CISO Instruction No. 2
Dated: November 27, 2020

F. No. 500/62/2015-FTTR-III
Government of India
Ministry of Finance
Department of Revenue
Central Board of Direct Taxes
(Foreign Tax & Tax Research Division)

To: Cadre Controlling Pr. CCsIT/Pr. DGsIT/CCsIT/DGsIT

Subject: Information Security Policy of Income-tax Department – reg

The tax administration is obliged to keep the information submitted by the taxpayers including their sensitive financial and personal information confidential and is required to take steps to ensure that they are not disclosed inappropriately, either intentionally or by accident. Maintaining the confidentiality of taxpayers' information has assumed a greater significance in view of increased availability of information in respect of offshore tax evasion, tax avoidance and stashing of unaccounted money abroad. The information in respect of such tax avoidance/evasion is often located outside the territorial jurisdiction and is obtained only through bilateral and multilateral cooperation amongst countries/jurisdictions.

2. The Government of India has played an important role on international forums in developing international consensus for such cooperation as per globally accepted norms. The exchange of information under the tax agreements is however contingent upon strict adherence to the norms of confidentiality as enshrined in the agreements. It is, therefore, essential that for continued assistance by the treaty partners of India, the information received is kept confidential and is used and disclosed strictly as per the terms of the Agreement.

3. An Information Security Committee (ISC) had been constituted in the Central Board of Direct Taxes (CBDT) under the chairmanship of Member (in-charge FT&TR) with a view to putting in place a robust Information Security Mechanism in the Department. The ISC consists of a Chief Information Security Officer (CISO) and other members from the FT&TR Division, TPL Division, Investigation Division of CBDT and Directorates of Systems and I&CI. The policies and protocols formulated by the ISC is implemented at the regional levels by the Local Information Security Committee (LISC) headed by the CIT(Admin & TPS) in the office of the concerned Pr. CCIT.

4. The CISO Instruction No.1 dated 10th July, 2015 has been the overarching policy document with respect to Information Security management in the Department. However, a need was felt to review the policy keeping in mind the changes processed within the Department. In view of this a revised Information Security Policy for the Income-tax Department has been approved by the Information Security Committee and Chairman, CBDT.

5. The **Income Tax Department (ITD) Information Security Policy** (hereafter referred to as 'Policy'), has been designed to address and manage both internal and external information security risks to

27-11-2020

the Income Tax Department. It will assist the Department in protecting the confidentiality, integrity and availability of data. The policy document is divided into the following chapters:

- Introduction
- Organization of Information Security
- Risk Management
- Human Resources Security
- Asset Management
- Access Control
- Operations Security
- Communication Security
- Security in development and support processes
- Supplier relationships
- Physical & Environmental Security
- Cryptography
- Information Security Incident Management
- Information security aspects of business continuity management
- Compliance

6. Income Tax Department provides computer devices, networks, and other electronic information systems to meet missions, goals and initiatives. All users must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. An **Acceptable Usage Policy** has been formulated to establish guidelines for acceptable and unacceptable use of assets of Income Tax Department. This policy applies to all End Users (Income Tax Department employees, contractors, consultants, third parties and their affiliates) having access to Income Tax Department resources.

7. The Income Tax Department (ITD) Information Security Policy and Acceptable Usage Policy document is circulated herewith for adoption by all offices under your charge. The Local Information Security Committees are to ensure the implementation of the policies outlined in the Policy document.

27-11-2020

(Rakesh Gupta)
Chief Information Security Officer, CBDT cum
CIT (C&S), CBDT

(राकेश गुप्ता) / (Rakesh Gupta)
आयकर आयुक्त (समन्वय और प्रणाली)
CIT (Coord & System)
के. प्र. कर बोर्ड / CBDT
वित्त मंत्रालय (राजस्व विभाग)
Ministry of Finance (Deptt. of Rev.)
भारत सरकार / Govt. of India
नई दिल्ली / New Delhi

Encl: 1. Income Tax Department (ITD) Information Security Policy document
2. Acceptable Usage Policy

INCOME TAX DEPARTMENT

GOVERNMENT OF INDIA

ITD Information Security Policy 2020

Contents

1 Introduction

1.1 Income Tax Department

1.1.1 The Income Tax Department (ITD) is a government agency undertaking direct tax collection of the Government of India. Income Tax Department is headed by the apex body Central Board of Direct Taxes (CBDT). The Central Board of Direct Taxes (CBDT) is a part of Department of Revenue in the Ministry of Finance. The CBDT provides inputs for policy and planning of direct taxes in India, and is also responsible for administration of direct tax laws through the ITD.

1.1.2 The field offices of Income Tax Department carry out duties assigned by CBDT. The Directorates are attached offices of CBDT which take responsibility of specialized functions in CBDT.

1.2 About the Document

1.2.1 The document, ITD Information Security Policy (hereafter referred to as 'Policy'), is designed to address and manage both internal and external information security risks to the ITD. It will assist ITD in protecting the confidentiality, integrity and availability of data. The Policy is intended to be a living document and will continue to be updated and improved as information security threats evolve further and become more sophisticated and/or if there are changes in the current IT landscape.

1.2.2 This policy outlines a high level security reference and should be viewed as a guiding document for developing specific security procedures and associated documents as per the requirements of individual offices. The policy needs to be adopted by all offices, irrespective of size, degree of information security risk or sophistication of its operations.

1.2.3 The Chief Information Security Officer (CISO) shall distribute this document to all employees as an information security guide and reference.

1.2.4 The relevant provisions of this policy will form a part of the contract of all third party vendors as an enclosure to their contracts at the time of signing contracts and also as and when it is updated.

1.3 Scope and Applicability

1.3.1 This policy is applicable to all offices functioning under Principal Chief Commissioners of Income-tax (CCA) in various regions as well as the offices working under the attached directorates of CBDT.

1.3.2 This policy applies to all Information assets of the Department, irrespective of where the information assets are hosted.

1.3.3 ITD employees, contractors, third party staff or any other partners who are directly or indirectly a part of ITD and have access to ITD information or information processing facilities shall adhere to this policy and ensure compliance.

1.3.4 This policy would apply in conjunction to the CISO Instruction No. 1 dated 10th July, 2015 of CBDT, MHA guidelines on information security and other applicable information security policies and laws.

1.4 Exception Management

1.4.1 All exceptions to the Policy shall be duly approved by CISO.

1.5 Terminology

For the purposes of this document, the following terms and definitions apply:

1.5.1 "Access Control" - Any method that physically, logically or technically secures an entry point into a system or physical space. Examples include (but are not limited to) door locks, biometric locks, magnetic card swipe access, number pad requiring PIN or an access code, login password, OTP, etc.

1.5.2 "Asset" - Anything that has value to the organization.

1.5.3 "Authorized User" - An individual who has approved access to an Information Asset in order to perform job responsibilities.

1.5.4 "Backup" - The activity of copying files or databases so that they will be preserved in case of equipment failure or other catastrophe.

1.5.5 "BISO" - Building Information Security Officer who serves as the focal point for all information security issues and concerns in the Building.

1.5.6 "Business Continuity Management" - Holistic management process that identifies potential threats to an organization and the impacts to operations that those threats, if realized, might cause and which provides a framework for building organizational resilience with the capability for an effective response that safeguard the interests of its key stakeholders, reputation, brand and value-creating activities.

1.5.7 "Change" - Any modification to configuration items (CIs), service or service components and/or its associated element that could have a potential impact on information systems and/or significant impact on the stability and reliability of the production environment.

1.5.8 "CISO" - Chief Information Security Officer, CBDT who serves as the focal point for all information security issues and concerns in the Income Tax Department.

1.5.9 "SISO" - Systems Information Security Officer who serves as the focal point for all information security issues and concerns in the Systems Directorate.

1.5.10 “Compliance assessment” - The process to identify and assess the requirements to achieve a state of being in accordance with established guidelines, specifications or legislation or standards.

1.5.11 “Contractor” - Person or firm that undertakes a contract to provide materials or labor to perform a service or do a job. The term is used interchangeably with MSP (Managed Service Provider).

1.5.12 “De-militarized zone (DMZ)” - Computer host or small network inserted as a "neutral zone" between private network and the outside public network. It prevents outside users from getting direct access to a server that has confidential information.

1.5.13 “Incident” - An occurrence that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies.

1.5.14 “Information Assets” - Business applications, system software, development tools, utilities, hardware, infrastructure and paper records used for information management and processing.

1.5.15 “Information Security” - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.

1.5.16 “ISC” - Information Security Committee constituted in the Central Board of Direct Taxes (CBDT) with a view to putting in place a robust Information Security Mechanism in the Department.

1.5.17 ISMS(Information Security Management System) - Set of policies and procedures for systematically managing an organization's sensitive data.

1.5.18 “LISC” - Local Information Security Committee set up in the cadre controlling authority to oversee implementation of the Information Security Mechanism in the region.

1.5.19 “LISO” - Local Information Security Officer who serves as the focal point for all information security issues and concerns in the region.

1.5.20 “Need to Know Principle” - Access privileges for any user should be limited to resources absolutely essential for completion of assigned duties or functions and nothing more.

1.5.21 “Personal Data” - Data relating to an individual or entity who is or can be identified either from the data or from the data in conjunction with other information that is in or is likely to come into, the possession of the data controller.

1.5.22 “PISO” - Project Information Security Officer who serves as the focal point for all information security issues and concerns in the Project.

1.5.23 “Privileged User” - User account which has fewer privileges than an administrator account but has permission above a normal user access.

1.5.24 “Restoration” - Process that involves copying backup files from secondary storage (tape or other backup media) to hard disk to ensure integrity and adequacy of information being backed up.

1.5.25 “Retention Period” - The amount of time in which a given set of data will remain available for restore.

1.5.26 “Risk Management” - Set of elements of an organization’s management system concerned with managing risk.

1.5.27 “Risk Treatment Plan” - The immediate output of risk assessments which defines how, based on the established criteria, each risk is to be handled.

1.5.28 “Risk” - The combination of the probability of an event and its consequences. There can be more than one consequence from an event and the consequences can be positive or negative.

1.5.29 “Segregation of Duties” - Concept of having more than one person required to complete a task. (The separation by sharing of more than one individual in one single task is an internal check mechanism intended to prevent fraud and error.)

1.5.30 “Third Party” - Any entity in relation to personal data, means any person other than the data subject, the data controller or any data processor or other person authorized to process data for the data controller.

2 Organization of Information Security

The purpose of this section is to define a suitable information security organization structure and define roles and responsibilities for coordination of information security activities within the organization.

2.1 Information Security Committee (ISC)

2.1.1 An Information Security Committee (ISC) has been constituted in the Central Board of Direct Taxes (CBDT) under the Chairmanship of Member (I/c FT & TR) with a view to putting in place a robust Information Security Mechanism in the Department.

2.1.2 The ISC shall have following responsibilities and authority:

i. Ratification of Information Security Policy for ITD.

ii. Oversee implementation of Information Security Policy

iii. Conduct review of the Information Security Policy to ensure continuing suitability, adequacy and effectiveness.

iv. Initiate internal and external security reviews and ensure that action is taken to rectify any identified shortfalls.

v. Oversee disciplinary action in cases of breach of Information Security Policy.

2.2 Chief Information Security Officer (CISO), CBDT

2.2.1 The Commissioner (Coordination & Systems), CBDT is the Chief Information Security Officer (CISO) for ITD.

2.2.2 The CISO shall have following responsibilities and authority:

i. Overall responsibility of establishing, implementing, operating, monitoring, reviewing, maintaining and improving the Information Security.

ii. Serve as the focal point for all information security issues and concerns.

iii. Approve, maintain and communicate ITD Information Security Policy

iv. Ensure that responsibilities are defined for and that procedures are in effect to promptly detect, investigate, report and resolve security incidents.

v. Ensure that ongoing information security awareness education and training is provided to all employees.

vi. Provide reports to the ISC on the status of information security, policy violations and information security incidents.

2.3 Local Information Security Committee (LISC)

2.3.1 Local Information Security Committee (LISC) will be set up in all Cadre Controlling Pr. CCsIT which will be headed by CIT (Admin) and comprising of two officers of the level of CIT and two officers of the level of Addl./Jt. CIT. Additional Commissioner (HQ) (Administration) will be the Member Secretary of the LISC.

2.3.2 The LISC shall have following responsibilities and authority:

i. Ensure compliance of Information Security Procedures with the ITD Information Security Policy. All exceptions to the Policy shall be duly approved by CISO.

ii. Oversee implementation of the Information Security Policies and Procedures in the region.

iii. Initiate internal and external security reviews in the region and ensure that action is taken to rectify any identified shortfalls.

iv. Conduct review of the Information Security Procedures to ensure continuing suitability, adequacy and effectiveness.

v. Provide monthly reports to the CISO on the status of information security, policy violations and information security incidents.

2.4 Local Information Security Officer (LISO)

2.4.1 The Commissioner (Admin) will be designated as the Local Information Security Officer (LISO) in each region.

2.4.2 The LISO shall have following responsibilities and authority:

i. Serve as the focal point for all information security issues and concerns in the region.

ii. Communicate Information Security Policies and Procedures to all employees in the region.

iii. Ensure that responsibilities are defined for and that procedures are in effect to promptly detect, investigate, report and resolve security incidents.

iv. Ensure that ongoing information security awareness education and training is provided to all employees and users in the region.

v. Provide reports to the LISC on the status of information security, policy violations and information security incidents.

2.5 Pr. Commissioner, Pr. Director, Commissioner, Additional Director General

2.5.1 The Pr. Commissioner, Pr. Director, Commissioner, Additional Director General shall have following responsibilities and authority:

i. Communicate Information Security Policies and Procedures to all employees, contractors and users working under them.

ii. Ensure that responsibilities are defined for and that procedures are in effect to promptly detect, investigate, report and resolve security incidents.

iii. Oversee implementation of Information Security Policies and Procedures.

iv. Ensure that ongoing information security awareness education and training is provided to all employees and users in the Department.

v. Provide reports to the LISO on the status of information security, policy violations and information security incidents.

2.6 Building Information Security Officer (BISO)

2.6.1 Normally the senior most officer in the building will be designated as the Building Information Security Officer (BISO) in each building or as nominated by the Pr. CCIT of the region.

2.6.2 The Building Information Security Officers (BISO) shall have following responsibilities and authority:

i. Ensure that responsibilities related to environmental and physical security in the building are defined and implemented.

ii. Oversee implementation of Information Security Policies and Procedures related to environmental and physical security in the building.

iii. Ensure that ongoing information security awareness education and training is provided to all employees and users in the building.

vi. Ensure that procedures are in effect to promptly detect, investigate, report and resolve security incidents.

iv. Provide reports to the LISO on the status of information security, policy violations and information security incidents.

2.7 Systems Information Security Officer (SISO)

2.7.1 The Additional Director General (Systems) (HQ) is the Systems Information Security Officer (SISO).

2.7.2 The SISO shall have following responsibilities and authority:

i. Serve as the focal point for all information security issues and concerns in the Systems Directorate.

ii. Maintain contact with special interest groups and authorized information security forums and communicate updates on new vulnerabilities, security threats, regulations and/or risks pertaining to the Project Information Security Officer (PISO).

iii. Provide reports to the CISO, CBDT on the status of information security policy violations and information security incidents.

2.8 Project Information Security Officer (PISO)

2.8.1 An officer of the rank of Addl./Jt./Deputy Director (Systems) will be designated as the Project Information Security Officer (PISO) in each Project/Module.

2.8.2 The Project Information Security Officer (PISO) shall have following responsibilities and authority:

i. Serve as the focal point for all information security issues and concerns in the Project.

ii. Ensure compliance of Project level Information Security Management System (ISMS) with the ITD Information Security Policy. All exceptions shall be duly approved by SISO.

iii. Ensure that ongoing information security awareness education and training is provided to all employees and users in the Project.

iv. Oversee implementation of Project level Information Security Management System.

v. Ensure that responsibilities are defined for and that procedures are in effect to promptly detect, investigate, report and resolve security incidents.

vi. Conduct review of the Project level Project level Information Security Management System to ensure continuing suitability, adequacy and effectiveness.

vii. Identify and address legal and regulatory requirements and contractual security obligations related to the Project.

viii. Facilitate internal and external assessments as per the required frequency.

ix. Closure of observations arising out of internal audits and external audits.

x. Provide reports to SISO on the status of information security, policy violations and information security incidents.

2.9 Commissioner (Audit)

2.9.1 The Commissioner (Audit) shall have following responsibilities and authority:

i. Conduct Information security audits to check compliance to Information Security Policies and Procedures in offices of the region;

ii. Report non-compliances, audit findings to the LISO;

iii. Follow up for closure of non-conformities.

2.10 Contact with special interest groups

2.10.1 SISO is responsible for maintaining appropriate contact with special interest groups and authorized information security forums. Advice is taken from these groups on leading information security practices, updates on new vulnerabilities, security threats, regulations and/or risks pertaining to the services that are provided by the organization. The updates are communicated to relevant personnel and implemented as and when required.

2.10.2 Contacts should be maintained with the following special interest groups, but not limited to:

i. Special Security Forums (e.g. Computer Emergency Response Team –In): Issue security guidelines, advisories and share information relating to latest changes in information security.

ii. Security Advisories: Provide objective, timely and comprehensive information about security threats and vulnerabilities.

3 Risk Management

3.1.1 The Department/Project shall establish and maintain Information Security Risk Management procedure covering Risk Assessment and treatment of identified Risks on continual basis.

3.1.2 Risk Assessment: Information Security (IS) Risk assessment shall be carried out periodically or in case of major event/change that impacts security of Information Asset. All the identified risk shall be captured in risk register.

3.1.3 Risk Analysis: The outcome of such Risk assessment shall be reviewed, and Corrective / Preventive actions shall be taken.

3.1.4 Risk Treatment: The procedure for Risk treatment shall be established.

3.1.5 Information Security Risk Management shall ensure that:

i. No critical Information and related assets are left out.

ii. Trivial assets are not over protected and important assets are not under protected.

iii. The asset owners from respective teams share the same perspective for Risk Assessment.

iv. Controls selected for risk mitigation are compatible with existing ones, which not only complement each other but also produce synergetic effect.

4 Human Resources Security

4.1 Job Descriptions – Roles and responsibilities

4.1.1 All job roles and responsibilities must be documented and must include general as well as specific responsibilities for implementing or maintaining security. All employees and other users must understand their job roles and responsibilities.

4.2 Background Checks

4.2.1 Background checks must be performed on all personnel (including temporary personnel and contract personnel) performing sensitive or critical job roles before they are selected for the position or transferred to the position. Further, personnel who are third party service providers must have undergone a background check by their respective organizations and the assurance of the same must be provided to the Department. Information provided by personnel, at the time of recruiting must be subjected to verification procedures.

4.3 Terms and Conditions of Employment

4.3.1 All employees, contractors and third-party users of the Department's Information Assets must sign and agree terms and conditions of their employment contract. These terms and conditions must include/state the organization's as well as the employee's responsibilities towards Information Security.

4.3.2 In some cases, an authorized representative can sign a blanket agreement on behalf of all contractors and third-party users. This needs to be specifically authorized by the Head of Department (HoD).

4.4 Management Responsibilities

4.4.1 All supervisory roles are responsible for the performance and conduct of the staff personnel reporting to them. The Head of the Departments (HoDs) are required to monitor performance and conduct of each of their staff, as well as to assess their impact on the security of the Information Assets to which the staff has access.

4.5 Confidentiality Agreements

4.5.1 All contractual employees and employees of contractors/MSPs/sub-contractors must sign appropriate confidentiality agreements to protect the confidential and sensitive information of the organization. All the activities involving confidential information will be monitored and audited periodically.

4.5.2 All contractual employees and employees of contractors/MSPs/sub-contractors are required to agree and sign non-disclosure obligations. Users are required not to disclose organizational information derived as a result of their access to the Department's Information Systems to unauthorized parties.

4.5.3 Procedure must be defined for reporting the violations of confidentiality agreements.

4.5.4 Appropriate disciplinary actions will be carried out against the Department employees in cases of breach of confidentiality agreements.

4.5.5 Action would be taken against contractual workers and third party vendors for any violation as per law and as per terms of the agreement.

4.6 Information Security Training and Awareness

4.6.1 Information Security Training and Awareness Programs must be provided to all the employees (including temporary personnel and contract personnel) and other third party users to create consciousness about the Information Security Policies and Procedures.

4.7 Disciplinary Process and Penal Process

4.7.1 There must be a formal disciplinary process for employees, and penal process for contractors or third party users who have violated the organizational security policies and procedures. Such a process can act as a deterrent. Additionally, the disciplinary or penal process must ensure correct and fair treatment of employees, contractors and third party users who are suspected of having committed serious breaches of security.

4.8 Employees, Contractors and Third Party Termination or Transfer of Employment

4.8.1 The Department must ensure that termination or transfer of employees, contractors and third party users are done in orderly manner and responsibilities are defined within the Department to ensure the same. The information assets of the Department available with terminated or transferred individuals must be taken back and all their access rights (both physical and logical) must be removed immediately

4.8.2 The Department must take into consideration the changes of responsibility or transfer of employees, contractors and third party users and access the appropriateness of their access when such occasions arise.

4.9 Return of Assets

4.9.1 All employees, contractors and third party users must return all of the organization’s information assets in their possession upon termination of their employment, contract or agreement.

4.10 Removal of Access Rights

4.10.1 The Department must ensure that the access rights of all employees, stakeholders, reporting entities, contractors and third-party users to information and information processing facilities must be removed upon termination of their employment, contract or agreement, or adjusted upon change.

5 Asset Management

5.1 Information Asset Inventory

5.1.1 An information asset is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information resources include information and related resources, such as personnel, equipment, funds, and information technology.

5.1.2 The Department's information assets must be listed in an Information Asset Inventory.

5.1.3 Each Information Asset must be clearly identified individually and (if appropriate) collectively in combination with other Assets to form an identifiable Information asset.

5.1.4 The Information Asset inventory must include all information necessary in order to recover from a disaster.

5.1.5 The Information Asset Inventory must contain the relevant information such as:

- Identification
- Description
- Location
- Owner
- Custodian
- Business value of the Information Asset
- Information Asset classification
- Validity of the classification

5.1.6 Examples of Information Assets include:

- Information assets: databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;
- Software assets: application software, system software, development tools, and utilities;
- Hardware assets: computer equipment, communications equipment, removable media, and other equipment.

5.2 Information Asset Classification Criteria

5.2.1 All Information Systems Assets must be classified according to this policy. All information must be handled according to the classification levels to ensure security of the information resource.

5.2.2 Risk classification will enable the Department to focus asset protection mechanisms on those Information Assets that are most susceptible to specific risks. Information Assets will be assigned classifications based on their susceptibility to risk.

5.3 Classification Guidelines

5.3.1 All the Department information must be classified into one of the following categories:

- **Top Secret:** Information unauthorized disclosure of which could be expected to cause exceptionally grave damage to the national security or national interest. This category is reserved for Nation's closest secrets and to be used with great reserve.
- **Secret:** Information unauthorized disclosure of which could be expected to cause serious damage to the national security or national interest or cause serious embarrassment in its functioning. This classification should be used for highly important information and is the highest classification normally used.
- **Confidential:** Information unauthorized disclosure of which could be expected to cause damage to the security of the organisation or could be prejudicial to the interest of the organisation, or could affect the organisation in its functioning. Most information will on proper analysis be classified no higher than confidential.
- **Restricted:** Information which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose.
- **Unclassified:** Information that requires no protection against disclosure. E.g. Public releases.

5.3.2 Information labeling and handling procedures must be developed, commensurate with the level of classification.

5.3.3 Procedures shall be defined for Data Management including guideline for retention, archival and destruction of data to ensure uniformity in the manner in which every project addresses record management as well as to ensure adequate compliance with all applicable regulations.

5.4 Acceptable Use of Information Assets

5.4.1 The Department must ensure that there are rules defined for the acceptable level of use for all the information assets of the organization.

5.4.2 The Department must ensure that the employees and other users follow the guidelines for the acceptable level of use of all the information assets. Information Assets must be used for official and operational purposes and must be protected from damage due to non-official usage.

5.4.3 Formal procedures or standards must be developed for handling and storage of information assets based on their classification to protect the information asset from unauthorized disclosure or misuse.

5.5 Media Handling and Security

5.5.1 Media must be protected from physical damages like fire, moisture and magnetic interference.

5.5.2 A stock or inventory of all the media must be maintained.

5.5.3 Media must be disposed off securely and safely when no longer required. Formal procedures for the secure disposal of media must be established to minimize the risk of sensitive and confidential information being disclosed to unauthorized persons.

5.5.4 Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.

6 Access Control

6.1 Business Requirement for Access Control

6.1.1 The access to the Department's information and information systems (Operating Systems, Applications, Databases, network equipment and others) must be according to the principles of "least privilege" and "need to know" basis.

6.1.2 The procedures must be administered to ensure that the appropriate level of access control is applied to protect the information in each application or system from unauthorized access, modification, disclosure or destruction to ensure that information remains accurate, confidential, and is available when required.

6.2 User Registration and de-registration

6.2.1 All the Department employees and other users must be granted access to the Department information systems and services through a formal user registration process that includes approval of access rights from authorised personnel before granting access.

6.2.2 In case of registration of a non-Department employee/ other user a formal request in a predefined format must come from the respective party before the access is granted.

6.2.3 All users must follow a formal de-registration process for revocation of access to all information systems and services which will include automated or timely intimation and revocation of access rights.

6.2.4 In case of de-registration of a non-Department employee/ other user a formal request must come from the respective party before the access is removed.

6.2.5 All the employees/ third parties must inform in advance about the required change in their access to the Department information systems. E.g. change in access of a principle officer due to change of his role.

6.2.6 User accounts which are inactive for a period of 45 days must be disabled automatically by the system.

6.2.7 User creation/ privilege/ role assignments should be done physically at the server end not through remote/ through web interfaces.

6.3 Privilege Management

6.3.1 Privileges associated with each type of information systems such as Operating System, Business Applications, Databases and Network Elements must be identified and documented.

6.3.2 Privileges must be allocated to individuals based on the requirements of their job function and role, on authorization from appropriate personnel. Additional privileges more than what is required for the job function must be allowed after getting approval from appropriate personnel.

6.3.3 System, Administrative or root accounts must be strictly limited and monitored by the Department.

6.4 User Password Management

6.4.1 All User passwords (Individual as well as Administrator) must remain confidential and must not be shared, posted or otherwise divulged in any manner.

6.4.2 An initial password must be provided to the users securely during the user creation process & the system must be configured to force the users to change the initial password immediately after the first logon.

6.4.3 Appropriate procedures must be put in place for storing and management of administrative passwords for critical information systems.

6.4.4 Two-factor authentication mechanism must be used to provide access to all critical information systems.

6.4.5 The password and account policy should be enforced for all user and administrative accounts on operating systems, applications, databases and all other information protected by password controls:

6.4.6 Due to system limitations or organizational necessity, if any of the password and account policy parameters cannot be followed, specific mechanisms must be put in place to obtain approvals and implement countermeasures to mitigate the risk of not following the password policy.

6.4.7 Where it is not possible to implement individual user-ids and passwords within the application itself (due to design parameters), alternative solutions for restricting and auditing access privileges must be evaluated for feasibility and must be implemented. As far as possible, Department must not make do with the concept of utilizing the same user-id and password for all users.

6.4.8 Strong Passwords must be constructed so that they are not guessed and compromised easily.

6.5 Review of User Access Rights

6.5.1 Department must review the access rights or privileges assigned to all individual users to the corresponding system periodically. Any exceptions noted must be addressed at the earliest.

6.6 User Responsibilities

6.6.1 All Information assets of the Department must be used for official purposes only by its authorized users. All users must adhere to safe usage practices that do not disrupt official work or bring disrepute to the Department.

6.6.2 Users are responsible to ensure that confidential, secret and top secret information asset is not stored on vulnerable machines.

6.6.3 Users must keep confidential, secret and top secret information under lock and key.

6.6.4 Users must destroy sensitive information after its intended use.

6.6.5 Users must ensure that all important information possessed by them is password protected and that the password is only shared with people on a need-to-know basis (if required).

6.6.6 Users must log out of computer terminal when finished accessing programs, or if left unattended.

6.6.7 Users must not share/ disclose their passwords with other users and third parties. All users are responsible for the activities performed through their login.

6.6.8 Users must not install any software or applications on their desktop that is not authorized or not essential to the Department's official work.

6.6.9 Users must not alter or change data contained within the Department computer systems in any way unless authorized to do so.

6.6.10 Users must not disclose any organizational data to anyone inside or outside the organization, unless authorized to do so.

6.6.11 Users must not install unauthorized hardware like a modem, removable media, boot device, etc. which could be used for either gaining access to the system or copying data from the system.

6.7 Operating System Access Control

6.7.1 Minimum Baseline Security Standards (MBSS) or hardening standards for all Operating Systems and critical applications must be developed and maintained. All installations of the operating systems and applications must be configured as per the MBSS.

6.7.2 While installing the Operating system, only the minimal set of services & applications required by the user should be installed/enabled. Some of the utilities/ programs that are enabled by default like Guest user account, file sharing, default passwords, sample networking programs, etc. must be disabled.

6.7.3 Access to operating systems should be controlled by a secure log-on procedure. User credentials required for access to various information systems must consist of a user ID and password or other credential (such as digital certificates, token, etc.) that is unique to an individual. Users must not have multiple accounts within the same computing environment.

6.7.4 Common user IDs must not be used unless they are absolutely essential. In situations where a common user ID is required, authorizations must be obtained from appropriate authorities before providing access. Further, individual ids must not be shared among users.

6.7.5 Restrictions should be enforced at operating system level to ensure adherence to password requirements.

6.7.6 Wherever applicable, access to various system utility programs that might be capable of overriding system and application controls must be controlled to ensure that the users do not obtain more information than what they require to perform their job function. Access to the utilities must be limited to technical staff only to assist end-users resolve problems.

6.7.7 Wherever technically feasible Operating Systems, Applications, Databases and Terminals or servers must timeout and clear the screen automatically if the terminal is inactive for more than 5 minutes.

6.8 Operating System, Applications & Databases

6.8.1 Access to information and application system functions by users and support personnel must be restricted in accordance with the access control policy and procedures.

6.8.2 Audits must be performed quarterly to ensure application security is maintained. In case of third party applications used in the Department, assurance must be obtained from third party vendors for application security built in the system.

6.8.3 Sensitive systems as well as applications must be identified and isolated from normal computing environment. When a sensitive application is to run in a shared environment, the application systems with which it shares resources must be identified and agreed with the application owner who is in-charge of the sensitive application as well as the Information Security Officer.

6.8.4 No employee must have direct access to the database of any application system.

6.8.5 The access of vendors to database and other sensitive information storing computers must be restricted.

7 Operations Security

7.1 Documented Operating Procedures

7.1.1 Operating procedures must be developed and maintained for all IT processes of the Department to enable the technical staff to perform their daily operations.

7.2 Operational Change Management

7.2.1 Changes to IT assets (including applications, servers, systems software, and security architecture and network devices) should be performed in a controlled manner to ensure that the risks associated with such changes are managed to an acceptable level. This involves obtaining prior approval, performing impact analysis, testing, and maintaining up-to-date documentation for the entire process. Changes should be tested in a non-production environment before deployment and ineffective changes should be rolled-back.

7.2.2 Appropriate procedures must be put in place for all changes requiring emergency actions and response process, which bypass the Policies and Procedures outlined.

7.3 Segregation of Duties in Operational Procedure

7.3.1 All IT processes must adopt the principle of segregation of duties to the maximum extent possible. The initiation of an event must be separated from its authorization. The following principles must be followed:

(i) Persons involved in operational functions must not be given additional responsibilities in system administration processes and vice versa

(ii) Persons involved in testing processes must not be given additional responsibilities in system administration processes and vice versa

(iii) The responsibility for performing a security review of the system or process must be completely independent from the roles and responsibilities for developing, maintaining, and using the system or process.

(iv) Where segregation of duties is not possible or practical, the process must include compensating controls – such as monitoring of activities, maintenance and review of audit trails and management supervision.

7.4 Separation of Development, Test and Production Facilities

7.4.1 Development, test, and production facilities and duties should be physically separated to reduce the risks of unauthorized changes to the production system.

7.4.2 Transfer of information between the development, test and production environments must be controlled.

7.5 Capacity management

7.5.1 The Department must continuously monitor the utilization and make projections for future requirements of information processing resources and plan accordingly to ensure that adequate information processing resources are available to meet the official requirements of the Department.

7.5.2 The projections must take account of future developments and system requirements and current and projected trends in the Department's information processing.

7.5.3 The Department must perform Capacity Planning study on a yearly basis. The Department shall identify the trends in usage, particularly in relation to applications or management information system tools.

7.6 Systems Acceptance

7.6.1 Acceptance criteria for new information systems, upgrades and new versions must be established and suitable tests of the system must be carried out prior to acceptance.

7.6.2 All the requirements and criteria for acceptance of new systems must be clearly defined, agreed, documented and tested.

7.7 Protection from Malware

7.7.1 PISO shall ensure that information and information processing facilities are protected against malware

7.7.2 Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

7.7.3 All servers, desktops, workstations, hand-held devices, gateways and any other access points to the Department's network must be protected against malicious code.

7.7.4 For all information processing facilities, antivirus with latest update must be installed. Anti-virus signatures (including IDS and OS signatures) should be downloaded on a standalone Internet computer and the signature should be updated on a central patch distribution server through a storage media. The central patch distribution server should, in turn, update IDS and OS signatures on all information processing facilities.

7.7.5 Anti-virus application and processes must ensure early detection, efficient containment and eradication of malicious code.

7.7.6 All the possible entry points in the network through which a virus attack is possible must be identified and all the traffic entering the network through these points must be routed via an antivirus gateway application for monitoring all the types of traffic flowing through the network, whether be it HTTP, FTP, SMTP or POP3.

7.7.7 Adequate user awareness measures should be implemented for the same.

7.7.8 Controls should be considered to prevent unauthorized mobile code execution.

7.8 Backup Policy

7.8.1 All application and operating systems software, data (including databases), application and operating systems configuration information, hardware configuration information (where applicable) and log files (logs from various systems that need to be backed) must be identified and documented.

7.8.2 Frequency of backup, medium of backup and storage of the backup must be identified and documented.

7.8.3 Backup of database must be done with additional security measures.

7.8.4 Information must be retained for the specified period.

7.8.5 A backup copy of the inventory, critical software, operating systems must be stored in a fire-rated container.

7.8.6 The number of backup sets to be maintained must be decided based on the criticality of information residing on the servers.

7.8.7 Backup register has to be maintained by personnel who takes backup and must be updated regularly.

7.8.8 All removable storage media available with the organization for issue must be serially numbered and labeled.

7.8.9 The safe custody of every used removable storage media is the personal responsibility of the concerned user.

7.8.10 Top secret, Secret and confidential information must not be stored on computers. If and when such top secret and sensitive information is processed on the PC, the information should be stored/ archived after the processing is over.

7.8.11 Before deleting a sensitive file from a storage media, some useless or junk information must be over-written on the file to prevent restoration of sensitive data by an unauthorized user.

7.8.12 In addition to the scheduled backups, backups must be taken in case any of the following event occurs

- Configuration change
- Upgrade of an operational system

7.8.13 Both onsite and offsite backup must be in safe custody in a fire-proof safe. If fire-proof safe is not possible, alternate controls must be put in place to protect those tapes from fire.

7.8.14 All movement of tapes between offsite and onsite locations must be tracked and recorded.

7.8.15 During transportation, removable storage media must be carried in appropriate mail-boxes to save these from damage.

7.8.16 Backup of data and authorization systems should be under direct control of the Department and not the vendor.

7.9 Recovery Policy

7.9.1 Backed up data must be provided for restoration purposes after approval and authorization

7.9.2 A log of backed data restored from backup media must be maintained

7.9.3 Recovery procedures and technical system features must exist to ensure that recovery is done in a secure and verifiable manner. Circumstances that can inhibit a trusted recovery must be documented and appropriate mitigating procedures must be in place.

7.10 Restoration Testing Policy

7.10.1 To verify the readability of backup media, mock restoration tests must be carried out, on the test systems periodically.

7.10.2 The entire process must be documented detailing the test plan, the activities carried out and the test results.

7.10.3 Exceptions identified during the testing process must be documented and reported.

7.11 Logging and Monitoring

7.11.1 Event Logging: User activities, exceptions, and security events should be logged and monitored. Logs must include the following:

- System starting and finishing times
- System errors or Faults and corrective action taken
- Confirmation of the correct handling of data files and computer output.
- The name of the person making the log entry

7.11.2 The activities of users with high levels of access (privileged users such as system technical staff and system operators) should be logged and independently reviewed on a regular basis.

7.11.3 All access to critical applications and the Department's network should be monitored for suspicious activities or security breaches. Adequate response mechanisms should be in place for containing security breaches.

7.11.4 System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

7.11.5 The audit logs should be retained based on the record retention requirements.

7.11.6 Logging facilities and log information should be protected against tampering and unauthorized access.

7.11.7 The clocks of all relevant information processing systems within the Department or security domain must be synchronized to a single reference accurate time source.

7.12 Control of operational software

7.12.1 Procedures shall be implemented to control the installation of software on operational systems.

7.13 Security of System documentation

7.13.1 System documentation must be protected from unauthorized access.

7.13.2 The system or application owner must authorize or approve distribution lists for system documentation. This list must be restricted to a minimum number of parties.

7.14 Technical Vulnerability Management

7.14.1 Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the department's exposure to such vulnerabilities shall be evaluated and appropriate measures taken to address the associated risk.

7.14.2 Restrictions on software installation must be placed. Rules governing the installation of software by users shall be established and implemented.

7.15 Information systems audit considerations

7.15.1 Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to official processes.

8 Communication Security

8.1 Network Security Management

8.1.1 The Department network must be used for valid official purposes only. The protection of information contained on the Department networks is therefore the responsibility of the Department and the activity and content of information on the Department computer networks is within the scope of review by the Department.

8.1.2 The Department must develop and implement network security systems and procedures, and provide network security resources (Firewall, IDS, etc.) to protect all organizational data, related application systems and operating systems software from unauthorized or illegal access at a level that is appropriate for the information or computing resources.

8.1.3 Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced

8.1.4 The Department must ensure that groups of information services, users and information systems are segregated on networks.

8.2 Network Access

8.2.1 All network and network services in the Department must be identified and documented.

8.2.2 Access to the Department network and network resources must be on need to know basis and authorizations must be obtained from appropriate authorities before providing access. Network and network services required for every job function and role must be identified and documented.

8.2.3 Connection capability of users (local or remote) should be restricted through access-control lists in Firewalls and switches. Additional services more than what is required for the job function must be allowed only after getting approval from appropriate personnel.

8.2.4 Technical staff must ensure that the host operating system is configured to validate each user prior to allowing network access.

8.2.5 Remote access for employees and other users must be controlled and allowed only after due approval by authorised personnel.

8.2.6 Remote access to reporting entities must be provided through SSL encrypted channels along with digital signatures (e.g., DSA, RSA, and ECDSA).

8.2.7 The information system must notify the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

8.2.8 All remote access to users (other than reporting entities) for the Department information systems must be mediated through an IPSEC VPN via a managed access control point, such as a remote access server or bastion host in a DMZ (De-Militarized Zone).

8.2.9 The information system must limit the number of concurrent sessions for any user to one.

8.2.10 The information systems must prevent further access to the systems by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

8.2.11 Access to critical devices like routers and firewalls must be restricted only to authorized terminals. The devices can be managed only from these authorized terminals in order to implement a principle of enforced path.

8.2.12 Physical and logical access to diagnostic and configuration ports must be controlled.-

8.2.13 Network and network services access must be periodically reviewed in order to ensure that unauthorized network services are not used or authorized network services are not accessed by unauthorized personnel.

8.2.14 Policies detailed in Access Controls Policy – User Account Management must be followed for providing access to network & network services for dedicated as well as shared networks.

8.2.15 Networks must be physically divided based on the criticality of the information stored in the networks. If the network is physically separated, controls must be in place to protect physical access to the network points at all ends.

8.2.16 All network equipment default passwords (e.g., routers) must be changed by technical staff during installation

8.2.17 To maintain the privacy of the Department information, its networks must not be used for personal and/ or private information unrelated to official purposes. The organization’s computers and resources must be used for valid official purposes only.

8.2.18 A legal message must be displayed on the screen whenever a user logs on to the network through any terminal to warn the user on using Department network for official use only. A message must be displayed on all external network connections warning potential users that unauthorized use is prohibited (e.g. Unauthorized access to the Department network is prohibited).

8.2.19 The use of personal communications equipment (modems, ISDN cards, etc.) attached directly to personal computers with remote control software must be prohibited.

8.2.20 Access to third parties must be given after carefully analyzing need and after assessing risks involved in providing such access.

8.2.21 Routing controls must be implemented for networks to ensure that computer connections and information flows do not breach the access control requirements of the applications.

8.3 Internet Service Management

8.3.1 Access to the Internet must be provided only to authorised users.

8.3.2 All Internet activity must pass through the Department's Firewall so that access controls and related security mechanisms can be applied.

8.3.3 Frequent Links visited by users must be monitored and reported on a periodic basis.

8.3.4 Any information received or gathered regarding system vulnerabilities shall be reported.

8.3.5 Downloading of software (both source and binary) from public sources (freeware/ shareware) is not allowed without authorization.

8.4 Network Device Management

8.4.1 All network equipment and communication lines must be identified, documented and updated regularly.

8.4.2 Network diagrams at all levels (WAN & LAN segments) must be maintained and updated regularly.

8.4.3 Minimum Baseline Security Standards (MBSS) must be developed and maintained and all network equipment must be configured as per MBSS.

8.4.4 Use of pirated and unlicensed software is strictly prohibited. Only original/ licensed software purchased must be used.

8.5 Information Transmission

8.5.1 Any information from the Department's environment traveling over third-party networks or public networks must be encrypted, wherever feasible. Classified information must only be transferred via accredited communications paths. Appropriate encryption algorithms must be used to maintain the integrity and confidentiality of the data.

8.5.2 Appropriate technology must be used for encryption e.g. WinZip or PGP.

8.5.3 Access to encryption software must be given only on a need basis after authorization from appropriate personnel.

8.5.4 Confidential, secret or top secret information transmitted over any communication network must be sent in an encrypted form.

8.5.5 Confidential, secret or top secret information not being actively used, when stored or transported in computer-readable storage media (such as magnetic tapes, floppy disks or CDs), must be in encrypted form.

8.5.6 To prevent unauthorized disclosure of data when computers are sent out for repair or used by others within or outside the organization and data cannot be deleted, all data stored on hard disks must be encrypted via user-transparent processes.

8.5.7 The strength of the encryption algorithm to be used in a given situation must be based on the classification of the data to be encrypted.

8.5.8 Software that performs unattended file transfer to or from other systems must authenticate the username-password, unless the information being transferred is classified as Unclassified.

8.6 Network Assessment

8.6.1 Network vulnerability assessments must be performed on an ongoing basis by competent personnel. The risks identified must be documented in the assessment report.

8.6.2 Assessment report must be submitted to the PISO regularly.

8.6.3 Third-party independent network assessment must be carried annually in order to provide assurance to the management, customers and stakeholders.

8.7 Mobile Devices and Tele-working

8.7.1 Appropriate security measures must be adopted to protect against the risks of using mobile computing and communication facilities such as laptops, mobile phones, personal digital assistant, and hand held devices. For instance, security measures such as hard disk encryption must be implemented on mobile devices such as laptops having the Department related internal or confidential information.

8.7.2 Stringent access controls such as two-factor authentication must be used when accessing the Department’s systems and information via tele-working.

8.7.3 The Department must identify the requirement for physical protection, access controls, cryptographic technique, backups, and virus protection for mobile computing.

8.7.4 The Department must ensure that users connecting remotely to the Department information systems comply to the Department information security policies before they can be allowed to use them.

8.8 Exchange of Information

8.8.1 To prevent loss, modification, destruction, or misuse of information, the Department must protect and control exchange of critical business information assets and software with third parties and outside organization.

8.8.2 Formal MoUs or agreements must be established with the third parties to exchange information. These MoUs or agreements must include the non-disclosure clause pertaining to the exchanged information.

8.8.3 Non-government e-mail providers (viz. Google, Yahoo, Rediff mails etc.) must not be used for exchanging classified information.

8.8.4 Formal agreements must be established for the exchange of critical information assets or software with outside organizations.

8.8.5 These agreements must include both physical and electronic exchanges.

8.8.6 These agreements must reflect the sensitivity of the critical information assets being exchanged and must describe any protection requirements.

8.8.7 These agreements must specify management responsibilities, notification requirements, packaging and transmission standards, courier identification, responsibilities and liabilities, data and software ownership, protection responsibilities and measures, and all encryption requirements.

8.8.8 Confidentiality or nondisclosure agreements: Requirements for confidentiality or non-disclosure agreements reflecting the department’s needs for the protection of information shall be identified, regularly reviewed and documented.

8.8.9 In the event of interconnection of business information systems with external entities such as third party organizations, adequate measures must be implemented to protect the information within the information systems.

8.9 Physical Media in Transit

8.9.1 Media containing information must be protected against unauthorized access, misuse or corruption during transportation beyond an organization’s physical boundaries.

8.10 Electronic Messaging and e-mail security

8.10.1 Information involved in electronic messaging must be adequately protected to prevent loss, modification or misuse of information.

8.10.2 All email attachments must be scanned by the Anti-Virus engine for the email application and must ideally be passed through a content inspection engine.

8.11 Publicly Available Information

8.11.1 Any information stored or generated in the Department that are made publicly available for public consumption must be identified, verified and approved by appropriate authorities before making it public.

8.11.2 Adequate controls must be put in place to ensure that integrity of Publicly Available Information is protected.

8.12 Internet Security Policy

8.12.1 Use of internet facilities is prohibited for malicious activities like hacking, phishing etc., and downloading, transmitting and publishing of obscene/ objectionable material as per Indian IT Act 2000 and further IT (AMENDMENT) ACT, 2008

8.12.2 Any violation of ITD policies or government regulations shall lead to disciplinary action.

8.12.3 The server logs and the electronic 'paper trails' shall be considered proof for deciding misuse of Internet facilities.

8.12.4 All nodes shall be provided with anti-virus, which scans all incoming and outgoing mails and disallows opening of suspicious attachments/ codes.

8.12.5 All PCs, which have Internet access facility, shall have a defined 'custodian / owner', who shall be held responsible for any violation of Internet usage policy from that PC.

8.12.6 Users should not use tools/software to bypass ITD's security framework such as proxy avoidance tools/websites, Instant Messengers, downloading of any tools/software that can be of use to jeopardize the security.

8.13 Wi-Fi Security

8.13.1 All the wireless AP should be WEP enabled. All the AP's should have SSID's defined. However the SSID broadcast should be disabled.

8.13.2 All the WEP keys should be Alpha numeric. The keys should not include the SSID of the AP or the department name.

8.13.3 The inbuilt MAC address filter / Firewall on the AP should be enabled. The connection to the AP should filtered Via MAC addresses.

8.14 Portable Storage device Security

8.14.1 Office equipment handling sensitive information should be USB blocked. In case of any need, approval of competent authority maybe taken.

8.14.2 User shall ensure that portable USB storage media used is free from virus.

8.14.3 User shall ensure that the execution of software from portable USB storage media is prohibited.

9 Security in development and support processes

9.1 Secure development policy

9.1.1 Rules for the development of software and systems shall be established and applied to developments within the Department.

9.1.2 Security requirements in an information system must be identified and documented during the requirements gathering and analysis phase of acquisition, development or change of information systems. They must be justified and agreed with business process owners.

9.1.3 Systems security requirements must reflect the business value of the information assets involved (in accordance with the Asset Classification Policy and Procedures) and the potential damage that may be caused due to absence of sufficient security.

9.1.4 A formal methodology must be defined and documented including security requirements for application development and maintenance process when done in-house.

9.1.5 Data input to applications must be validated to ensure that this data is correct and appropriate.

9.1.6 Validation checks must be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

9.1.7 Requirements for ensuring authenticity and protecting message integrity in applications must be identified, and appropriate controls identified and implemented.

9.1.8 Data output from an application must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

9.1.9 All new information systems and services that are acquired, developed or enhanced shall undergo security assessment using a formalized process, to ensure that appropriate security controls are identified and incorporated in them;

9.2 Security of System Files

9.2.1 Test data must be selected carefully, and protected and controlled.

9.2.2 Program source code available with the Department must be stored under restriction and only authorized personnel should have access to the same.

9.3 System change control procedures

9.3.1 Formal procedures must be developed for change management. All proposed system changes must be authorized and reviewed to verify that they do not compromise the security of either the system or the operating environment.

9.3.2 Business critical applications must be reviewed and tested prior to installation of OS patches or updates in a test environment in order to ensure that there is no adverse impact on security due to the changes in the operating system

9.3.3 Modifications to software packages must be discouraged. As far as possible, and practicable, vendor-supplied software packages must be used without modification. All necessary modifications (including configuration changes, changes to reports, etc.) to software packages must be made in accordance with formal Program Change Control Procedures.

9.4 Third party software Development

9.4.1 If the software is developed by a third-party, the Department must ensure that software development processes are in compliance to Department's Information Systems Acquisition, Development and Maintenance Methodology

9.4.2 The Department must have appropriate licensing agreements and contractual requirements for quality and accuracy of code

9.4.3 The Department must get assurance from the third-party for quality and accuracy of the work carried out

9.4.4 The Department must get the ownership of the source code. If this is not feasible to the third-party, the code must be kept under an escrow arrangement.

9.4.5 The Department must get the rights of access for audit of the quality and accuracy of the work.

9.4.6 The Department must perform testing processes as per the Department's Information Systems Acquisition, Development and Maintenance Methodology.

9.4.7 The Department must ensure scanning of outbound media and, periodic monitoring of systems activities to ensure no information leakage occurs. For developing software, actual sensitive data should not be provided to the software developing vendor.

9.5 Securing application services on public networks

9.5.1 Prior to deployment, all publicly available systems for e.g. website should be tested for threats such as denial of service, etc. and it shall be ensured that the identified vulnerabilities are fixed prior to publishing any information in such systems;

9.5.2 Review of all public interfaces shall be carried out periodically;

9.5.3 Information contained on the publicly available systems like website, should be accurate, authentic and posted only after the required approval is obtained; and

9.5.4 Processed information shall be obtained in compliance with the required data protection legislation.

9.6 Technical review of applications after operating platform changes

9.6.1 New releases/ Patches pertaining to the operating system shall be tested before being implemented in the operational environment to ensure that there is no adverse impact on operation, application controls or security. In case of any exceptions due to technical limitations, approval shall be taken from the Department Head for acceptance of tests conducted by the vendor/ supplier, which shall be subjected to audit;

9.6.2 The application controls shall be reviewed to ensure that they have not been compromised by the operating system changes; and

9.6.3 The Department shall ensure that notification of operating system changes is provided in time so that appropriate tests and reviews are done before implementation.

9.7 Secure system engineering principles

9.7.1 Principles for engineering secure systems need to be established, documented, maintained and applied to any information system implementation.

9.7.2 Leading practices for web application security such as OWASP shall be adopted for developing all web based applications.

9.8 System security testing

9.8.1 The Department shall ensure that Testing is conducted from security perspective during the development phase. These tests shall be conducted against the security requirements identified in the planning phase and the vulnerabilities, which can be exploited by internal/ external threat source, in the modules being developed.

9.9 System acceptance testing

9.9.1 Acceptance criteria for new information systems and information processing facilities, upgrades and new versions should be defined in the Functional Specification Document and Business Request Document;

9.9.2 Security clearance is obtained before any new information systems, upgrades and/ or new versions are accepted; and

9.9.3 User Acceptance Testing (UAT) is conducted prior to the deployment of the systems in the production environment.

9.10 Test Data

9.10.1 Test data shall be selected carefully, protected and controlled.

10 Supplier relationships

10.1 Information security policy for supplier relationships

10.1.1 The Department shall ensure Information security requirements for mitigating the risks associated with supplier's access to the department's assets shall be agreed with the supplier and documented.

10.1.2 Contracts must include information security requirements to ensure compliance to the Department's security policies and procedures. All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the department's information.

10.1.3 Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

10.2 Service Delivery

10.2.1 The Department shall ensure that all services to be provided by the outsourced party are clearly identified and the relationship with the outsourced party is managed through clearly identified point of contacts in the Department and the outsourced party.

10.2.2 The Department shall conduct a risk assessment to identify potential risks to the Department's Information Security as a result of outsourcing information or data processing functions or services to third party organizations.

10.2.3 A formal contract should be entered between the Department and all third parties providing service to the Department or using the Department's information systems. The services to be provided by the outsourced party must be covered by a strong Service Level Agreement ('SLA') that takes into consideration expected levels of service, security, monitoring, contingency and other stipulations as appropriate.

10.2.4 All contractors must be required to provide information to the Department about related subcontractors and obtain the Department's permission for the subcontracting, prior to initiation of work by the subcontractor.

10.2.5 Non-Disclosure or Confidentiality agreements to protect the Department's information assets must be signed by vendors, third parties, contractors and also by sub-contractors of the vendors.

10.3 Monitoring and Review of Third Party Services

10.3.1 Security controls and service levels, associated reports and records of third party service providers should be independently assessed, reviewed and monitored.

Vendor audits must be carried out at least annually to review the services offered by the third party.

10.4 Managing Changes in Third Party Services

10.4.1 Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, must be managed, taking account of the criticality of systems and processes involved and re-assessment of risks.

11 Physical & Environmental Security

11.1 Physical Security Perimeter

11.1.1 All the Department areas must be logically divided into different physical zones. Each zone must have appropriate level of access restrictions and access authorization requirements.

11.1.2 Areas containing critical IT equipment or handling sensitive information such as information received from foreign jurisdictions or information related to sensitive investigation matter must be designated as High Security Zones. Critical or sensitive information processing facilities must be protected by defined security perimeters, with appropriate security barriers and entry controls.

11.1.3 Server room or other areas containing critical IT equipment must be secured using biometric access control mechanism.

11.2 Physical entry controls

11.2.1 Only those individuals, whose job description needs demand access to the Department's Information or Information Systems, must be allowed to enter the premises using an access card.

11.2.2 Visitors' entry into the premises must be restricted by appropriate security validations like checking the identity (company ID, driving license, voters ID etc) of the visitor, random frisking of visitors, checking their belongings and bags, etc.

11.2.3 Additional security controls like capturing the photograph of visitors entering into the Department's premises should be implemented based on the risk assessment of the building.

11.2.4 A confirmation from the visited employee must be taken before allowing a visitor inside the Department premises. Following information must be entered related to the visitor:

- Name
- Address
- Whom to meet
- Purpose
- Declaration of equipment/ devices
- Date
- Card no. given

11.2.5 All movement of material going in and out of premises must be duly authorized and tracked.

11.2.6 The Department employees must be given physical access only on a need to know basis of the activities conducted at the premises.

11.2.7 Access to all the visitors/ daily wagers must be determined/regulated strictly as per the requirements .Designated visitor areas may be there in every office.

11.2.8 Employees must not permit unknown or unauthorized persons to pass through doors requiring access cards, at the same time when they pass through them.

11.2.9 Employees and visitors must always wear Identification badge and ensure that it is visible.

11.2.10 Off-hour (other than normal business hours) access to the Department must be strictly controlled. In addition to identification badges, visitors must be made to sign in a visitor information system maintained by the security guard at the entrance. The visitor information system must indicate the name of the person, department, In-time, Out-time and the signature of the visitor.

11.2.11 All opening of the Data Centre/ server room should be monitored round the clock by surveillance video cameras.

11.3 Securing Offices, Rooms and Facilities

11.3.1 Depending on the sensitivity of information handled within, the physical security for offices, rooms and facilities must be designed and applied. Access to server room must be restricted. Only technical staff and those authorized must be allowed to access the Server room.

11.3.2 All the Department cabins must be locked after the employees leave for the day and must be checked by the security guards. The Department cabin keys must be kept with the Department employees only.

11.3.3 Personally-owned cameras, audio recording equipment, or video recording equipment must not be accessible or used within the Department facility.

11.3.4 Physical access control software must be maintained by the Department personnel only.

11.3.5 Loss of access cards/ keys must be immediately reported to the BISO, who shall take appropriate action to prevent unauthorized access.

11.3.6 The Department must employ and maintain automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.

11.4 Protecting against External and Environmental Hazards

11.4.1 The Department's offices must be fitted with appropriate firefighting devices at critical locations in order to arrest the fire and to avoid damage to the various resources of the Department. Selected Department employees must know how to use these fire-fighting devices.

11.4.2 Safety measures like fire and earthquake evacuation drills must be practiced regularly.

11.4.3 Appropriate safety measures must be taken to avoid loss and damage due to Water flooding or inappropriate drainage system within the premises of the Department.

11.4.4 Physical protection against damage from natural or man-made disaster must be designed and applied.

11.5 Working in Secure Areas

11.5.1 Any activity carried out in the Department's facility by an external party must be supervised.

11.5.2 Restricted access for the Department's premises to contracted support services personnel must be granted only when required and for the definite timeline. Their access must be authorized and monitored by the Department.

11.6 Clear-desk clear-screen policy

11.6.1 All information users are required to ensure that they maintain a clear desk while not at their desk. Users are also required to ensure that all documents that contain information that they work on be stored safe in the cabinets provided to them.

11.6.2 The Department must ensure that all the incoming mails are received and passed on to respective employee.

11.6.3 All information users must also ensure that there is no muster surfing over screen which can disclose confidential, secret or top secret information to unauthorized employees, third parties and contractors.

11.7 Public Access, Delivery and Loading Areas

11.7.1 The security guard at the reception must inspect all the consignment for any hazardous content. All the consignments must be recorded with their date and time of entry/ exit in the equipment movement register so that they can be traced back at any point of time.

11.7.2 Access points such as delivery areas and other points where unauthorized persons may enter the premises must be controlled and isolated from information processing facilities.

11.8 Equipment Siting and Protection

11.8.1 All the electronic office equipment including faxes, printers and EPABX, must be physically secured.

11.9 Security of Desktops and Network Hubs

11.9.1 Desktops must be adequately protected from fire, theft, water and pollution damage and power supply fluctuations.

11.9.2 Wherever necessary, hardware/ software security locks must be procured and installed on PCs as a protection against unauthorized access.

11.9.3 Networks hubs must be secured from fire, heat, dust and water.

11.9.4 Interception or damage to Network cables must be controlled.

11.10 Supporting Utilities

11.10.1Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities.

11.10.2There must be a provision to maintain regular power supply within the Department. Alternate power supply sources must be present to ensure a continuous power supply in the absence of primary power sources.

11.11 Cabling Security

11.11.1Adequate protection must be applied to protect power and telecommunications cabling carrying data or supporting information services from interception or damage.

11.12 Equipment Maintenance

11.12.1All Equipment must be correctly maintained to ensure its continued availability and integrity.

11.13 Security of Equipment Off-Premises

11.13.1Security must be applied to off-site equipment (e.g. Laptops) taking into account the different risks of working outside the organization’s premises.

11.14 Secure Disposal or Re-use of Equipment

11.14.1IT hardware and equipment must be disposed off only after approval. Further, appropriate data and media destruction should be performed prior to disposal. Disposal of retired hardware and media should comply with prevalent environmental regulations.

11.14.2The Department’s shall document risk-based media disposal process to remove Data from IT devices and media prior to disposal or re-use by using one or more of the following methods (including virtualized environments):

- Physically Destroy: Physical destructions must be performed in such a manner that the information contained can no longer be read or recovered.
- Digitally Wipe: Overwrite all locations a minimum of three (3) times (first time with a character, second time with its complement, and the third time with a random character).
- Degauss: subject storage media to concentrated magnetic field designed specifically to ensure insufficient magnetic remnants.

11.15 Removal of Information Assets

11.15.1Equipment, information or software must not be taken off-site without prior authorization.

11.15.2Any information asset required to be taken off-site must be recorded before it is taken off-site.

11.15.3Risk assessment or due diligence must be performed before the information asset is moved from its original location.

11.15.4No storage media within the Department must be allowed to be taken outside the Department under any circumstances. Defective storage media (e.g. hard disks) must not be handed over to the vendor under any circumstances. The faulty storage media should be retained by the Department.

12 Cryptography

12.1 Use of Cryptographic Controls

11.15.5Risk assessment must be carried out to identify the needs, methodology, work areas and usage of encryption or cryptography

11.15.6Cryptographic controls must be used for securing information that is top secret, secret and confidential. They must be used if the information could not be protected by any other means and wherever applicable and feasible

11.15.7The definition of top secret, secret and confidential Information will be based upon the respective Information Owner's discretion as per the Information Classification Policy

11.15.8Top secret, secret and confidential information that are not actively used, when stored or transported in computer-readable storage media (such as servers, magnetic tapes, floppy disks or CDs), must be in encrypted form wherever feasible and applicable.

11.15.9Information used to verify the identification of remote terminals for employees and other users must be appropriately protected. Static or reusable authentication information must be encrypted during storage and while passing through the network using encryption software or hardware.

11.15.10 VPN connections must be established with the remote users before they are allowed access to the sensitive information. The algorithm and key strength to be used must be decided in advance.

11.15.11 Remote users such as the reporting entities must establish connection using digital signatures as well as SSL connection to get access to THE Department information systems.

11.15.12 It is mandatory to use encryption system duly approved by the SAG/Cipher Bureau only, as per the "Crypto System Acquisition Policy 2006" or extant policy in place.

11.15.13 The PKI encryption infrastructure should be SAG/Cipher Bureau certified. The certificates to be used for PKI should be obtained from the Chief Controller of certifying Authority as per the Indian Information Technology Act 2000 and further IT (Amendment) Act, 2008.

12.2 Key Management

11.15.14 Type and strength of the encryption algorithm to be used in a given situation must be based on the criticality of the official information handled.

11.15.15 The length of the cryptographic keys must comply with contractual requirements, agreements and other regulations.

11.15.16 Where possible, encryption keys must not be transmitted over the network. If the keys used to govern the encryption process are to be transmitted over the network, then they must be transmitted through secure communication channels.

11.15.17 All cryptographic keys and passwords must be stored in a secure location.

12.3 Key Ownership

11.15.18 Administrative control for the encryption/ decryption key management and password management etc. must be with the Department and not with any vendor / third party.

13 INFORMATION SECURITY INCIDENT MANAGEMENT

13.1 Reporting Information Security Events and Weaknesses

11.15.19 An Incident is defined as the occurrence of any exceptional situation that could compromise the Confidentiality, Integrity or Availability of Information and Information Systems of the Department. It is related to exceptional situations or a situation that warrants intervention having the potential to cause injury or significant property damage.

11.15.20 Security weaknesses (vulnerability in the information system, which could be exploited to compromise the Confidentiality, Integrity or Availability of the system), software malfunctions (any abnormality or deviation in the functioning of a software application) and violations of the Department's security policies and procedures must also be considered an incident.

11.15.21 The Department must implement procedures for detecting, recording, analyzing, reporting, acting upon incidents immediately related to exceptional situations in day-to-day administration of the IT and information security related areas.

11.15.22 An incident management framework must be developed and followed to respond to an incident at the Department.

11.15.23 The incidents must be reported immediately to the appropriate authorities and corrective actions must be taken immediately to avoid the recurrence of such events in future.

11.15.24 All employees/ other users must also be made aware of the procedures for reporting different types of incidents (like security breach, threat, weakness, or malfunction) that might have an impact on the security of organizational assets.

11.15.25 All reported incidents must be logged, analyzed and classified according to predefined criteria mentioned in the Incident Management Framework.

11.15.26All employees and other users of information systems and services must be required to note and report any observed or suspected security weaknesses in systems or services.

11.15.27 Escalations and actions must be as per the classification of Incidents.

13.2 Contact with authorities

11.15.28 Appropriate contacts with relevant authorities must be maintained to escalate to the respective authorities as required.

13.3 Management of Information Security Incidents and Improvements

11.15.29 Management responsibilities and procedures must be established to ensure a quick, effective, and orderly response to information security incidents.

11.15.30 There must be mechanisms in place to learn from incidents and enable the types, impacts, and costs of incidents and malfunctions to be quantified and monitored.

11.15.31 Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence must be collected, retained, and presented to conform to the rules for evidence laid down.

13.4 Collection of evidence

11.15.32 The Department shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

13.5 Breach of information received from foreign authorities under tax treaties

13.5.1 The breach protocol in case of breach of any treaty related information must be activated immediately under the supervision of the Information Security Committee.

14 Information security aspects of business continuity management

14.1 Information security continuity

14.1.1 A managed process must be developed and maintained for business continuity throughout the organization that addresses the requirements needed for the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

14.1.2 A comprehensive Business Continuity Plan (BCP) must be developed and implemented in order to maintain or restore the Department operations in the required time scales following interruption to, or failure of, critical processes. The BCP must include effective Disaster Recovery procedures for quickly recovering from an emergency with minimum impact to the Department's operations.

14.1.3 Business Continuity Plan must be developed based on critical processes and the likely disruptive events along with their probability, impact and consequences for information security identified through Business Impact Analysis.

14.2 Testing of business continuity plans

14.2.1 BCP must be tested bi-annually to identify incorrect assumptions, oversights, or changes in equipment or personnel.

14.2.2 Test results must reported to PISO and must be used to revise the BCP

14.2.3 Emergency exits must be tested periodically to ensure that the access security systems are operational.

14.3 Business Continuity Planning Framework

14.3.1 A single framework of business continuity plans must be maintained to ensure all plans, across processes are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

14.4 Review of BCP

14.4.1 BCP must be reviewed bi-annually after each test and updated to ensure that the BCP considers the effectiveness of the current nature of processes, infrastructure, personnel, etc.

14.5 Redundancies

14.5.1 The Department shall ensure that Information processing facilities are implemented with redundancy sufficient to meet availability requirements.

15 Compliance

15.1 Compliance with Legal requirements

15.1.1 Identification of applicable legislation: All relevant statutory, regulatory and contractual requirements must be defined explicitly and documented for each of the Department's information systems. The Department must ensure compliance to each of the Laws and Acts relevant to its operations, wherever applicable. These will include but not limited to the Information Technology (IT) Act, MHA guidelines, Official Secrets Act, the guidance and instructions issued by the ITD from time to time, CERT-IN guidelines or any other laws or acts applicable to the organization.

15.1.2 Intellectual Property Rights: Procedures must be put in place to ensure that terms and conditions and license requirements of the copyrighted software or any other proprietary information used within the Department are complied with.

15.1.3 Protection of organizational records: The Department's organizational important records relating to Information Security must be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and official requirements.

15.1.4 Data protection and privacy of personal information: Data protection and privacy must be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

15.1.5 Prevention of Misuse of Information Processing Facilities: Information processing facilities must be used as per policies detailed in the Information Security Policy and User Policies and guidelines. Disciplinary action may be taken for any wilful violation to the policies.

15.1.6 Regulation of cryptographic controls: Cryptographic controls, wherever applicable, must be used in compliance with all relevant agreements, laws, and regulations.

15.2 Compliance with Security Policies and Standards and Technical Compliance

15.2.1 The Department management must ensure that all security procedures are carried out correctly to achieve compliance with security policies and standards.

15.2.2 Agreements with the third parties must specify the mandate for them to comply with the Department security policies and procedures.

15.3 Independent Technical Compliance Review & Reporting

15.3.1 Information processing resources and associated documentation must be reviewed immediately after installation and thereafter on a quarterly basis to verify that they are compliant with the security policies and standards. Findings and recommendations in the report must be communicated to the concerned department personnel for implementation.

15.3.2 The Department information processing resources must be reviewed by an independent third-party at least on an annual basis. The findings must be reported to senior management.

15.4 Information Security Reviews

15.4.1 The Department must conduct internal and external information security audits by competent independent internal and external auditors respectively to ensure compliance with the information security policies, procedures, standards and guidelines.

15.4.2 Formal procedures must be developed for planning and reporting audits and audit findings and ensuring the implementation of a prompt and accurate remedial action.

15.4.3 Audit requirements and activities involving checks on operational systems must be carefully planned and agreed to minimize the risk of disruptions to organizational processes.

15.4.4 Access to information systems audit tools must be protected to prevent any possible misuse or compromise.

15.5 Policy Review

15.5.1 The Policy shall be reviewed on a periodic basis and/or after any significant changes in ITD guidelines, technology changes, regulatory requirements or legal requirements to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the Policy.

15.5.2 The results of the reviews shall be clearly documented, and records shall be maintained.

INCOME TAX DEPARTMENT
GOVERNMENT OF INDIA

ITD Acceptable Usage Policy 2020

Contents

1. Introduction

The purpose of this policy is to establish acceptable and unacceptable use of assets of Income Tax Department. Income Tax Department provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and all users must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets.

2. Scope

This policy applies to all End Users (Income Tax Department employees, contractors, consultants, third parties and their affiliates) having access to Income Tax Department resources.

3. Acceptable Usage Standard

3.1 Software Usage

3.1.1. The organization has licensed the use of certain commercial software, applications, operating system, database, programs (e.g. MS Windows, MS Office and Anti-Virus) for official purposes.

3.1.2. No user should create, use or distribute copies of such software that are not in compliance with the license agreement for the software. Violation of this protocol may lead to disciplinary action including penalty.

3.1.3. Preservation, use or distribution of cracked / pirated / unlicensed version of software is not permissible and illegal.

3.2 System and IT Asset Usage

3.2.1 Restrict physical access to desktop, laptop, handheld devices to authorized personnel only.

3.2.2 Secure desktop / laptop (screen-lock / log-out) prior to leaving the workstation to prevent unauthorised access.

3.2.3 Ensure IT assets are used for authorised purposes only.

3.2.4 Do not share password with anyone, even with the system / network administrator.

3.2.5 Keep eatables away from workstations to avoid any accidental spills.

3.2.6 Do not try to install, modify or uninstall any software by your own. If required to do so, seek prior approval and seek assistance of authorised personnel.

3.2.7 If any malfunctioning of system / network resources is noticed, do not try to fix it. Inform helpdesk on priority to get this resolved.

3.2.8 Always shut down the workstation properly before leaving it unattended for a long duration or at the end of work for the day.

3.2.9 Do not store any personal data in organization provided systems.

3.2.10 No personal devices like computer, laptop or smart devices should be connected to the organization's network. If requirement justifies to do so, seek assistance of helpdesk.

3.2.11 In case of loss, damage or theft of organization's asset, employee should immediately inform supervisory officer formally about the incident.

3.2.12 Assets which are not in use / pertaining to any separated employee must be handed over to authorized person.

3.3 Network Usage

3.3.1 Organization provided systems (e.g. laptops, desktops, and handheld devices) may be configured to get connectivity to organization's network by either connecting through LAN cable or Wi-Fi at dedicated zone inside office premises. Users are not required to configure anything on their own to get the connectivity.

3.3.2 In the event of inaccessibility to the organization's network, do not try to tamper with network settings and LAN cables / devices. Inform the helpdesk support staff instead.

3.3.3 Do not switch off the network devices like network switches, routers, Wi-Fi access point etc.

3.3.4 Assets like laptop, handheld devices etc., not pertaining to the Income Tax Department should not be connected to ITD's network. In case of appropriate requirement, a formal approval should be taken from supervisory officer. Once approved, technical support personnel may facilitate the same on a limited connectivity based on actual requirement.

3.3.5 Wireless Access Point passwords should not be shared with anyone under any circumstances.

3.3.6 Do not send unnecessary traffic, such as chain mails, on the network.

3.3.7 Disruptive behaviour, such as introducing malicious codes or intentionally destroying or modifying files on the network is strictly prohibited.

3.3.8 In the event that the user is aware / suspects that his / her system is compromised / affected by any malware, he/she should not connect the system to the organization's network. The user should get in touch with helpdesk personnel on priority basis.

3.4 Internet Usage

3.4.1 Any personal use of the network for commercial, illegal or unethical purposes is strictly prohibited.

3.4.2 Email and file transfers are for official use only by authorized users.

3.4.3 Use of other user's credentials for internet use is strictly prohibited.

3.4.4 Confidential information is not to be transmitted over internet. If confidential information is required to be transmitted over internet, the information must be encrypted and approval from supervisory officer must be obtained for sharing confidential information over internet.

3.4.5 Access to obscene, pornographic or offensive sites is strictly prohibited.

3.4.6 Individual users are responsible for ensuring that antivirus software is installed in their workstation and up-to-date.

3.4.7 Playing on-line games / gambling is strictly prohibited.

3.4.8 Casual browsing websites or social networking sites are not to be accessed during office hours unless it is required for official purposes.

3.4.9 Any attempt at defeating of security restrictions on organization systems and applications is strictly prohibited.

3.4.10 Do not download unnecessary software, songs, and videos from the internet. These take up significant internet bandwidth and may adversely affect functionalities.

3.5 Mail Usage

3.5.1 Mail id creation, change in mail configuration, mail id revocation is sole discretion of Systems.

3.5.2 Use organizational mail box for official correspondences only. Personal mail id should not be used for official communications.

3.5.3 Employees must be aware that the electronic mail messages sent and received using organizational resources are not private and are subject to viewing, downloading, inspection, release and archiving.

3.5.4 Always be cautious before opening any email, unless user is confident that it is coming from legitimate source and the communication is expected. In case of detecting any suspicious mail, consult with Technical support on priority basis.

3.5.5 Sending / forwarding chain mails, spam mails are prohibited.

3.5.6 Abusing, usage of profane, threatening, racist, sexist or otherwise objectionable language / content in either public or private communication is strictly prohibited.

3.5.7 Causing congestion, disruption, disablement, alteration or impairment of organization's mail system is objectionable.

3.5.8 Avoid sending large size attachments over email. If required so, consult with Systems and use shared network folder / ftp services instead.

3.5.9 Do not reply to any spam mail, even if it gives instruction to do so.

3.5.10 Mail Attachment limit/restriction, in-coming / outgoing and Bulk Mail restrictions will be implemented and will be reviewed on need basis.

4 Exception

If any acceptable usage requirement has any implementation discrepancies, then the same must be recorded, justified with risk assessment where applicable and approved by the CISO.

5 Compliance

Any employee or personnel found to have violated this policy is subject to disciplinary action that will be handled via existing rules, regulations and procedures.

***