FOREWORD

The Security Manual for Licensed Defence Companies in the private sector is being issued in pursuance of para 12 of the Press Note No.2 (2002 series) issued by the Department of Industrial Policy & Promotion (DIPP), Ministry of Commerce and Industry, Government of India laying down guidelines for licensing production of arms and ammunitions. In terms of para 12 of the said Press Note, licensed defence companies are required to put in place adequate safety and security procedures once licence is granted and production commences and this would be subject to verifications by authorised Government agencies.

2. The Industrial Licence is issued by DIPP, being the licensing authority, in terms of the Rule 7 of the Registration and Licensing of Industries Undertaking Rules framed under Industries (Development & Regulation) Act 1951, subject to the conditions stipulated in the Industrial Licence. The Industrial Licence contains a Footnote to the effect that detailed instructions issued by the Ministry of Defence (Department of Defence Production) from time to time in regard to conditions stipulated in the Industrial Licence in terms of Para 12 & 15 of the Press Note 2 (2002 series) on adequate safety and security procedures to be put in place by the licensee and on sale of defence items produced under the industrial licence shall also be followed by the licensee for strict compliance. This Security Manual is, therefore, being issued for strict compliance by licensed defence companies in the private sector as a part of the licensing conditions prescribed in the Industrial Licence.

3. 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 of licensed defence industries in the private sector are also “prohibited places” in terms of the provisions of the Official Secrets Act, 1923.

4. The Security Manual prescribes minimum standards of security and other safeguards which should be strictly complied with and put in place by the licensee in order to prevent any unauthorised disclosure of classified information and materials. All Defence Public Sector Undertakings and the Ordnance Factories, which have their own respective Security Manuals/Instructions, shall update their Manuals in order to incorporate these standards.

5. DPSUs, Ordnance Factories and 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. These additional safeguards shall be disclosed forthwith to the concerned desk in the Industrial Security Branch in the Intelligence Bureau, and to Director (DIP) in the Department of Defence Production.

6. Any suggestions regarding improvements/modifications required in the Security Manual may be sent to MHA under intimation to MOD [DDP/DIP Division].

*****
EXECUTIVE SUMMARY

Introduction

This Security Manual is an effort to lay down in detail the security architecture that needs to be put in place by the Indian defence companies in the private sector immediately after obtaining industrial licence from the Department of Industrial Policy & Promotion (DIPP) and before commencing commercial production. It prescribes a set of minimum security standards that shall be strictly complied with by the Indian Licensed Defence Industry (ILDC) uniformly across the board for production of defence equipment and items in the private sector. In case, however, any classified project assigned to an ILDC necessitates additional security requirements over and above those detailed in this Security Manual, the same shall be separately spelt out in the RFP and subsequently form part of the contractual document.

Responsibilitles of ILDC

Immediately after obtaining industrial licence, the ILDC is required to give an undertaking that it shall comply with the provisions of the Security Manual. The undertaking shall be forwarded to the IS Division of the MHA under intimation to DIPP and DIP Division in the Department of Defence Production, Ministry of Defence. 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 authorized agency. In summary, the responsibilities of the ILDC, inter alia, mainly entail the following:-

Security Organisation & Personnel Security

- Appointment of an Indian citizen as the Company Chief Security Officer (CCSO) who will be responsible for implementing the security architecture in the company as detailed in this Security Manual;
- Thorough verification of character and antecedents of all persons before joining and periodic security check of all personnel employed including all levels of management;
- Briefing all employees on security do’s/don’ts as part of induction programme and obtaining a written undertaking from them at the time of joining that they have read and understood the contents of this Security Manual. Their attention may also be drawn in particular to the Official Secrets Act, 1923 which extends to the whole of India and applies to servants of the Government and to citizens of India outside India.
- Periodic Training/briefing of employees on the security architecture.
- Reporting to the nearest office of IB any information in regard to actual, possible or probable espionage, sabotage, terrorism or subversive activities in its locations;
Reporting to the nearest office of IB any adverse information about any employee(s) that has come to notice;

Submission of the following Reports to the Industrial Security Branch of IB:
- Monthly report on loss/recovery of arms, ammunition and explosives.
- Monthly report of fire accidents and other incidents/accidents.
- Quarterly report on the visits of foreign business visitors.
- Half yearly report on Action Taken Report on the visits of IB and other agencies nominated by MHA for external security audit.
- Half yearly report on internal inspections of manufacturing facilities.
- Quarterly report forwarding list of employees cleared from security angle.

Document Security

- Ensuring safe custody of classified documents and material and maintaining a security system to prevent their unauthorized removal from the facility;
- Developing procedures for safeguarding classified material in emergency situations;

Communication, Computer and Cyber Security

- Appointment of an Indian citizen as Information Security Officer who would, *inter alia*, be responsible to undertake activities like development, implementation and evaluation of the facility Information Systems (IS) program, safeguard computer storage media, software, sensitive and proprietary data and prevent threats to computer and cyber security.
- Designate a Computer Security Officer (CSO) to supervise all computer security measures. CSO shall be an Indian citizen.

Security of Premises and Physical Security Measures

- Institute Physical security measures through deployment of security personnel/guards for security of premises, perimetric and proper access control and maintaining round the clock surveillance and monitoring through CCTVs and intruder alarm system.
- Equipping the Entry and Exit gates with DFMDs and HHMDs and manual I-Card checking facility and deploying adequate number of security personnel for frisking and baggage screening of employees moving in and out of the plant/facility.
- Patrolling in and around the Vital Points including night patrolling by guards and dog squads, if required.
- Installing Automatic Vehicle and Baggage Scanners to check the material.
- Setting up a Control Centre with monitoring and recording for 30 days with replaying facility for monitoring all visitors' activities within the plant/facility. The Control Room should be manned round the clock with standby arrangements in place.
- Ensure that the vehicles for transportation of explosive materials/finished products are escorted by the armed guards.
Visit of foreign nationals

➢ Reporting the details of the visit of the foreign nationals permitted with the approval of CEOs/Chairman/MD, indicating the purpose, duration and site/place of the visit, to the nearest office of the IB within two days of the visit.

Disaster Management Plan

➢ Drawing up an elaborate disaster management plan to safeguard the plant/facility from major catastrophic incidents and carrying out frequent rehearsals to ensure effectiveness of the plan/facility in the event of any disaster.

Security Audit and compliance to security audit observations

➢ Carrying out internal security audit at least twice a year to ascertain the level of compliance of security instructions and procedures contained in this Security Manual. In case the ILDC is a multi facility organization, the Head Office shall also carry out security audit once a year.
➢ Submitting a self certification committing itself to the internal security audit, to the DIP Division in the Department of Defence Production/MOD and MHA.
➢ Providing all the requisite assistance to the IB for carrying out external security audit once in two years and to any other agency nominated by the MHA for external security audit on an annual basis. It may be noted that MHA shall also be at liberty to visit any ILDC for a random security system assessment.
➢ Ensuring strict compliance to the security audit observations and monitor the timely implementation of corrective/preventive actions and its effectiveness. Compliance report shall also be submitted to the IB and IS Division of the MHA.

Waste Management

➢ Devise comprehensive guidelines for waste management and components rejected during the QA evaluation and periodically reviewing the guidelines depending upon the work being executed at the plant.

Miscellaneous

➢ Reporting the incidents of breach of security involving loss of any type to the Ministry of Defence automatically and immediately after their occurrence.
➢ Returning all classified information and materials in its possession to its rightful owner or Ministry of Defence, within two days of the cancellation of industrial licence as a penalty for non-compliance of security guidelines.
It must be noted that the onus is on the licensed companies to strictly adhere to and comply with the provisions of this Security Manual in letter and spirit. Consequences of non-compliance will depend upon the severity of the security breach and violations, which may lead to cancellation of the industrial licence and imposition of penalty prescribed under the statutory provisions of the Industrial (Development & Regulation) Act, 1951.
FLOW DIAGRAM ON REPORTING AND COMPLIANCE

Post issue of Industrial Licence

- Undertaking to MHA/MOD/DIPP on compliance of provisions of Security manual (Immediately)
- Self certification on compliance to internal security audit (31st March of every year)
- Report on Loss/recovery/unearthed Arms and Ammunition and Explosives (Monthly)
- Report to IB/MHA/DDP on compliance with observations of Internal and External Security Audit (Half-yearly)
- Internal Inspection Reports of Manufacturing Facilities (Half-yearly)

- Report on Visit of foreign business visitors (Quarterly)
- Action taken report to IB (Half-yearly)
- Report on Fire accidents & other incidents / accidents to IB (Monthly)
- Report to MHA on list of employees cleared from security angle (Quarterly)
<table>
<thead>
<tr>
<th>TOPIC</th>
<th>PAGE No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>2</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Flow Diagram for Reporting and Compliance</td>
<td>7</td>
</tr>
<tr>
<td>Table of Contents</td>
<td>8</td>
</tr>
<tr>
<td>List of Abbreviations used</td>
<td>11</td>
</tr>
<tr>
<td>Chapter 1 - General Provisions, Requirement and Responsibility</td>
<td>12</td>
</tr>
<tr>
<td>- Purpose</td>
<td></td>
</tr>
<tr>
<td>- Scope</td>
<td></td>
</tr>
<tr>
<td>- Authority</td>
<td></td>
</tr>
<tr>
<td>- Interpretation of this Manual</td>
<td></td>
</tr>
<tr>
<td>- Waiver and exceptions to the provisions of the Manual</td>
<td></td>
</tr>
<tr>
<td>- Responsibility of Management and employees</td>
<td></td>
</tr>
<tr>
<td>Chapter 2 – Security Organisation and Personnel Security</td>
<td>14</td>
</tr>
<tr>
<td>- Company Chief Security Officer (CCSO)</td>
<td></td>
</tr>
<tr>
<td>- Responsibilities and duties of CCSO</td>
<td></td>
</tr>
<tr>
<td>- Reports of loss, compromise or suspected compromise</td>
<td></td>
</tr>
<tr>
<td>- Reporting procedures</td>
<td></td>
</tr>
<tr>
<td>- Personnel Security</td>
<td></td>
</tr>
<tr>
<td>Chapter 3 – Document and Material Security</td>
<td>21</td>
</tr>
<tr>
<td>- Security Classification</td>
<td></td>
</tr>
<tr>
<td>- Guidelines on Classifications</td>
<td></td>
</tr>
<tr>
<td>- Marking of Classified Documents</td>
<td></td>
</tr>
<tr>
<td>- Accounting of Classified Documents and Materials</td>
<td></td>
</tr>
<tr>
<td>- List of Documents, Checks &amp; Annual accounting</td>
<td></td>
</tr>
<tr>
<td>- Care&amp; Custody of Classified Documents and Materials and responsibility of holders</td>
<td></td>
</tr>
<tr>
<td>- Emergency Procedures</td>
<td></td>
</tr>
<tr>
<td>- Disclosure</td>
<td></td>
</tr>
<tr>
<td>- Downgrading, Disposal &amp; Destruction of Classified Documents and Materials</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 4 – Communication Security
- Telephone
- Cell or Mobile Phones
- Telex, Teleprinter and Fax Communications

Chapter 5 - Computer and Cyber Security (Information Systems Security)
- General
- ISO 27001 Compliance
- Common Requirements
- Enterprise Resource Planning
- Physical and software security
- Acquisition of Computer hardware and software
- Threats to and Vulnerability of computerised information, Malicious code, virus measures and countermeasures
- Miscellaneous aspects
- Guidelines for computer users and operators
- Instructions on use of Internet

Chapter 6 – Security of Premises and Physical Security Measures
- Physical Security Measures
- Declaration of facility as prohibited place
- Layout of Premises
- Setting up of Plant Security Council
- Perimeter, Access Control and Security Personnel
- Identity documents, Entry points and parking of vehicles
- Reception office and visitors
- Key organisation
- Late sitting in Office
- Entry and Parking of vehicles
- Photography
- Carriage of weapons
- Carriage of liquor
- Security measures for Sensitive / Secure/ storage areas for classified equipment
- Transportation of Explosive material/finished products
- Building Security
- Emergency response/contingency plan

Chapter 7 – Visits and Meetings
- Visits of foreign national(s)
- Meetings
- Request from ILDC to attend classified meetings
<table>
<thead>
<tr>
<th>Chapter 8 – Subcontracting</th>
<th>69</th>
</tr>
</thead>
<tbody>
<tr>
<td>• General</td>
<td></td>
</tr>
<tr>
<td>• Responsibilities</td>
<td></td>
</tr>
<tr>
<td>• Security clearances</td>
<td></td>
</tr>
<tr>
<td>• Notification of Unsatisfactory Conditions</td>
<td></td>
</tr>
<tr>
<td>• Termination/ Banning of Subcontract</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 9 - International Security Provisions</th>
<th>71</th>
</tr>
</thead>
<tbody>
<tr>
<td>• General</td>
<td></td>
</tr>
<tr>
<td>• Import of equipment</td>
<td></td>
</tr>
<tr>
<td>• Warning to Consignees</td>
<td></td>
</tr>
<tr>
<td>• Handing and Taking Over</td>
<td></td>
</tr>
<tr>
<td>• Movement</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 10 – Training</th>
<th>73</th>
</tr>
</thead>
<tbody>
<tr>
<td>• General</td>
<td></td>
</tr>
<tr>
<td>• Security briefing</td>
<td></td>
</tr>
<tr>
<td>• Refresher Training</td>
<td></td>
</tr>
<tr>
<td>• Security training of Vendors/Contractors and Casual Labourers</td>
<td></td>
</tr>
<tr>
<td>• Training of project work Trainees</td>
<td></td>
</tr>
<tr>
<td>• Debriefing</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 11 – Miscellaneous</th>
<th>75</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Nodal Agency</td>
<td></td>
</tr>
<tr>
<td>• Publicity and Photography</td>
<td></td>
</tr>
<tr>
<td>• Trials and Demonstration</td>
<td></td>
</tr>
<tr>
<td>• Rejects and Salvage</td>
<td></td>
</tr>
<tr>
<td>• Disaster Management</td>
<td></td>
</tr>
<tr>
<td>• Internal Security Audit</td>
<td></td>
</tr>
<tr>
<td>• Action on Completion of Audit</td>
<td></td>
</tr>
<tr>
<td>• Penalty for Non Compliance</td>
<td></td>
</tr>
<tr>
<td>• External Security Audit</td>
<td></td>
</tr>
<tr>
<td>• Penalty for Non-compliance of security guidelines by ILDC</td>
<td></td>
</tr>
<tr>
<td>• Alternate Power Source</td>
<td></td>
</tr>
<tr>
<td>• Investigations of compromising emanations</td>
<td></td>
</tr>
<tr>
<td>• Retention of Classified Documents Generated Under In-house R&amp;D Efforts</td>
<td></td>
</tr>
<tr>
<td>• Classified Waste Management</td>
<td></td>
</tr>
<tr>
<td>• Waste Management</td>
<td></td>
</tr>
<tr>
<td>• Compliance Statement</td>
<td></td>
</tr>
</tbody>
</table>
### List of abbreviations

<table>
<thead>
<tr>
<th>A.1</th>
<th>ILDC</th>
<th>Indian Licensed Defense Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.2</td>
<td>DPSU</td>
<td>Defense Public Sector Undertaking</td>
</tr>
<tr>
<td>A.3</td>
<td>DIPP</td>
<td>Department of Industrial Policy and Promotion</td>
</tr>
<tr>
<td>A.4</td>
<td>CCSO</td>
<td>Company Chief Security Officer</td>
</tr>
<tr>
<td>A.5</td>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>A.6</td>
<td>CMD</td>
<td>Chairman and Managing Director</td>
</tr>
<tr>
<td>A.7</td>
<td>OFB</td>
<td>Ordnance Factory Board</td>
</tr>
<tr>
<td>A.8</td>
<td>MOD</td>
<td>Ministry of Defense</td>
</tr>
<tr>
<td>A.9</td>
<td>DDP</td>
<td>Department of Defence Production</td>
</tr>
<tr>
<td>A.10</td>
<td>TOP SEC</td>
<td>Top Secret</td>
</tr>
<tr>
<td>A.11</td>
<td>CONFD</td>
<td>Confidential</td>
</tr>
<tr>
<td>A.12</td>
<td>RESTD</td>
<td>Restricted</td>
</tr>
<tr>
<td>A.13</td>
<td>RAX</td>
<td>Rural Automatic Exchange</td>
</tr>
<tr>
<td>A.14</td>
<td>COTS</td>
<td>Commercial of the Shelf</td>
</tr>
<tr>
<td>A.15</td>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>A.16</td>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>A.17</td>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>A.18</td>
<td>ID</td>
<td>Identification Card</td>
</tr>
<tr>
<td>A.19</td>
<td>CCTV</td>
<td>Closed Circuit TV</td>
</tr>
<tr>
<td>A.20</td>
<td>NSA</td>
<td>National Security Authority</td>
</tr>
<tr>
<td>A.21</td>
<td>MHA</td>
<td>Ministry of Home Affairs</td>
</tr>
<tr>
<td>A.22</td>
<td>CSA</td>
<td>Competent Security Authority</td>
</tr>
<tr>
<td>A.23</td>
<td>IB</td>
<td>Intelligence Bureau</td>
</tr>
<tr>
<td>A.24</td>
<td>IR&amp;D</td>
<td>In-house Research and Development</td>
</tr>
<tr>
<td>A.25</td>
<td>HQ</td>
<td>Head Quarters</td>
</tr>
<tr>
<td>A.26</td>
<td>MFO</td>
<td>Multi Facility Organization</td>
</tr>
<tr>
<td>A.27</td>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>A.28</td>
<td>GSM</td>
<td>Global System Monitoring</td>
</tr>
<tr>
<td>A.29</td>
<td>ANPR</td>
<td>Automatic Number Plate Recognition</td>
</tr>
<tr>
<td>A.30</td>
<td>DFMD</td>
<td>Door Framed Metal Detector</td>
</tr>
<tr>
<td>A.31</td>
<td>OSA</td>
<td>Official Secrets Act</td>
</tr>
<tr>
<td>A.32</td>
<td>DSA</td>
<td>Designated Security Agency</td>
</tr>
<tr>
<td>A.33</td>
<td>QA</td>
<td>Quality Assurance</td>
</tr>
</tbody>
</table>
CHAPTER - I

General Provisions, Requirements and Responsibility

1.1 **Purpose.** The Manual lays down the Security Guidelines for Indian Licensed Defence Companies (ILDC), as mandated by License Conditions vide Para 12 of Government of India, Ministry of Commerce and Industry, Department of Industrial Policy and Promotion, Press Note No 2 (2002 Series). The Manual is issued by Ministry of Home Affairs and lays down guidelines for minimum safety and security procedures which the licensee is required to comply with as part of the licensing conditions of the Industrial Licence. The Manual prescribes the procedures, requirements, restrictions and other measures to protect the unauthorised disclosure and transmission/movement of classified information and materials, in order that that India's national security interests are not adversely affected by such unauthorised disclosure or movement. The Manual also controls the authorised disclosure of classified information and materials released by MOD/MHA to ILDC.

1.2 **Scope.**

1.2.1 The Manual is applicable to all Indian companies issued with Industrial License by Ministry of Commerce/DIPP for manufacture of defence products under Industries (Development & Regulation) Act, 1951.

1.2.2 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.

1.2.3 Implementation of changes to this Manual by ILDC shall be effected to their manual and procedures with immediate effect.

1.3 **Authority:**

1.3.1 The Committee headed by MHA in the Internal Security Division is responsible for providing overall policy direction, periodic review and modification of this Security Manual.

1.3.2 The IB is the designated agency for inspecting and monitoring ILDCs who require or will require access to, or who store or will store classified information and materials covered by this Manual. The Industrial Security Branch in the IB is the designated branch for this purpose.
1.4 **Interpretations of this Manual.** Request for interpretation of this Manual by ILDCs shall be forwarded to the IS Division in the MHA.

1.5 **Responsibility of the Management and Employees.**

1.5.1 It is the direct responsibility of every employee of the company to safeguard the security of all classified information and materials to which he has access in course of his duties or which he comes in possession in any other way.

1.5.2 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 of classified information or materials, either deliberately or inadvertently.

1.5.3 Every employee in the officer grade 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.

1.5.4 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 these 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, who would ensure that security measures necessary for implementing applicable provisions of this Manual are in place and its supervision is being implemented in the true spirit of the intention. Persons of Indian Origin and Non-Resident Indians shall be excluded from such appointments. The CCSO will be responsible for framing internal security policies, Internal Audit, Training, Review and up-dation 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 be placed high in the hierarchy for reporting to derive the benefit of functional independence and to enforce Security norms without fear or favour.

2.2 **Responsibilities and Duties of CCSO**

(a) **Implementation of the security provisions as laid down in this Manual.**

(b) Keep himself fully conversant with all security instructions and ensuring that the security instructions are fully understood by all employees and are implemented or complied with, within their respective sections and offices.

(c) He shall be responsible for the proper conduct, discipline and performance of all the personnel in Security department.

(d) He shall also be responsible and ensure that fire service section in fully equipped and personnel are well trained. He shall take prompt action whenever necessity arises.

(e) He shall also be responsible for the duties of his subordinate staff and carry out any other lawful and reasonable orders issued to him by management.

(f) Be responsible for implementation of computer and information technology related security instructions within the company.

(g) Carrying out periodic surprise checks and maintain a record of such checks.

(h) Submitting a monthly security report to the CEO/Head of the sub-units/division of the company indicating lapses noticed by him.

(i) Arranging regular programmes to apprise the employees on security matters.
(j) Maintaining constant liaison with the nodal offices in Ministries.

(k) Carrying out improvement in the security system for the premises under his charge, as required, over and above the security manual.

(l) Arrange Internal & External Security Audits.

2.3 **Reports of Loss, Compromise or Suspected Compromise**

2.3.1 In order to prevent any security breaches following are to be completely avoided:-

(a) Employees carrying classified documents or materials to outside their offices without proper authority.

(b) Transmission of classified files, documents or materials from one building to another without proper security precautions.

(c) Leaving offices unattended, unlocked with classified files, papers or materials lying either on the office tables or in unlocked almirah or drawers.

(d) Carelessness in not observing the laid down instructions on photocopying/ duplication of classified documents and materials and subsequent accounting.

(e) Carelessness in storing data on various media like discs of a PC, floppies, magnetic tapes and other such means and carriage of floppies, CDs, Zip drives and laptops within Security Zone without proper authority or permission.

(f) Lack of proper accounting of Floppies, CDs, Zip drives/ Pen drives and proper safeguarding of data contained therein.

(g) Failure to weed out old and unwanted classified documents and lack of effort to keep the number of classified documents to bare minimum.

(h) Carelessness in not complying with instructions in the safeguarding of classified material and documents.

(i) Failure to immediately report incidents of breaches of security.
(j) Carrying of Cell phone in Security Zone without permission.

(k) Carrying waste paper without shredding them properly and not ensuring full destruction of waste papers.

(l) Non-depositing of office room keys with the guard rooms or leaving the room unlocked.

(m) Consumption of liquor or engaging in gambling within Security Zone.

(n) Detailing of staff after office hours without proper authorization and supervision by officers.

(o) Improper entry/ parking of private vehicles.

(p) Installation of internet connections without permission from competent office.

2.3.2 The Number of Internet Connections shall be controlled by the CSSO.

2.3.3 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 trace the culprit.

(d) To prevent recurrence and suggest remedial measures.

2.3.4 If classified information or materials have been compromised it is the duty of every employee to report immediately in writing to the CCSO. If a classified document or material is found in a wrong place, the finder should forward it to the CCSO and not to the person for whom it was meant. In every case where it is suspected that a leakage of information has taken place, unit head or concerned officers of the unit/division shall report the case immediately in writing to the CCSO. The loss of any document or material in office or in transit will be reported immediately in writing, with details, to the CCSO who shall then decide on the further course of action.

2.3.5 When cases of security violations are detected by the Security Staff, preliminary reports containing brief details of the lapse will be handed over by them to the defaulter immediately on occurrence. These will be followed
immediately by formal violation reports addressed to the head of the department. Replies on the security violations will be forwarded by all concerned offices within a week of initiation of violation reports. All Branches or Directorates Offices should keep the time factor in view and forward the replies indicating the following:-

(a) Circumstances leading to the violation of Security Instructions.
(b) Action taken or proposed to be taken against the defaulter.

2.3.6 In case an inquiry has been instituted, a tentative time frame by which it will be completed has to be provided. A fortnightly progress report shall be submitted to the office of the Company Chief Security Officer till the case is finalised.

2.4 Reporting Procedure

2.4.1 The ILDC shall at the earliest report in writing to the nearest office of IB regarding any information or materials in regard to actual, possible or probable espionage, sabotage, terrorism or subversive activities in any of the ILDC locations. A copy of the written report shall also be sent to IB.

2.4.2 The ILDC shall also report to the nearest office of IB any adverse information about any employee (s) which has come to his knowledge while performance of their role and responsibilities within the ILDC facilities.

2.4.3 The ILDC shall also report to the IB the following:-

(a) Unauthorised 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.
2.4.4 The ILDC shall forward to designated agency the reports as given below:

<table>
<thead>
<tr>
<th>Sl.No.</th>
<th>Periodicity</th>
<th>Title of Report</th>
<th>Report to be rendered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Monthly</td>
<td>Loss /recovery/ unearthed Arms and Ammunition and Explosives</td>
<td>Industrial Security Branch in IB</td>
</tr>
<tr>
<td>2</td>
<td>Monthly</td>
<td>Fire accidents &amp; other incidents / accidents</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Quarterly</td>
<td>Visits of foreign business visitors</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Half Yearly</td>
<td>Action taken report of IB visit</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Half Yearly</td>
<td>Internal Inspection Reports of Manufacturing Facilities</td>
<td></td>
</tr>
</tbody>
</table>

2.5 **Personnel Security**

2.5.1 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) Hacking of website
   (i) Unauthorized use of Pen Drive
   (ii) Unauthorized use of Internet Connection

2.5.2 It is necessary that all chances of an unreliable person dealing with classified documents and materials be eliminated. It is by strictly following certain
precautions that chances of leakage due to the above causes could be minimised. To achieve this objective, it is necessary to observe the precautions given below:

(a) All personnel employed for the plant should undergo a diligent security check (including all levels of management). There should be a periodic check and review of all personnel employed in the plant. This could be at pre-determined intervals and should cover immediate family members as well. The help of security agencies should be incorporated if required.

(b) Character and antecedent verification has to be carried out for all persons before joining the ILDC

i. Police clearance shall be obtained for all employees.

ii. Reference checks shall be carried out with persons of repute known to the candidate. Also previous employment verification shall be carried out.

(c) Thorough verification of character and antecedents of persons to be employed to deal with classified matters shall be made before his employment.

(d) All officers should abide by the provisions laid down in the Official Secrets Act 1923 and give a declaration to that effect.

(e) 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 IB, and also every two years thereafter.

(f) Temporary transfers to a SECRET Section shall generally be avoided. In rare cases, when such a transfer becomes unavoidable only those persons, whose antecedents have been verified, as above, shall be transferred to such sections.

(g) Only permanent employees shall be posted in TOP SECRET and in SECRET sections to deal with classified documents.

(h) Police verification shall also be carried out in respect of Contract Engineers who are taken on various projects.

(i) 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 designated agency in MHA every quarter. The licensee shall define the code of conduct of such persons.

2.5.3 It is the duty of every employee of the company to keep a close watch on the behaviour of every employee dealing with classified documents and materials and, any behaviour which gives the slightest indication of suspicious conduct shall be looked into and if there is any substance in the suspicion, it should be brought promptly to the notice of the CCSO who shall take further follow up action in the matter.

2.5.4 Such suspicious behaviour may include staying in offices at odd hours, making a copies of documents, inquisitiveness about matters with which the person is not directly concerned, frequent unauthorised absence from the office, absence on leave at certain regular intervals or on fixed days, bad habits, drunkenness and living beyond means. It must be understood that weakness in character often induces a person to barter official SECRETS for money or other considerations.

2.5.5 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 of any of his subordinates and suitably caution the officer against such lapses.

2.5.6 Personnel security is of the highest importance. If a person dealing with classified information and materials is completely reliable in every respect, then the chances of leakage shall be minimised to a great extent. Therefore, before employing anyone in a classified section, it must be established beyond doubt that he/she is careful, attentive and serious in his work and is a person of good character and is reliable in every way.
CHAPTER - 3
Document and Material Security

3.1 Security Classification of Documents and Materials

3.1.1 Need and Responsibility for Security Classification. To safeguard official information, documents and materials must be examined and graded into proper categories so that they may be recognized and accorded proper importance during handling.

3.1.2 Classification of Documents and Materials. Documents and Materials shall be classified as follows:-

(a) TOP SECRET
(b) SECRET
(c) CONFIDENTIAL
(d) RESTRICTED

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

3.1.3 TOP SECRET. “TOP SECRET” shall be applied to information and material, 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.

3.1.4 SECRET. “SECRET” shall be applied to information and material, 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.

3.1.5 CONFIDENTIAL. “CONFIDENTIAL” shall be applied to information and material, 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.

3.1.6 Restricted. “Restricted” shall be applied to information and material which is essentially meant for official use only and which should not be published or communicated, to anyone except for official purpose.

3.1.7 UNCLASSIFIED. The designation UNCLASSIFIED is used to identify information and material that does not require a security classification.
3.2 Guidelines on Classification.

3.2.1 There is a general tendency to give a document or material a higher security classification than it deserves. This imposes on every one, who handles such a document, the burden of taking various precautions which in fact may not be necessary, judged from the contents of the document or material. At the same time fixing too low a classification may cause disclosure of the contents of the document and this may jeopardise national interests. Therefore, great care must be taken in accordance with security classification to documents and materials.

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

3.2.3 The document or material 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.

3.2.4 An extract from a paper having a higher classification may be given a downgrading. In this extract, a reference may be made to the original letter by quoting its number without mentioning the subject, i.e., without in anyway disclosing the nature of the original document.

3.3 Marking of Classified Documents and Materials. The classified documents and materials shall be prepared and marked as per the guidelines described below, as applicable, in the following manner:

3.3.1 All documents including noting portion 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. The security grading will be underlined except when it is stamped. In the case of documents in book form, whether they be securely bound or not, the front and back outer covers will also be marked, as stated above. Any insertions, such as maps, or illustrations of an individually classified nature will also be similarly marked.

Files, folders, binders, envelopes, and other items containing classified documents, when not in secure storage, shall be conspicuously marked with the highest classification of any classified item included in the group. Cover sheets may be used for this purpose.
Similar procedures shall be followed for classified materials.

3.3.2 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. This needs to be done only on the outer side of the covers. “TOP SECRET” files/documents will be maintained as under:

(a) Subject-wise TOP SECRET part case files would be maintained having only such enclosures as have been actually classified as TOP SECRET.

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

(c) The part case files will be properly docketed. All part files on the same subject should be amalgamated after action is completed in each such case and the entire file on the same subject re-page numbered and proper entries made against the concerned part files in the register maintained for the purpose.

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

3.3.4 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.

3.3.5 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.

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

3.3.7 Marking Wholly Unclassified Material. Normally, wholly UNCLASSIFIED material will not be marked or stamped UNCLASSIFIED unless it is essential to convey to a recipient of such material that (a) the material has been examined specifically with a view to impose a security classification and has been determined not to require classification; or (b) the material has been reviewed and has been determined to no longer require classification and it is declassified.

3.3.8 Marking for ILDC Developed Information and Materials. 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. If the information was not previously classified, but the ILDC believes the information may or should be classified, the ILDC should protect the information as though classified at the appropriate level.

3.4 Accounting of Classified Documents and Materials

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

3.4.2 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. Under this 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 the document has not reached the destination, the Head of the office concerned shall immediately report the matter to CCSO. Wherever possible classified documents shall be hand delivered to the recipient.

(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 should also note the number of copies made.

(f) In normal circumstances, a TOP SECRET document shall not be further copied by the addressee. However, in certain rare situations, it might become necessary to have a certain number of additional copies prepared for simultaneous examination. In such circumstances, additional copies of a TOP SECRET document may be made after
obtaining order in writing from the CEO/CMD/Chairman of the ILDC. It is, however very essential that the originator be informed immediately of this requirement and of the distribution of the copies made, serial number wise.

3.5 **List of Documents, Checks and Annual Accounting.**

3.5.1 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.

3.5.2 Two security inspections 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. During these inspections a physical verification of all the classified files and materials shall be carried out.

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

3.5.4 A separate Diary and Despatch book shall be maintained for TOP SECRET and other classified correspondence.

3.5.5 A register of classified publications or books shall be maintained in which particulars of receipt, issue, including loan issue and disposal will be entered. Separate pages may be allotted for each category of classified publications.

3.5.6 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.

3.5.7 **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 to ensure that all classified material and security repositories have been appropriately secured.

b) ILDCs that operate multiple work shifts shall perform the security checks at the end of the last working shift in which classified material was removed from storage for use. The checks are not required during continuous 24-hour operations.
3.6 Care and Custody of Classified Documents and Materials; Responsibility of Holders

3.6.1 All categories of classified documents and materials 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. Such document and material is passed on by him to another individual authorized to deal with it and the transfer is duly recorded only when the receipt is obtained.

3.6.2 Other Classified Documents and Materials 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.

3.6.3 Individuals in charge of Classified Documents and Materials are responsible for their safe custody and their disclosure is limited to only those, who are directly concerned with the documents and materials in their performance of duty.

3.6.4 Classified Documents and Materials are normally entrusted to the holders of specific appointments, for the better performance of their duties, rather than to named individuals.

3.6.5 When an individual who has charge of any Classified Documents and Materials is about to vacate his appointment, whether on transfer or on retirement or otherwise, he will hand over both the list and the documents and materials to his successor or his superior officer after obtaining the necessary receipt.

3.6.6 Should it be necessary to transfer a registered document or material from one office to another, a proper handing over certificate must be obtained under intimation to the issuing authority.

3.7 Care of Classified Documents and Materials

3.7.1 The holders of classified documents will ensure that lists of classified documents are kept and checks carried out periodically. Accountable documents will be recorded in separate registers as this will facilitate the periodical checking and rendering of necessary certificates.

3.7.2 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.

3.7.3 If instructed to take TOP SECRET documents from one place to another, individuals must carry them in securely fastened boxes or bags duly locked,
which must always be in their possession and must NEVER be left unattended.

3.7.4 When an individual is the sole occupant of a room and during working hours, leaves the room for a short period, he must ensure that all TOP SECRET documents are locked in safes or cupboards. Other documents may be left unlocked provided the room is locked and the key is with him. If a room is occupied by more than one individual, the individual leaving the room will ensure that all classified documents are locked properly. Before closing the room for the day, it will be ensured that all classified files or documents are securely locked in.

3.7.5 Classified papers should not be left lying about in the absence of the person in whose charge these are held. He must ensure that whenever he leaves his desk for any purpose and duration, including lunch hours, all classified documents are locked in safes or boxes or cupboards of which the keys must be with him and the room should be locked. Security of other documents should be safeguarded during lunch intervals by locking the rooms.

3.7.6 Similar procedures shall be carried out in respect of classified materials.

3.8 **Custody of Classified Documents and Materials**

ILDC authorized to store classified documents and materials shall establish and maintain a system to deter and detect unauthorized introduction or removal of classified documents and materials from their facility. The objective is to discourage the introduction or removal of classified material without proper authority. If the unauthorized introduction or removal of classified material can be reasonably foreclosed through technical means, which are encouraged, no further controls are necessary. Personnel who have a legitimate need to remove or transport classified material should be provided appropriate authorization for passing through designated entry/exit points.

3.8.1 Classified documents except those marked Restricted should be kept in any steel safes or almirahs or cupboards. Restricted documents may be kept in any secure place to which the public do not have access.

3.8.2 Greatest care shall be taken to ensure that safes or other receptacles used for similar purposes are securely locked when not in use. 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 to its fullest extent and locked immediately and all
locks provided will be used and no safeguard will be relaxed on the
ground that temporarily the safe is vacant or its contents
unimportant.

(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.

(d) When the keys of any receptacle (including record of the combination
for a dial lock) is lost, missing or believed to be compromised, the
incident will be reported forthwith as in the case of classified
documents.

(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 recognised, and will be
handled according to the highest category of document contained in
the safe.

3.8.3 **Notebooks, Laptops, PCs or Electronic Recording Media etc.** 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, floppies and zip drives etc. If used,
these will be handled as per the security classification of data contained therein.

3.8.4 **Segregation and Care of SECRET Section.** Any branch/ department or section
which has to deal generally with classified documents in substantial measure
must provide for complete segregation of 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. In case of loss or misplacement of a key in
such section the entire locking system shall be replaced. This procedure must
be followed even when the keys were missing for some time and found
subsequently and it is not possible to establish beyond doubt that there was
no opportunity for any unauthorised person to make a duplicate key.

3.8.5 **Static Protective Arrangements.** 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.

3.8.6 **Guarding - Provision for Lighting.** There must be provision of adequate guards both by day and by night to prevent the entry of unauthorised persons. The officer in charge of such a section shall ensure that only authorised persons have legitimate access to his section. If a paper is brought by a person not himself authorised 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. Lighting arrangements both inside the Section dealing with classified documents and in the corridors approaching should be adequate.

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

(b) **SECRET or Classified Documents.** Whenever SECRET or classified documents are required to be photocopied or cyckostyled, it should be done under the supervision of the signatory officer or by an officer nominated by him.

(c) The officer supervising the above cyckostyling work will ensure that no additional copies are made and extra copies or stencil paper or carbon copies are destroyed in his presence.

3.8.8 **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.
3.8.9 Opening and Diarising 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) Diarising.

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

3.8.10 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 despatch clearly written. The time of despatch would also be
indicated in the despatch register. The receiver shall scrutinise 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) Restricted documents may be sent in single envelope.

(iv) 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 despatched by civil post.

(v) 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.

(vi) Classified materials 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) Envelopes containing RESTRICTED documents may be sealed with economy slips, which will be impressed with the originator’s stamp, so that part of the stamp is on the economy slip and part is on the envelope.

(iii) 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.

(iv) Only official seals shall be used to make impression on the wax used for sealing.
(c) **Movement of Classified Documents and Materials**

(i) **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 authorised 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 not below Section Officer or equivalent. CONFIDENTIAL files or documents may be transmitted through any member of the staff entrusted to deal with it.

(ii) **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 authorised courier and not through peons or registry. Such despatch shall be carried out only after ascertaining the availability of the addressee(s) in the office. If the carriage involves movement in public area Journey shall be undertaken only in an authorised transport and not in a public transport. Wherever feasible, a second person shall also be nominated to accompany the courier. TOP SECRET document will be accompanied by two acknowledgement slips. First acknowledgement slip will be attached to the inner sealed cover while the second acknowledgement slip will be contained within the inner sealed cover attached to the TOP SECRET papers. First acknowledgement slip will be signed by the personal staff of the officer whereas second acknowledgement slip will be signed by the officer to whom the TOP SECRET document has been addressed. In order to avoid delay in the receipt of acknowledgement slips, these will preferably be returned by the addressee through the same courier to the originator. If, due to unavoidable reasons second acknowledgement slip cannot be returned through the courier, the addressee is responsible to ensure that it is received by the originator within 48 hours. Other important aspects in this regard would include – sealing the inner cover in the presence of the originator, maintaining a separate movement register for TOP SECRET documents which should contain the time and date of despatch of the TOP SECRET cover and the time and date of the acknowledgment by the personal staff as well as the recipient officer respectively and institution of a system of
regular as well as spot checks by all offices, departments and sections to ensure that these procedures are being adhered.

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

(iv) 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.

(v) 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.

(vi) In rare cases only duplicate key be handed over to the person with the following additional precautions being taken - The duplicate key shall be handed over to the peon carrying mail in a sealed cover. In the event of more than one addressee, the key shall be re-sealed by subsequent addressee(s) also before handing it over to the peon and loose or open letters shall not be kept in the Mail Box or Bag in case duplicate key is being handed over to the peon carrying the mail.

(vii) 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.

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

(ix) Similar care shall be taken in the movement of classified materials.
(d) Carrying Classified Documents or Materials to Residence or Outside Office. Carrying of classified documents and materials to residence of officers is prohibited.

(e) Transmission of Classified Documents to Outstations within India. Classified documents will be despatched 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 despatched 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 Interdepartmental and Other Meetings. Instructions on preparation, handling and custody of documents/papers including computer storage media such as floppies, CDs, Pen Drives, given in this chapter will apply equally to such information. 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 authorised officers will carry such papers/documents for the meeting. These documents will not be carried to residence except where permitted.

3.9 Emergency Procedures. ILDCs shall develop procedures for safeguarding classified material 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 material.

3.10 Disclosure

3.10.1 General. ILDCs shall ensure that classified information is disclosed only to authorised persons.

3.10.2 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 fulfillment of a classified contract or subcontract.

3.10.3 Disclosure to Subcontractors. ILDCs are authorized to disclose classified information to a subcontractor when access is necessary for the performance of tasks or services essential to the fulfillment of a prime contract or a subcontract. Prior authorisation shall be obtained by the ILDC in writing from the Government Agency having classification jurisdiction over the information involved for this purpose.

3.10.4 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 3.10.3 for subcontractors.

3.10.5 Disclosure in an MFO. Disclosure of classified information between facilities of the MFO shall be accomplished in the same manner as prescribed in 3.10.2 for employees.
3.10.6 Disclosure of Classified Information to Other Persons. ILDCs shall not disclose classified information to other persons unless release of the information is authorized in writing by the Government Agency having classification jurisdiction over the information involved.

3.10.7 Disclosure to Other ILDCs. ILDCs shall not disclose classified information to another ILDC except in furtherance of a contract or a subcontract, and only with prior approval of the authority that has original jurisdiction over that information.

3.10.8 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.

3.10.9 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.

3.11 Down Grading, Disposal and Destruction of Documents

3.11.1 All organisations, 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.

3.11.2 Downgrading. No classified documents shall be downgraded without authorisation.

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.

3.11.3 Upgrading Action. When a notice is received to upgrade material to a higher level, for example from CONFIDENTIAL to SECRET, the new markings shall be
immediately entered on the material 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 material. Other holders shall be notified as appropriate if further dissemination of the material has been made by the ILDC.

3.11.3 **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.

3.11.4 **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. Documents other than classified may be destroyed at the discretion of the head of the office concerned.

3.11.5 A record will be kept of all graded documents and materials destroyed. For destruction of classified documents, the following method should be followed:

(a) All classified papers will be shredded to a size not exceeding 1.9 mm x 13 mm and cross cut.

(b) All TOP SECRET documents including the shredded ones will be destroyed either by burning or any other means inside the security premises under the personal supervision of the officer holding these documents on his charge.

(c) All SECRET documents including the shredded ones will be destroyed either by burning or any other means under the supervision of an officer.

(d) Other Classified documents or material shall be destroyed under the supervision of a Section Officer.

(e) 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.

(f) 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 unauthorised persons.

3.11.6 **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 materials. 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 kept in these rooms will be under the charge of an official not below the rank of Section Officer/Assistant.

(d) 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.

(e) Annual physical verification of the documents should be carried out by the Officer-in-Charge and report of the same be furnished to the Head of the Department concerned.
CHAPTER 4

Communication Security

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

4.2 Telephones.

4.2.1 No form of telephonic conversation, including intercom PAX or RAX 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) To prevent misuse, telephones, especially RAX, should be kept locked when the officer is away from his office.

(d) Cordless phones will not be used.

(e) 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.

(f) 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.

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

(h) Telephone conversation is totally unsafe; thus if at all classified information has to be passed on phone, proper secrecy device should be used.
(i) All telephones should have the facility to identify the telephone number of the caller i.e. they should be provided with a caller ID facility.

4.3 Cell or Mobile Phones

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

4.3.2 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’s enable monitoring of Communication from briefcase sized equipment. A number of Indian vendors are marketing GSM monitoring systems. Due to its 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.

4.3.3 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.

4.4 Telex, Teleprinter and FAX communications. Telex, Teleprinter and FAX communications are also vulnerable to interception or leakage, e.g. across connection. It is, therefore, necessary to identify the party end before transmitting a message. Enciphering devices, if available, should be made use of at both the ends of Teleprinter communication. 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.
4.4.1 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 authorised to despatch the Fax.
CHAPTER 5
Computer and Cyber Security

5.1 General

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 integrity to ensure the availability of the data and system.

Protection requires a balanced approach 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.

ILDC management should appoint Information Security Officer with clearly defined 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.

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’s, 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) Accidental/Intentional cross connection between the Organisation Local Area Network and Internet.

(d) Spoofing by intruders.

(e) Defacing of various Websites by anonymous Hackers.
5.2 ISO 27001 Compliance:

The companies shall have ISO27001 compliant but certification is not necessary. Appropriate controls shall be implemented to accommodate the guidelines given in this manual.

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).

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

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 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.

This International standard adopts the “Plan-Do-Check-Act” (PDCA) model, which is applied to structure all ISMS processes.

Compliance to 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.
5.3 Common Requirements:

(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 (CAI) confidentiality, integrity or availability. 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.,

(f) Control and audit logs should be available in centralised systems/applications for Successive Logon Attempts, Multiple Logon Control, Session termination and User Inactivity etc.,

(g) 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.

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

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

(j) 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.

(k) Centralised Anti Virus management solution should be in place for effective implementation of Anti Virus solution.

(l) System should be in place for internal incident management as well as for implementation of time to time necessary guidelines / measures from CERT-India; and should be able to detect any violations to existing policies and ensure updating IT infrastructure.

5.4 **Enterprise Resource Planning (ERP)** should be implemented, system which integrates internal and external management information across an 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.

5.5 **Physical and Software Security.**

5.5.1 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 unauthorised access and software and data from intentional, accidental or environmental corruption must be ensured at all costs. This should be ensured by:-

(a) Restricting access to the computer by:-

(i) Properly guarding the rooms where computers are used.

(ii) Providing hardware locks to the computer rooms.

(iii) Taking anti-theft precautions.

(iv) Allowing entry to the computer room only to authorised persons holding proper identity cards or passes.

(b) Safeguarding the computer storage media, software, sensitive and proprietary data by:-
(i) Safekeeping of computer storage media, (floppies, CDs, magnetic tapes, hard disk, USB drives etc).

(ii) Shredding or secure disposal of console logs or printouts, used printer ribbons & carbons, damaged floppies, tapes and hard disks etc.

(c) Protection of Switches/Routers and other connectivity devices.

5.5.2 Adequate protection is required both for the operating system software and application software. In order to prevent unauthorised 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 authorised 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.

5.6 **Acquisition of Computer hardware and Software**

5.6.1 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.

5.6.2 If development of software application is outsourced, antecedents of the personnel/company developing the software should be verified. 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.

5.6.3 The firms, which are offering AMC, should be positively vetted by CCSO (with help from MoD/IB is 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.
5.6.4 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.

5.6.5 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.

5.7 Threats To and Vulnerability of Computerised Information, Virus Menace and Countermeasures

5.7.1 Computer systems and data without adequate access controls are vulnerable to a variety of threats including theft, fraud and vandalism. Potential losses range from use of computing time to unauthorised access, modifications or destruction of valuable data. The ramifications of such actions may range from trivial to catastrophic, if not checked on time. Technique that can be used to control the access to data is the authorization of a particular user to 'READ' 'WRITE' 'APPEND' and/or 'EXECUTE' a particular file stored on the computer.

5.7.2 Protection from Virus. Viruses are malicious programmes, when active, lead to hardware failure or system failure which requires re-booting etc. The most common sources of these viruses are through pirated or gifted software. Some common precautions for preventing or containing viruses are:-

(a) Use 'write protection' in floppies, CDs, Pen Drives and cartridge tapes, wherever possible.

(b) In case of software developed in-house, establish a stringent system of logs indicating when changes in the code were made and nature of change.
(c) Take regular backups on floppies, CDs, DVDs, Tapes etc. as appropriate.

(d) Do not open email attachments from unknown sources or unsolicited emails. If emails from known sender contain attachments, confirm from sender or open only if explicitly called for.

(e) Do not transfer infected or even suspected data from one system to another.

(f) Use antivirus software to safeguard the system and data from virus and keep the anti-virus software always updated.

(g) Antivirus software must be configured to scan all storage media on access and to carry out scheduled scans of all drives at least once a day.

(h) Proper Patch Management solution should be in place for updation of Operating System (OS) and Security patches.

5.7.3 Password

(a) Every computer/terminal should be protected with multilevel password. Each level should have different password.

(b) A password should have at least 8 characters and be a combination of upper and lower case alphabets, numerals and special characters to make it complex.

(c) Password should be changed periodically at least once a fortnight, and not be shared with any unauthorised person.

(d) Apply the following tests to create strong password:-

(i) Strength Test. Is the Password as strong (in length and content) as the rules prescribe?

(ii) Unique Test. Is the Password unique and unrelated to your profile or other password?

(iii) Practical Test. Can you remember it without having to write down?

(iv) Recent Test. Have you changed it recently as prescribed?
5.7.4 Access Control.

(a) Computers used for classified application should have additional level of security by installing effective Access Control system.

(b) When a computer is used as stand-alone, it should not be provided with the Network and Communication ports.

(c) Appropriate software tools like Device lock may be installed to disable USB ports, Parallel Ports, Floppy Drives and other removable Drives. Such Ports/Drives should be disabled. Record of such activity should be maintained.

(d) As a general rule, no computer utilised for classified application should be provided with internal Combo Drives (CD/DVP Reader plus writer or CD/DVD write should be used on need basis on specific authorisation by the controlling Officer in writing. Such drives should be kept in safe custody under lock and key, when not used.

(e) The Real time Clock of the Information System devices (Computers, Servers, Network devices and Network Security devices etc.,) should be set accurately to ensure the accuracy of the audit-logs, which may be required for analysing breach of security.

(f) The Real time Clock of the Computers or Communication Device should be set to Indian Standard time. There should be a procedure to check and correct drift in the Real time Clock.

(g) In a networked scenario all unused ports of the switch should be disabled.

(h) Use of proper Network access control mechanism to disallow connecting unauthorised devices to network.

5.7.5 Safe Storage of Classified/Sensitive Data.

(a) A suitable encryption package for storing TOP SECRET/Highly Sensitive Data in Computer Storage Media (excluding hard disk) may be identified and used, as necessary.

(b) The removable hard Disk and the Computer Media containing encryption/decryption algorithm, if used, should be kept at a highly secured place, as applicable to paper based files of similar
classification. The source keys/ program for encryption/decryption should be kept in a separate media and cabinet.

(c) Copying of the data from Computer Storage Media should be done under proper authorisation by supervisory officer in charge of the section/branch/unit.

(d) When a file is deleted its contents are not actually erased from the Computer Storage Media. With appropriate tools the contents can be retrieved. To reduce this security risk, the file contains classified data may be overwritten several times with the junk Data. (To mitigate the security risk associated with it, the media to be wiped to the level the data cannot be retrieved)

(e) Computer Storage Media with Read only facility like CDR/DVDR, used for Classified work should be kept in safe custody. It is recommended to destroy those, when not required, by following the set procedures.

5.7.6 Miscellaneous Aspects

5.7.6.1 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 verifications of critically placed functionaries of the computer system handling sensitive information by CCSO (with help from MoD/IB is so required) in addition to the verification done by the civil police.

(c) In-house sensitisation and periodical briefing of concerned personnel of various departments regarding computer security.

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

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

5.7.6.2 Cataloguing of Floppies and CDs. The Floppies, CDs (RW), Cartridge Tapes, Pen drives (USB sticks) used should be serially numbered with name of the concerned written in indelible ink. A register should be maintained 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.

5.7.6.3 Pen Drives / USB Sticks. Use of pen drives 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 pen drives within the classified zones/areas. Pen drives will be issued only to such individuals who possess the permission by name and it will be in their personal charge. Procurement of pen drives where considered essential will be done centrally by the CCSO with written approval of the CEO/Chairman/CMD. All instructions relating to classified documents contained in this Manual are equally applicable to pen drives. Carriage of pen drives 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 monthly 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 within the classified area/zone. Loss of Pen 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.

5.7.6.4 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/thump drive/hard disk/palmtop/Electronic Notebook and mobile phones with Bluetooth/GPRS 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 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.

5.7.6.5 Personnel travelling with Laptop holding classified data for presentations or discussions outside office premises should take following steps:-

(a) Put a secure lock on the hard disc of Laptop to prevent unauthorised access.

(b) Ensure physical security of the Laptop.

(c) After the presentation is completed the data should be completely erased from the hard disc in such a way that it would not be retrieved in any manner.

(d) Ensure that no TOP SECRET files are stored in the Laptop while carrying the same to residence.

(e) Desktop encryption software should be used to protect the data from unauthorized access.

(f) Encryption software should be used for USB pen drive and all removable drives.

5.7.6.6 **Scanners.** All scanners will remain in the physical custody of their owners preferably an officer and record of classified documents scanned should be kept.

5.7.6.7 **Destruction and Weeding.**

(a) Damaged and unusable floppies/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.
(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, pulverisation and smelting etc.

5.7.6.8 Computer Security Audit.

(a) An officer should be designated as Computer Security officer (CSO) who will supervise all computer security measures within his offices/branches/section. The CSO shall not be a foreign citizen, or a Person of Indian Origin, or a Non-Resident Indian.

(b) Periodic security audit of the computers should be carried out to ensure that the laid down guidelines are strictly followed.

(c) 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.

5.8 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 floppies, 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 floppies, 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 strips 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 floppies, 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 floppies 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 over or taking over between the shift-in-charge.

(xix) Damaged and unusable floppies, 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 of DHQ Security Zone will be password protected and prior permission of security office is obtained.

(xxiv) Some PCs like HCL computers 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 unauthorised personnel.

(xxvii) **Cyber Hygiene.** Maintenance of good hygiene in the cyber world is as relevant as in our personal hygiene. Aspects of good passwords, file management etc have been comprehensively covered, though systematic and periodic maintenance of individual computers and network devices be ensured.
(xxviii) Internet PC, as should be periodically updated for - as patches released by OEM, Live updates for anti-virus/Anti spy ware and Portable storage media used on internet machine to be scanned for spyware, Trojan and another suspicious malware before being used on LAN.

(b) **DON'Ts.**

(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 floppies 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 or floppies 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 or floppies outside the office building. In case a data floppy has to be taken outside the office building, its movement will be with the 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 floppies or 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.

5.9 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. Unauthorised and 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 CCSO. Internet connectivity should be provided to the offices only on a stand-alone PC. The Internet PC should not be used for office work. Modems will not be connected to any PC other than the Internet PC. 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. Official Laptop where permitted should not be allowed to the Internet Room to the network or for any other purpose. No classified office work will be done in Internet computers.
CHAPTER – 6
Security of Premises and Physical Security Measures

6.1 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.

6.2 Declaration of facilities as Prohibited Place: All defence related establishments automatically fall under category of ‘Prohibited Place’ under the Official Secret Act, 1923.

6.3 Layout of Premises:

a. Perimeter walls and limited ‘entry’ / ‘exit’ points are essential requirements of security.

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

c. The Reception shall be conveniently situated near the main entrance so as to provide clear access to visitors without entering the factory premises.

d. The office of the Chief of Security of the Unit shall be situated near the reception.

e. All Secure / Sensitive / Manufacturing / Storage facilities shall be inside the main gate, with necessary additional security measures as prescribed.

f. Main entry gate shall have search bays.

g. Separate gates shall be provided for entry and exit of materials.

h. Parking shall be outside the main entry and sufficiently away from the main facility inside the outer perimeter boundary.

6.4 Setting up of Plant Security Council: A Council to be constituted under the chairmanship of Head of Unit with CCSO as member Secretary & other divisional heads as members. The Council shall meet monthly and to review the existing security requirements/arrangements and take corrective actions.

6.5 Perimetric, Access Control and Security Personnel: The private sector defence companies shall comply with perimetric, Access Control systems and Security requirement as per details given below:

<table>
<thead>
<tr>
<th>Category</th>
<th>Head</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perimetric and</td>
<td>Physical Security on</td>
<td>Single wall (12 feet) with barbed wire fencing and track upfront.</td>
</tr>
<tr>
<td>Access</td>
<td>the perimeter</td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td></td>
<td>Depending upon the layout of the plot adequate watch tower(s) with spot lights day and night cameras for</td>
</tr>
</tbody>
</table>
| Security Personnel | Monitoring, 2X Watch Towers with Spot Light.  
Night Cameras fitted on Perimeter Walls  
Communication equipments for linking with control station and provision for raising an alarm by using sirens or loud hailers |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Perimeter Control</td>
<td>Perimeter and entry/exit points lighting and video streaming by surveillance cameras to Control Room.</td>
</tr>
<tr>
<td>Surveillance &amp; Monitoring</td>
<td>24X7 Video Monitoring, Recording and Archival. Failsafe Standby arrangements for continuous recording in case of power failure or breakdown of main equipments. Provision of UPS for Power Failure</td>
</tr>
<tr>
<td>Access Control</td>
<td>Biometric access control to each room of each building/workshop areas with intruder alarm with data logs of Access</td>
</tr>
<tr>
<td>Control Centre</td>
<td>Control Room with monitoring, recording for 30 days and replaying facility. Access control monitoring and card management. Communication to Management and Responders Visitor control with monitoring of all visitor activities within the plant</td>
</tr>
<tr>
<td>Material</td>
<td>Automatic Vehicle and Baggage Scanners</td>
</tr>
</tbody>
</table>
| Security Personnel | Company Chief Security Officer reporting to MD  
Perimeter Patrol  
Quick Response Team (trained) including Fire Fighting  
Entry/Exit gates (DFMD & Hand Held Detectors & manual I-Card checking) |
6.6 **Identity Documents, Entry Points and Parking of Vehicles.**

6.6.1 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 of the employee  
c) Staff Number  
d) Photograph  
e) Signature of issuing authority  
f) Blood group  
g) Date of issue and validity  
h) Machine Serial no.  
i) Signature of employee  
j) Address of Unit

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 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 is not allowed.

(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 further follow up action.