	Value

*****