This document is to be used to communicate a consistent notion of IT Security related Management directives to the HP Treasuries organization

IT Security Policy Manual

DTA,Govt. of Himachal Pradesh

CyberQ Consulting Pvt. Ltd.

Document Control

Document Name	Information Security Management System Manual
Document Reference Number	HPDTA/ISMS/SM
Classification	Internal
Version Number	D 1.3
Date	03.11.17
Reviewed by	
Approved by	

Revision History

Date	Version	Description	Created By
23.06.17	D 1.0	First Draft	ISMS Team
14.07.17	D 1.1	F.B. from HQ review incorporated	ISMS Team
01.09.17	D 1.2	F.B. from Dharmshala w/s incorporated	ISMS Team
03.11.17	D 1.3	All comments from HQ incorporated	ISMS Team
01.12.17	V 1.0	Baselined	ISMS Team

Distribution

- File server
- Intranet Portal

Documentation Status

This is a controlled document. This document may be printed; however, any printed copies of the document are not controlled. The electronic version maintained in the file server and Intranet ISMS Portal is the controlled copy.

Related documents

S. No.	Document Reference Number	Document Name	Version
1	HPDTA/ISMS/ITAUP	IT Acceptable Use Policy	V1.0
2	HPDTA/ISMS/CHKLST	HPDTA Audit Checklists	D 1.0

Acronyms and Abbreviations

Term	Description
Govt.	Government of India
CERT-In	Indian Computer Emergency Response Team
CMD	Chairman cum Managing Director
HPDTA	Himachal Pradesh Directorate of Treasuries Accounts and Lotteries
HOD	Head of Department
DTO	District Treasury Officer
SMS	Security Management System
ISSC	Information Security Steering Committee
ISDR	Information Security Department Representative
SIRT	Security Incident Response Team
CISO	Chief Information Security Officer
ITSM	IT Support Member at DTO/TO

TABLE OF CONTENTS

1. Introduction

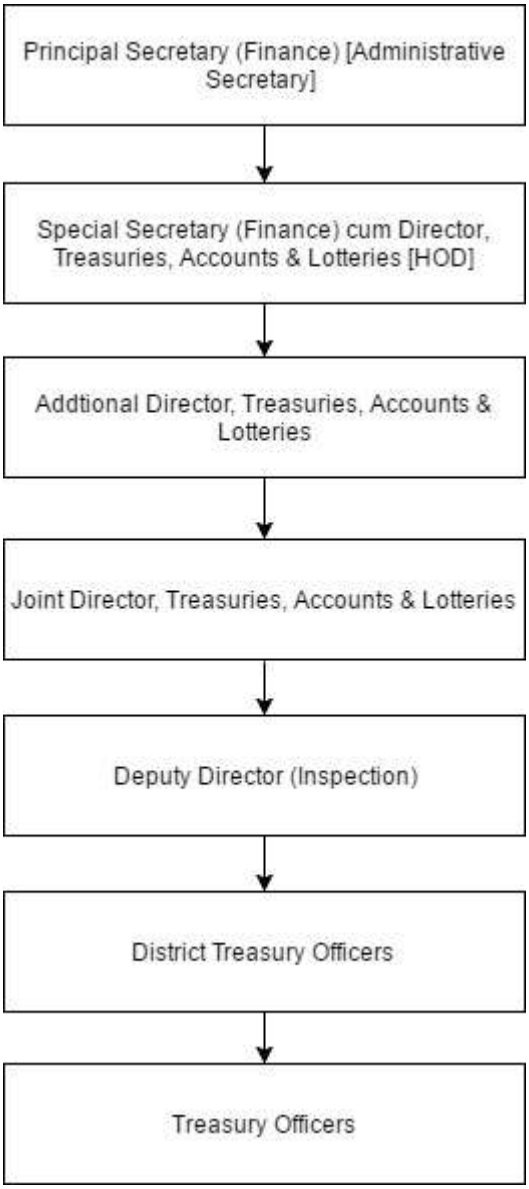
The Directorate of Treasuries Accounts and Lotteries (DTA) is responsible for carrying out financial transactions and payments on behalf of the Himachal Pradesh State Government. The DTA is an integral part of the Finance Department and is responsible for all government financial transactions inter alia collection of government receipts, making payments on behalf of the state, and compilation of accounts for rendition to the state's Accountant General (AG). The DTA has 18 Treasuries and 87 sub-treasuries across the state under it which provide its services to the various Departments through their Drawing & Disbursement Officers (DDOs). The DTA is catering to a large number of internal and external customers including 4700 DDOs, 200,000 employees, 120,000 pensioners, and 62,000 NPS subscribers besides a large number of vendors. The DTA has undertaken multiple modernization steps to increase the efficiency and effectiveness of service delivery. These include development and deployment of various application software like Online Treasury Information System (OLTIS), e-Vitran, e-salary, e-pension, Cyber Treasury, e-NPS, e-Kosh etc. Modernization of treasury functions has been very rapid and significant, but the new ways of functioning were not evaluated with respect to the information security threats. This can pose significant risks in future. GoHP, with technical assistance from the World Bank, has undertaken an information security risk assessment of its treasury operations and IT systems with an objective of creating a comprehensive IT Security Policy for DTA.

2. Purpose

The purpose of this IT Security Policy Manual is to communicate a consistent notion of Management directives to the HP Treasuries organization for performing its operations in a secure manner while conforming to the business, technical, legal and regulatory environment of HP Treasuries.

3. Context of the Organization

The Directorate of Treasuries Accounts and Lotteries (DTA) is responsible for carrying out financial transactions and payments on behalf of the Himachal Pradesh State Government. The hierarchical structure of the DTA is as follows:



Administrative control of all Treasuries and Sub Treasuries in the State rests with this Department. Apart from this, the department is also responsible for making available to all other departments, Boards and corporations, the trained and skilled personnel of Subordinate Accounts Services cadre to exercise effective check and control over the Finances of Government.

Functions of the Department:

i. Financial transaction of State Government
   a. Receipts due to the Government
   b. All payments on behalf of Government.
ii. Proper Accounting/compilation of Government Accounts
iii. Rendition of accounts to the Accountant General
iv. Nodal agency for procurement and distribution of Non-Postal stamps.
v. Custodian of valuables, opium etc.
vi. Nodal agency of Pension disbursement system.
vii. Supplying of voucher No. and CTRs to the DDO's
viii. Budget control / Financial control of DDO's.
ix. Advisory Role in Financial matters to DDO's.
x. As a banker in Non-Banking Sub Treasuries.
xi. Nodal agency for NPAs.

3.1. Stakeholders (External and Internal)

The information resources of HPDTA are being utilized by various departments across HPDTA and also by the DDOs' offices in various departments of Himachal Pradesh in support of the treasuries functions. The interested parties, relevant to information security, are:-

1. Drawing and Disbursement Officers of various departments and their staff:

   The services of these offices contribute directly to the main operations of the treasuries department and hence their handling of information resources is of vital importance with respect to the information security of HPDTA.

2. National Informatics Centre, Shimla:

   The development and maintenance of the HIMKOSH applications are the responsibility of NIC, Shimla. The ability of these applications to defend against cyber-attacks are therefore dependent on security features built into these applications.

3. HIMSWAN:

   This agency provides the Wide-Area Network connectivity services to many HPDTA offices and DDOs across the state. Together with connectivity, they also additionally provide certain technical security controls to their users.

4. BSNL:

   This ISP provides basic internet connectivity service to many HPDTA offices and DDOs who are not on HIMSWAN.

5. NIC Cloud:

   The HIMKOSH applications together with their databases are hosted by the NIC Cloud services. It is understood that the service provider is responsible for taking care of all the security related aspects for these information assets.

6. HPSEDC:

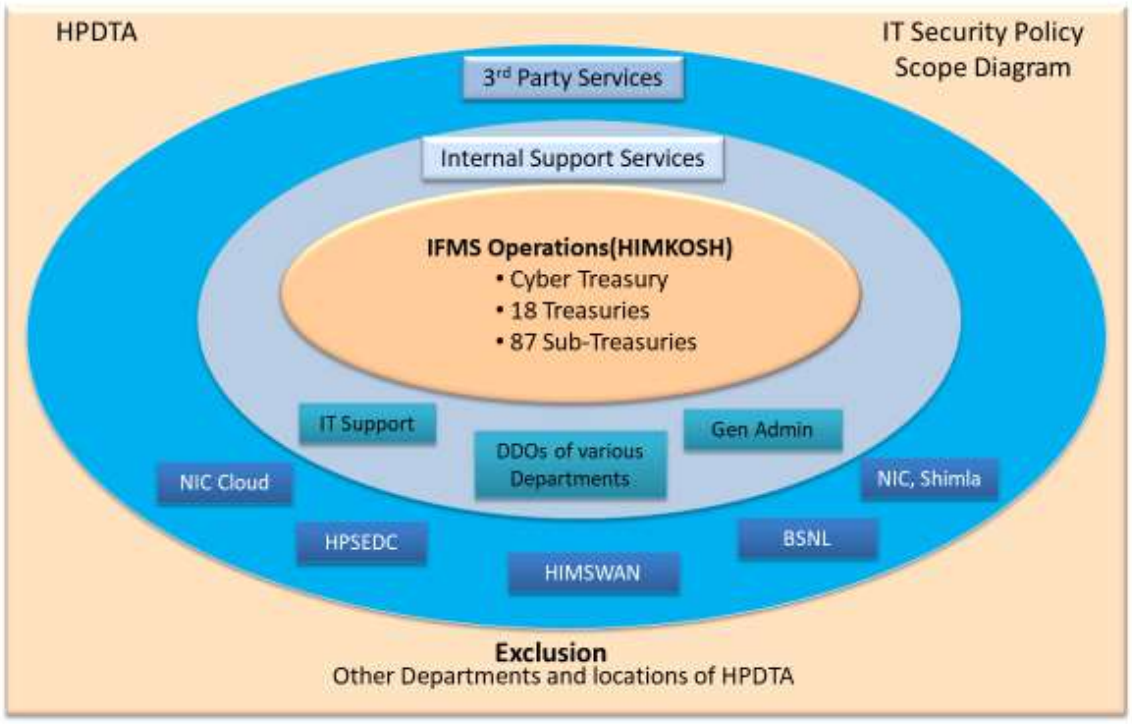
   HP State Electronics Development Corporation Ltd. is entrusted with the responsibility of supply and maintenance of all IT hardware and software to HPDTA offices.

3.2. Scope

The Scope of the IT Security Policy, described in this document, thus encompasses all the stakeholders mentioned in the section above and it embraces the following:

- HIMKOSH operations and its Information Assets,
- Internal Support Services related to HIMKOSH operations,
- Third Party Services related to the HIMKOSH operations.

The Scope of the IT Security Policy, thus, can be pictorially described as shown below:



4. Leadership

4.1. Leadership and commitment

The top management of HPDTA is committed to information security in the organization and has demonstrated leadership and commitment to the information security management system by establishing Information Security Policy in line with the business strategy of HPDTA.

Directorate of Treasuries, Accounts & Lotteries

Government of Himachal Pradesh

Information Security Policy

Directorate of Treasuries, Accounts and Lotteries, Government of Himachal Pradesh, is committed to ensure the confidentiality, integrity and availability of information to all employees and the users of HIMKOSH (the Integrated Finance Management System, Himachal Pradesh). This shall be achieved by meeting regulatory requirements, business continuity planning, developing competencies and adopting innovative and state of the art strategies to suitably address Information Security.

The Information security policy aims to protect the information of all Treasuries and Sub-treasuries of the state from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimize damage and maximize efficiency and effectiveness of service delivery.

This policy has been approved by the Director of HPDTA. It is applicable to and shall be communicated to all employees, stakeholders and interested parties.

Other than the above “Information Security Policy”, a set of supporting policies for security shall be defined, approved by management, published and communicated to employees and relevant external parties. These policies are defined in sections 9 to 27 of this document.

4.3. Organizational Roles and Responsibilities

An Information Security Steering Committee (ISSC) shall be established to ensure that the responsibilities and authorities for roles relevant to Information security are assigned and communicated. The ISSC shall be chaired by the Director of HPDTA and have the following members:

a) Director, Treasuries : Chairman
b) Additional Director : Chief Information Security Officer (CISO)
c) Joint Director : Member Secretary
d) Deputy Director : Member
e) DTO of Cyber Treasury : Member
f) DTOs of all Districts Treasuries : Guest Members (on invitation)
g) SIO of NIC, Shimla : Guest Member (on invitation)

The ISSC shall implement the Security Policies across the organization with active assistance from the following:

1. TOs of all Sub-Treasuries
2. DDOs of various departments
3. IT Support Team at HQ
4. IT Support Member in each Treasury office :

The responsibilities related to Information Security for the ISSC team are as defined below:

4.3.1. Responsibilities of ISSC

1) Focal point for decisions on all Information security issues;
2) Approving the release of Information Security Policies and related processes in the organization (including DDOs' offices);
3) Ensuring implementation of established Information Security Policies and related processes across the organization;
4) Assessing the adequacy of information security policies through conduct of periodic Information Security Audits as per Information Security Audit Policy (ref Section 5);
5) Ensuring Corrective as well as Preventive measures to close all non-conformities identified during the Information Security Audits, in a timely manner;
6) Creation of a Security Incident Response Team (SIRT) and its effective operations as per Security Incident Management Policy (ref Section 25);
7) Coordinating with NIC, HIMSWAN and BSNL for ensuring business continuity of Treasuries operations utilizing NIC Cloud services and connectivity from HIMSWAN and BSNL;
8) Ensuring appropriate awareness and training programs for HPDTA employees, DDOs and their staff, contractors and users of HIMKOSH to comprehend organization's security policies;
9) Ensuring that all individuals involved in HIMKOSH operations and use of its information assets commit to adhere to IT Acceptable Use policy;
10) Seeking advice from relevant domain experts on issues of information security;
11) Initiating appropriate disciplinary process in case of Information security breaches;
12) Establishing and maintaining contacts with all relevant external information security groups under Govt. of India;

13) Implementing fire incidents management and other physical security related processes in office premises;
14) Holding regular ISSC meetings at least once every three months.

4.3.2. Information Security Related Responsibilities of Other Officials

ROLES / BUSINESS PROCESS	DEALING HAND AT DDO	DDO	DTO/TO
New Employee Registration	Dealing hand to ensure correctness and completeness of all entries while preparing new employee form.	All entries in form to be verified and then to be sent by DDO.	To do complete-ness check of supporting documents and verification of entries made by DDO for all cases.
Transfer of Employee	Changes in allowances / deductions to be correctly entered	DDO to verify correctness of changes made by dealing hand	To cross-check changes in all cases.
Monthly salary processing	Changes to allowances/ deductions/ increments to be correctly done for each employee	DDO to check changes to allowances/ deductions/ increments and submit to DTO	To verify the correctness of salary bills and their authenticity in all cases
Vendor Registration	Ensure all entries are correctly filled, e.g account details.	DDO to verify vendor details filled by dealing hand	
Messenger registration		To select a trusted person as messenger	
Bill Passing and Processing	Dealing hand to ensure all entries are correctly filled	Bills must be submitted only by DDO through their respective logins.	Scrutiny to be done for supporting docs for all bills submitted by DDO

General	(1) Pass-words not to be shared (not even within the team) (2) Everybody in team to change pass-words in case of exit of any member	(1) DDO not to share pass-word with his staff (2) DDO to change pass-word in case of exit of any staff member	(1) DTO/TO not to share pass-word with his staff (2) DTO/TO to change pass-word in case of exit of any staff member

4.3.3. Internal Auditors

- Planning internal information security audits in the organization.
- Conducting of internal information security audits as per audit program/plan.
- Reviewing and analyzing root cause of non-conformities.
- Consolidation of Internal Audit findings and submission of audit report to concerned authority.
- Authorized to report the findings and closure status directly to the CISO.

4.3.4. Security Incident Response Team (SIRT)

- To contain and mitigate the impact of any information security incident, a Security Incident Management Committee (SIRT) shall be created by the Information Security Steering Committee in its first meeting, their responsibilities and authority shall be as follows:
- The SIRT is responsible to create and implement a mechanism for reporting, containment, mitigation, and correction of any information security incident.
- The guidelines for the security incident management is detailed in the document on Information Security Incident Management Process (section 25).

4.3.5. IT Support Team at HQ

- Facilitate the creation and deletion of email IDs by NIC, on request from the HODs of the users
- Inventory Audits will get conducted by the CISO through assigned team members from IT Support Team at HQ
- At the Treasuries HQ, the services of the ISP and HPSEDC will be periodically monitored for compliance against their committed SLAs by the IT Support Team
- Coordination and technical guidance to the IT Support Members at all Treasury offices

4.3.6. IT Support Member at each Treasury Office

- IT Support Members are required to maintain inventory of hardware and software in their respective offices
- DTO/TO, through their IT Support Members, shall organize removal and allocation of Application access rights for users, upon resignation or transfer

- IT Support member shall be the **System Admin** for all the IT systems in his/her office and is responsible for implementing general operating system access controls on user PCs or Laptops
- To take care of updates or upgradation of applications, operating systems and anti-malware solutions, as and when needed
- To periodically monitor for compliance the services of the ISP and HPSEDC against their committed SLAs and to report the findings to the IT Support Team at HQ
- To act as IT Support advisor to the concerned DDOs, as and when needed

5. Internal Audit

Policy : *"Establish, implement and define methods to carry out Internal Information Security Audits for verifying effective implementation and maintenance of Information Security Policies"*

6. Tasks

6.1. Audit Planning

- The annual audit programme shall be made at the beginning of the calendar and shared with the respective stakeholders (Refer: Annexure 1: Annual Audit Programme Template).
- All changes in the audit programme shall be approved by CISO.
- Internal Auditors who will be selected shall be independent from the area/function under scope.
- Internal Audit shall be conducted at least once in every six months.
- ISSC shall ensure the competencies of the Auditor carrying out Audit.
- The Auditor shall communicate the scope of the audit and audit criteria to the respective ISDR beforehand (Refer: Annexure B: Audit Plan Template).
- All changes in the audit plan shall be approved by CISO

6.2. Execution of the Internal Audit

- The Audit shall be carried as per Audit plan shared and with the help of Audit Checklists provided in the document HPDTA Audit Checklists
- The Audit shall be done on sampling basis.
- The Auditor shall note down the observations during the Audit and keep the auditee informed about the findings.

6.3. Audit Closure

- The auditor shall conduct the closure meeting of the audit.
- The auditor shall brief out the findings both positive and Non Conformances in the closure meeting.

6.4. Audit reporting

- The Auditor shall submit Audit report to the CISO
- CISO shall share the Audit Report with the respective department and ask for RCA, Corrections and CA plan.
- ISDR shall review the closure of NC and share report in the next Audit
- All major NCs shall be reviewed by CISO.

Internal audits are conducted half yearly to provide information whether the information security management system of the organization conforms to the:

- Requirements of its own information security management system;
- Requirements of the International Standards applicable
- Is effectively implemented and maintained;
- Audit programmers that take into consideration the importance of processes concerned and results of previous audits are planned, implemented and maintained;
- Audit criteria and scope for each audit are defined;
- Auditors are selected;
- Audits are conducted to ensure objectivity and impartiality of the audit process;
- Results of the audits are reported to the relevant management;
- Documented information as evidence of the audit programmers and audit results is retained;

6.5. Management Review

Reviews of the information security management system are conducted by chairperson of ISSC at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The following are taken into consideration in management reviews:

- Status of reviews from previous management reviews;
- Changes in external and internal issues those are relevant to the information security management system;
- Feedback on the information security performance, including trends in:
  - Non conformities and corrective actions;
  - Monitoring and measuring results;
- Audit results;
- Fulfillment of information security objectives;
- Feedback from interested parties;
- Results of risk assessment and status of risk treatment plan;
- Opportunities for continual improvement;

Decisions related to continual improvement opportunities and any needs for changes to the information security management system are included in outputs of management reviews.

Documented information as evidence of the results of management reviews is retained by the organization.

7. Improvement

7.1. Nonconformity and corrective action

When nonconformity occurs, the organization reacts to the nonconformity, and as applicable,

- Takes action to control and correct it;
- Deals with the consequences;
- Evaluates the need for action to eliminate the causes of nonconformity so that it does not recur, or occur elsewhere by:
- Reviewing the nonconformity;

- Identifying the causes of the nonconformity;
- Identifying if similar nonconformities exist or could potentially occur;
- Implements any action needed;
- Reviews the effectiveness of any corrective action taken;
- Makes changes to the information security management system, if necessary;
- Corrective actions that are appropriate to the effects of the nonconformities encountered are taken;
- Documented information, as evidence of the nature of the nonconformities and any subsequent actions taken, is retained by the organization;
- Documented information, as evidence of the results of any corrective action, is retained by the organization;

7.2. Continual improvement

The suitability, adequacy and effectiveness of the organization's information security management system are continually improved upon.

8. Information Security Policies

9. Human Resource Security

Policy : *"Security roles and responsibilities of employees, contractors and third party users shall be aligned with HPDTA's information security policy. Adequate level of awareness, education and training in security procedures and correct use of information processing facilities shall be provided to them to minimize possible security risks. The change in responsibilities of employees and/or their exit from the organization shall be securely managed. In case of any breach of the security policies, HPDTA shall initiate internal investigation through a formal committee, which shall be formulated by the CISO. The same may have one or more committee members. This is a confidential process and the CISO shall take appropriate decisions on penalties based on the merits of the case."*

10.Tasks

10.1. Information Security Awareness, Education and Training

For a security awareness program to have an impact, it must be communicated to the employees, contractors and third-party users on a regular basis. Communication methods that repeat and reinforce lesson objectives from annual trainings may include but are not limited to-

- Emails
- Posters
- Intranet site
- Quizzes

The general aspects of information security which need to be covered in the IS awareness training program will be as follows-

- Responsibility of management for information security throughout the organization.
- Need to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts and agreements.
- Accountability of process owners for their actions and general responsibilities towards securing or protecting information belonging to the organization and its stakeholders.
- Information security awareness for-
    - Cyber attacks
    - Password Policy
    - Social Engineering
    - Clear Desk and Clear Screen policy
    - Physical Security controls
- Awareness about the basic controls (such as password security, malware controls and logical access controls etc.).

- Awareness about user's responsibilities to comply with HPDTA's security policies and procedures.
- The training plans are reviewed by ISSC at least once a year.
- The contents of training material are always kept updated so that it remains in line with HPDTA's current policies and procedures.

10.2. Post Training

- Training attendance sheet is maintained;
- Trainees are assessed during the training by the trainer;
- Trainees are required to give feedback for the training conducted;
- Feedback given by trainees is collated and analyzed;
- ISSC is updated on the results of analysis;
- Continual improvement is taken on the basis of the result of analysis;

11.Asset Management

Policy : *"All assets shall be accounted for and have a nominated owner. Acceptable use of assets shall be established. Information shall be classified to indicate the need, priorities and expected degree of protection."*

12. Task

12.1. Inventory of assets

- Assets associated with information and information processing facilities are identified and an inventory of these assets is drawn up and maintained;
- The asset inventory is always kept updated;

12.2. Hardware and Software Inventory Updating

- DTO/TO, with the help of his nominated IT Support staff member, maintains an Inventory Register for Hardware and Software in his office.
- Hardware includes network devices, external hard disks, CDs, pen drives and desktops.
- This Inventory Register is updated in the following cases:
    - New hardware/software is procured
    - Allocation of hardware is changed to another user
    - Software is installed/un-installed from a system
    - Hardware is removed

12.3. Inventory Audits

- CISO assigns team members from IT Support staff at Treasuries HQ for the inventory audits.
- Team members refer to the Inventory Register and cross check the entries.
- The systems are checked for the hardware information that includes ID, make, model, configuration and service tag number, serial number, IP address, host name, user and department information, and software installed (including License status, type, version number).
- In case of any discrepancy, DTO/TO or his designated IT Support member is informed and the discrepancy is resolved.
- This Inventory Audit is done half-yearly.

12.4. Acceptable use of assets

- Rules for the acceptable use of information assets are defined and communicated in IT Acceptable Use Policy(Refer-HPDTA/IS/ITAUP : IT Acceptable Use Policy);
- All users having access to the information assets need to be aware and accept the information security requirements associated with them;

12.5. Return of assets

- All users are required to return the organizational assets that they have in their possession, upon termination or transfer of their employment, contract or agreement.

12.6. Information classification

12.6.1. Information Asset Identification and Classification

Identification and Classification of information assets is done on the basis of the business needs and the impact of asset loss on the continuity of business. The asset owner identifies the assets in their respective Treasuries/Sub-treasuries.

12.6.2. Classification of Information

Information Assets - All information assets (soft/hard copy) are classified based on their confidentiality requirement as:

- Confidential
- Restricted
- Internal
- Public

Confidential: Confidential information is the most sensitive form of information. It is so sensitive that disclosure or usage would have a definite impact on HPDTA's business. Extremely prohibitive controls need to be applied.

Restricted: Restricted information is a sensitive form of information. This information is distributed on a "Need to Know" basis only. This information should be made available only to specific group of people within the department.

Internal: Such information is the property of HPDTA. HPDTA have the sole right over this information. This form of information must be used within HPDTA and not shared externally or with third parties unless authorized to do so.

Public: Sharing of such information does not have any impact on the confidentiality of the information asset and thus has a very low confidentiality rating. This form of information comes from public sources or is provided by HPDTA to the general public.

12.6.3. Labeling of Physical Assets

Physical assets, e.g., Desktops, Laptops & network devices, external media are identified by unique numbers, which are created using the following Asset Identification Numbering convention.

Each Asset Number is made up of four fields placed in the following sequence

Location/Type/Year of purchase/Serial Number (e.g. KLU1/RTR/15/010)

Location field: Office location represented by three letters in capital followed by one numeral, e.g. SML2, KLU1, etc.

Type field: The type of equipment or asset represented by three letters in capital, e.g. SRV (server), LAP (laptop), COM (workstation or PC), RTR (router), SWC (switch), UPS (uninterruptable power supply), MON (monitor), LCD (LCD screen), PRJ (projector), PRT (printer), PCP (photo-copier), etc.

Year of purchase field: The calendar year in which the subject asset has been purchased which is represented by last two digits of the year, e.g., 10 (2010), 17 (2017), etc.

Serial number: This is a sequence number given to the asset in a sequential fashion for the year and for the particular location or office. This field consists of three digits starting from 001.

The asset identification numbers thus formed are printed on long-lasting and water-proof material tags and pasted to the subject assets on easily discoverable surface, e.g., on top right corner of a Laptop.

12.6.4. Labeling of Documents

In case of electronic documents, headers/footers are to be added to clearly indicate the labelling.

12.6.5. Handling of Assets

	Confidential	**Restricted**	**Internal**
Copying	Extremely restricted	Copies to be accounted for in the Asset Register.	Copies should be restricted.
Storage	Access should only be with the owner, and senior management as designated by the owner	Access should only be with the owner, senior management and third party as designated by the owner. Backup copies to be maintained offsite.	Read access to the whole organization. Backup copies to be maintained offsite.
Transmission	Transmission using encryption or password protection only	Can be sent through email	Can be sent through mail, courier or fax. Security should be

			ensured in case of courier
Destruction	Any copies not in use should be destroyed securely.	Any copies not in use should be destroyed securely.	Any copies not in use should be destroyed securely

12.7. Media Handling

12.7.1. Management of removable media

- Refer HPDTA/ISMS/ITAUP : IT Acceptable Use Policy

13. Access Control

Policy : *"Allocation of access rights to information systems, network and services shall be controlled. User shall be made aware of the responsibilities for maintaining effective access controls."*

14. Tasks

14.1. General rules for access control

The following are considered when specifying access control rules:

- Differentiating between rules that must always be enforced and rules that are optional.
- Rules will be based on the premise, "All must be generally forbidden unless expressly permitted".
- Changes in user permissions that are initiated automatically by the information processing system and those initiated by an administrator.
- Rules, which require administrator or other approval before enactment and those which do not.
- No user accounts or group accounts are created for any user having external domain to the organization.

14.2. User Access Management

Granting Access Right

Level of access that is granted to the users through information systems is appropriate to the business purpose.

User Registration for HIMKOSH (IFMS) Applications

- The DDO of the department/office, to which the applicant belongs, raises a request for granting access to the HIMKOSH applications by writing a letter to the related DTO/TO in the format provided in Annexure 6A and filling in the attached IPAO-DDO-Login Request Form.
- After validating the authenticity of the application, the DTO/TO creates login credentials for the applicant who can be either a DDO or a Dealing Assistant. The IP number of the concerned DDO or the Dealing Assistant is used as the User ID for access to the HIMKOSH applications.
- The Password, thus created, is conveyed to the originating DDO's office in the IPAO-DDO Login Request form in the format provided in Annexure 6A, and acknowledgement received back.
- A copy of the IPAO-DDO Login Request form is retained by the Treasury for record purposes and the original form returned to the DDO's office in a sealed envelope with a covering letter in the format provided in Annexure 6B.
- For registration of users in the offices of the Treasuries, login credentials are issued using similar process.

- A formal record of all users, registered to use the restricted service, is maintained by DTO/TO.
- The user rights are reviewed periodically (quarterly) by DTO/TO to ensure that the access is in line with the job requirements and records of the same are maintained. They are modified whenever the user's work profile changes. All redundant User IDs are removed.
- Concerned department heads must inform DTO/TO about all users who are transferred to other departments or who leave the organization. The access rights of such users are removed/ updated immediately by DTO/TO.

For Emails

- Access to email is by webmail, given to authorized users only.
- User raises a request for email ID, with approval from department head, to Treasury Headquarter
- New email IDs are only created by Treasury Headquarter officials.
- New user subscription form is filled at https://mail.gov.in/ for single or multiple email IDs.
- Email ID and temporary password are then sent to users registered mobile no. by NIC.
- Only the E-mail account provided by the Department shall be used for official communication.

14.3. Password Management of User Accounts and network devices

Refer IT Acceptable Usage Policy V1.0

14.4. Guest Accounts for Internet Usage

Guest accounts are created / extended for a limited duration only after approval from DTO/TO, which are removed when their purpose is completed.

14.5. User password setting guidelines

Refer IT Acceptable Use Policy V1.0

14.6. Operating system access control

IT Support Member is responsible for implementing the following general operating system access control functions:

- Applying user identification and authentication mechanisms.
- Access to specific information resources e.g., system level application resources and data will be authorized by the IT Support Member.
- Access to operating system source files, configuration files and file directories is restricted to IT Support Member only.
- Create and change user profiles.
- Access to system utilities is given only to the IT Support Member.
- Only IT Support Member are allowed to access system logs or audit logs for review purposes.

14.7. Application level access control

- Provide access control for the module level in application system.
- e.g., Billing person may be allowed to access only those menus that allow entry of bill details, but do not allow access to menus that allow access to other modules.
- Restricting users' knowledge of information or application system functions, which they are not authorized to access with appropriate editing of user documentation.
- Controlling the access rights of users, e.g. read, writes, delete and execute.
- Ensuring that outputs from Application Systems handling sensitive information contain only the information that is relevant to the use of the output and is sent only to authorized terminals and locations.

Periodic review of such outputs to ensure that redundant information is removed (specific to the application being handled).

14.8. Access to computer features that bypass security

Computer vendor supplied privileged logon IDs are changed immediately upon installation.

14.9. Password Policy

Refer IT Acceptable Usage Policy V1.0

15.Physical and Environmental Security

Policy :*"Organization's sensitive information processing facilities shall be housed in secure areas. Physical protection shall be provided against natural and man-made disasters. Access to premises shall be controlled."*

16. Tasks

16.1. Secure areas

16.1.1. Physical Security Perimeter and Entry Controls

- The security perimeter is defined. The strength of perimeter is directly proportional to the criticality of the assets to the business;
- Entry to the Strong room is controlled and access is restricted to the authorized personnel only;
- Physical barriers are built to prevent unauthorized physical access and environment contamination;
- Office areas housing workstations/network equipment, and document storage rooms are not accessible to public and unauthorized personnel.
- Appropriate physical entry controls are implemented in the organization;
- Visitors/Service Engineers are not allowed to take Laptop, Pen Drive / External HDD or any other media inside the working areas.

16.1.2. Protection against environmental threats

- Fire Fighting equipment is suitably placed in working areas by Fire and Safety department and they are maintained as per the instructions by suppliers;
- Combustible material other than the information asset or its components are not stored within or in proximity to office areas housing workstations/network equipment;
- Large lead-acid batteries used in UPS equipment are also kept away from Office areas housing workstations/network equipment as they are prone to catching fire by accident.
- The organization is well protected from fire by fire prevention and detection systems installed at appropriate locations;
- Fire drills are held every six months and a report of the same is sent to the ISSC;
- All fire exits of the work area are clearly indicated;
- Explicit instructions are boldly and clearly written for the safe evacuation of personnel in the event of a disaster.
- Lightning protection system is installed to protect the office structure and information systems from damage due to lightning strikes.

16.2. Equipment Security

Policy: *"Equipments shall be protected to reduce the risks from environmental threats and unauthorized access. Power and telecommunication cables shall be appropriately protected from interception or damage. Equipment shall be correctly maintained to ensure its continued availability and integrity. Secure equipment disposal procedures shall be followed."*

16.2.1. Equipment:

16.2.1.1. Equipment siting and protection

- Equipment in the premises are appropriately positioned (sited) to minimize unnecessary extraneous access to work areas;
- All critical information assets are located in physically protected areas. Appropriate controls are used to protect against physical and environmental threats, e.g. fire, explosives, theft, smoke, chemical effects, power-supply interference, communications interference, electromagnetic radiation and vandalism;
- Storage facilities are secured to avoid unauthorized access;
- Wherever needed appropriate temperature and humidity control equipment are used to control and monitor the work areas housing IT equipment;
- Lightning protection is applied to all buildings and lightning protection filters are fitted to all incoming power and communication lines;
- Equipment that goes out of the premises must be accompanied with a Material Movement Gate Pass. Details are also entered in the outgoing equipment register.

16.2.2. Supporting Utilities

- All equipments are protected from power outages by dedicated generators/ UPS.
- The supporting utilities (e.g. electricity, telecommunications, and air-conditioning/ heating) are installed and maintained as per the equipment manufacturer's specifications and local legal requirements;
- The supporting utilities undergo preventive maintenance regularly to ensure their proper functioning.

16.2.3. Cabling Security

- Power and telecommunications cables carrying data or supporting information services are protected from interception, interference or physical damage;
- Power/electrical and data/signal cables are routed through separate paths to prevent interference;
- Only authorized personnel have access to patch panels and cable rooms;

- Clearly identifiable cable and equipment marking is used to minimize handling errors, such as accidental patching of wrong network cables.

16.2.4. Secure disposal or re-use of equipment

- Equipment having storage media is disposed only after ensuring that all sensitive data and licensed software have been removed or securely overwritten. This is done only after authorization of concerned TO/DTO;
- Storage media containing confidential, restricted or copyrighted information is physically destroyed or the information is destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function;
- Overwriting tools that are applicable to the technology of storage media are used for securely over-writing it.
- In case of disposal of old servers, which were earlier hosting the IFMS applications at various Treasury offices (i.e. before shifting to NIC Cloud), the useful historical data are to be backed up before over-writing/deleting the storage devices on them.
- The backup of useful historical data from the above-mentioned servers are to be taken manually, by the IT Support Members of the respective Treasury Offices on an one-time basis, on to an External Hard Disk, which is then stored in a designated locked cupboard (archive) in the HPDTA Head Office at Shimla.
- The records of the above backup activity are centrally monitored and maintained by the IT Support Team at the HPDTA Head Office at Shimla.

16.2.5. E-waste Disposal and Management

Disposal of Electronic Waste or E-waste shall be done as per E-Waste (Management) Rules, 2016 of the Government of India.

HPDTA is a bulk consumer of electrical and electronic equipment such as Personal Computers, Laptop Computers, Printers, Copying Machines, Telephone Equipment, LCD Displays, Fluorescent Lamps, etc. (as described in Schedule I of the above mentioned Rule).

HPDTA shall

- Ensure that e-waste generated by them is channelized through collection center or dealer of authorised producer or dismantler or recycler or through the designated take-back service provider of the producer to authorised dismantler or recycler;
- Maintain records of e-waste generated by them in Form-2 and make such records available for scrutiny by the concerned State Pollution Control Board;
- Ensure that such end-of-life electrical and electronic equipment are not admixed with e-waste containing radioactive material as covered under the provisions of the Atomic Energy Act, 1962 (33 of 1962) and rules made thereunder;
- File annual returns in Form-3, to the concerned State Pollution Control Board on or before the 30th day of June following the financial year to which that return relates.

Since HPDTA is a consumer with multiple offices in the state, one annual return combining information from all the offices shall be filed to the concerned State Pollution Control Board on or before the 30th day of June following the financial year to which that return relates.

17. IT Operations Security

Policy : *"Management and operations of all information processing facilities shall be controlled to reduce the risk of negligent or deliberate misuse. Services delivered by third parties shall be managed according to Organization's information security requirements."*

18. Tasks

18.1. Separation of development, test, and operational facilities

- Separate development, quality and production platforms shall be made available for SYSTEM/OS/APPLICATION landscape to maintain confidentiality, integrity and availability of operational data.
- Separate development and production platforms shall be made available for IT applications to maintain confidentiality, integrity and availability of operational data.

18.2. Installation of Software

- Only licensed versions of management-approved operating software are installed on the systems by the government approved supplier (HPSEDC).
- Random checks/audits shall be carried out to verify legality of the software by the Inventory Audit teams (ref sec 9.3).
- Unauthorized software found during the audits are uninstalled from the system by the audit team.

18.3. Upgrade/Downgrade software

Upgrade of software is taken care of only if advised by the IT Support person as designated by respective DTO/TO.

18.4. Desktop Installation and Maintenance by authorized vendors

- **System Installation**
  - Authorised team member from HPSEDC will plan installation activities based on the information received from Department Head.
  - System installation will cover the installation of desired OS & applications along with the system hardening.
  - Asset tagging is done along with the installation process; IT Support Member needs to ensure that the asset tags are unique as per HPDTA standards.
  - Once the entire installation process is done to the satisfaction of the IT Support member, the systems are moved to the respective workplace/user desk. The installation may also happen at the User location.

- In case of the allocated system to any user is not repairable, it will be replaced by a new one.
- In case the system warranty has expired and the allocated system is not in working condition, IT Support will organize replacement of the system depending on the business criticality of the system

18.5. Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

18.5.1. Management of technical vulnerabilities of IFMS Applications (HIMKOSH)

- NIC, Shimla, the developers of HIMKOSH applications, are responsible for the technical vulnerability management of these applications, including vulnerability monitoring, vulnerability risk assessment, patching and asset tracking.

18.6. Create/Delete User ID (Employee/Trainee)

- A unique employee code (IP Number) for each new employee is generated through the system by concerned DTO/TO. (Ref Sec 14.2 User Access Management)
- Once the respective employee leaves the organization, all his access rights are removed, user name is deleted and email password is changed immediately.

18.7. Service Level expected from NIC Cloud

- Application Server uptime at NIC Cloud is expected to be at least 99.9% . Downtime of this service is noted in a Critical Service Downtime Log, which is maintained by the IT Support Team at HQ and reviewed on a monthly basis by the CISO.

18.8. Anti-Virus

- HPDTA has a client-level anti-virus suite which takes regular updates from the internet automatically. For this purpose, the user systems are configured to Auto-Update the anti-virus databases at regular intervals.
- Malwares and viruses detected are configured to be moved to quarantine automatically.

19. Communications Security

Policy: "*Controls shall be established to safeguard the confidentiality and integrity of data passing over public and internal networks, and the users shall be provided access to the network services that have been specifically authorized*."

20. Tasks

20.1. Security of Network Services

- HPDTA ensures that the Network Service Providers implement security measures like firewall, content filtering, white-listing of safe websites, etc. to protect information in users' systems and applications.
- The service provider also ensures that internet connectivity at committed bandwidth is available at least 99.9% of the time at all offices of HPDTA.
- The above conditions are made part of the Service Level Agreement with the ISP and periodically monitored for compliance by a designated IT Support member at each office of DTO/TO/HQ.

20.2. E-mail Security

- Authorized users are assigned a unique email ID which relates to his/her official designation (and not personal name).
- Access to email is by webmail is given to authorized users only.
- Scanning and content filtering of all incoming mails and attachments is done at the mail gateway server to prevent spam/malware.
- Size of Mailboxes is aligned with the role of the employee in the organization.
- Size of outgoing mails, inclusive of attachment, is limited to 25 MB. Mails greater than this size are not accepted by e-mail server.
- In case of transfer of a user resulting in change of his designation, the user will relinquish the ownership of his earlier mail-box (with all official mails) and hand it over to the new incumbent to his earlier position.
  Under such circumstances if the user's earlier mail-box happens to contain mails other than official ones, e.g. mails from technology news sites, etc., he will be free to remove them, if he chooses to do so.
- Other users' responsibilities related to email security are mentioned in the IT Acceptable Use Policy (section 3.7).

20.3. Security in Social Networking

- Registration on social networking domains with official email is not allowed unless required in the normal course of duties.
- Creation or distribution of any disruptive or offensive messages, including offensive comments about any race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, national origin is not allowed.
- On social networking sites high security settings are used while being very limited in sharing personal information.

- Department/Government related information and confidential data are not to be shared on social networking websites.
- Unsolicited contacts from individuals in person, on telephone, or on internet who are seeking personal or corporate data are not entertained.

21. System Acquisition, Development and Maintenance

Policy: *"Security requirements shall be identified and agreed prior to the development, implementation and enhancement of information systems."*

22. Tasks

22.1. Security requirements of information systems

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

22.1.1. Information Security requirements analysis and specification

- Information security requirements are identified and included in the requirements for any new application in the application requirements form/note sheet.
- Security requirements for any change in the existing application are documented in the change request form as per Change Management Process.

22.1.2. Securing application services on public networks

- All information hosted on the Department websites is approved by the Management.
- SSL/TLS Protocol is used to secure all the application services running on the Internet.

22.1.3. Protecting application services transactions

- Vulnerability assessment and penetration testing of HPDTA's IFMS (HIMKOSH) Internet facing infrastructure is conducted annually through external auditor.
- Vulnerability assessment is conducted, through an external auditor, for all the applications of HPDTA, especially for those deployed over public networks, annually or whenever any major change is made.

22.2. Security in development and support processes

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

22.2.1. Secure development policy

- Security requirements are analyzed during the design phase for development and enhancement of applications,
- Security requirements are also analyzed during evaluation or acquisition of any outsourced software product,
- Application developers are guided to include security in the software development lifecycle by adopting:
    - Security in software development methodology;
    - Secure coding guidelines;
    - Security in version control;
- Application developers are to be trained to enhance their application security knowledge such that they are capable of developing secure applications.
- If application development is outsourced, the organization obtains assurance from interested party in regard to compliance of employing secure development standards.

22.2.2. System change control procedures

- Changes to application systems are carried out in a controlled manner as per the change management process.
    - Documentation pertaining to changes in system, approval including after change performance are maintained.
- All the applications requiring modifications due to any vulnerability found during the vulnerability assessment are corrected by using Change Management Process
- Changes are not to be carried out in production environment directly.

22.2.3. Technical review of applications after operating system changes

- All servers are installed with the required operating system and configured with hardening to ensure that only required services and software are available in the server.
- New releases/Patches pertaining to the operating system are tested in test/development server before applying in production environment to ensure that there is no adverse impact on operation, application controls or security.

22.2.4. Change Management Process for Application Software

Any changes or modifications to application software are carried out through the Change Management Process which consists of the following tasks:

22.2.4.1. Change Initiation

- Initiator raises the request for change (RFC) through the change request form (ref Annx.7)
- Change Request form consists of:
    - Initiator(requestor) name
    - Business need
    - Details of the change
    - Approver name

- Implementer name
- Result of Change

22.2.4.2. Change Impact Analysis & Classification

- Possible implications of making the change are analyzed by the NIC development team
- Risks associated with the change are evaluated
- Effect of proposed change on performance and quality are analyzed
- Business and technical consequences of making the change are analyzed
- How the proposed changed will be verified is documented

22.2.4.3. Change Evaluation & Approval

- Change is evaluated before approval, in terms of
  - Expected benefits of the proposed change
  - Availability of necessary resources
  - Any effect on already established IT security policies
- After evaluation, change is sent for approval by CISO in case it is having major impact on the production system
- Only approved change is sent for implementation to the authorized implementer in NIC.

22.2.4.4. Change Building, Testing & Implementation

- Only approved change is implemented; In case of any emergency change, formal documentation may be done after implementation
- Rejected change, if any, is sent back to the initiator for the necessary action
- During implementation following points are considered:
  - Both the software developed and the hardware purchased matches the predefined specifications
  - The envisaged schedules are met and the appropriate resources are assigned
  - The test environment is realistic and simulates the live environment closely
  - The back-out/rollout plans will allow the last stable configuration to be recovered rapidly
- Log of every change implementation is maintained.

22.2.4.5. Change Review & Closure

- Implementation of all major impact changes are reviewed for correctness by the CISO

22.2.5. System security testing

- Testing of security functionalities are carried out during development.
- The testing environment is segregated from the development and production environment.
- The security testing is carried out by developers before offering to process owner.

22.2.6. System acceptance testing

- Acceptance criteria for new information systems and upgrades are established for testing of the systems before acceptance.
- All information systems are configured according to security requirements of HPDTA.
- Adequate documentation is carried out in regard to system requirements and technical specifications, design documents, user manual, results of unit, integration and user acceptance testing before deployment.

22.3. Test Data

Objective: To ensure the protection of data used for testing.

22.3.1. Protection of test data

- An approval is sought from the CISO if live production data is used for testing.
- There is separate authorization, each time production system data is copied to a test application system.

23. Supplier Relationships

23.1. Information Security in Supplier Relationships

Policy : *"Information security requirements for mitigating the risks associated with supplier's access to the HPDTA's information assets need to be agreed upon with the supplier. Agreements with suppliers shall include requirements to address the information security risks associated with information and communication technology services."*

24. Tasks

24.1. Monitoring and review of supplier services

- Review of third party services shall be performed to determine the adequacy of the information security controls in use.
- Additionally the performance of third parties shall also be evaluated based on the quality of work rendered during periodic equipment maintenance and adherence to service levels.

24.2. Continual Assessment of Supplier Performance

The performance of the supplier is continually assessed to ensure that it is able to fulfill its contractual obligations. This is as per the periodicity agreed between the Supplier and HPDTA in Contract.

Individual reviews from all stakeholders are taken periodically and final consolidated ratings calculated are shared with the suppliers.

25. Information Security Incident Management

Policy : *"Appropriate controls shall be established to ensure a quick, effective, and orderly management of information security incidents and weaknesses."*

26.Tasks

26.1. Identifying a security incident/ weakness

Any incident, the occurrence of which violates an explicit or implied security policy is a security incident. A weakness in the system which may lead to a security incident is a security weakness. Please refer to **Annex 3** for possible Security Incidents or weaknesses.

26.2. Reporting information security events

- Employees report a security incident/ weakness by :
    - Sending mail to the Helpdesk / SIRT member
    - Sending an email at **addtre-hp@nic.in**
    - Telephone on SIRT member extension number/ mobile in case the incident requires immediate attention
    - Inform in person
    - Telephone on CISO extension number/ mobile
    - Inform in person to CISO

- Employees are to make sure that any security weakness or incident, even if it is of a minor nature, is not left unreported, as it may cause harm if left unattended over a period of time.
- If the incident is not valid, the same is informed to the reporter else the incident is categorized for severity and logged on for investigation by internal investigating team.
- Employees are advised not to try and prove that weakness as it may cause damage to the organization and result in legal liability for the employee trying to prove it.
- Investigation team collects evidences of the incident as reported and sends a report to the SIRT Head.
- SIRT Head reviews the report and closes the investigation.

26.3. Logging and Escalation of Security Incidents and weaknesses

- The SIRT takes appropriate action on the incident if it requires immediate action
- All reported security incidents and weaknesses are logged in the "Security Incident Register". Sample security incident logs are shown in Annexure 5.
- They are brought to the notice of the Chief Information Security Officer.
- SIRT assigns the incident to the relevant authority for follow-up.
- SIRT gets the SI Register filled up with the following information:
    - S.No
    - Incident No.
    - Incident Description

- Type of incident (security breach/ weakness / malfunction)
- Date and time of incident
- Severity Level
- Reported by
- Reported To
- Assigned to
- Correction Details
- Corrected By
- Root Cause
- Business Impact
- Corrective Steps
- Target Date
- Closure Date & Time
- Result
- Learning

- Security incidents are classified as high, medium or low severity depending on the impact that it has on the organization's business or service to customers.
- SIRT is responsible for closure of all security incidents. Where action is not completed by the date agreed, the situation shall be reviewed and revised actions recorded, taking into account security risks. This may require a short-term fix until a more permanent solution can be implemented.
- Once the issue has been dealt with and closed, the person who reported the incident is notified of the result.
- A final report on the incident is to be made, documenting the actions taken for resolution, and also bringing out learning's from the incident and proposed actions for improvement. A template for the report is placed as Annexure 4.

26.4. Handling Security Incidents and weakness

- Severity levels for Security incidents are classified as **Critical & Normal**.
- The timeline to close the incident is defined as follows:
  - **For Critical – response within 24 hrs, resolution within 72 hrs**
  - **For Normal - response within 48 hrs, resolution >72 hrs**
- If required, disciplinary action may be taken as per the policy of HPDTA.
- Employees who commit errors (laptop / mobile handling etc.) that lead to security incident are to be counselled by their reporting managers.
- Once the issue has been dealt with, the Security Incident report is closed and the incident log is updated.

26.5. Analysis of Security Incidents

- The incidents/weaknesses are collated and analyzed to detect trends. This analysis report indicates the following:
  - No. of incidents logged
  - No. of incidents closed
  - Actual time to resolve,
  - Corrective action taken
  - Root Cause Analysis

- Lessons learnt
- Any monetary/ reputation/ client losses incurred
- Preventive actions to be initiated

26.6. Collection of evidence

- In case an incident leads to legal action against the person or organization, Head of SIRT will ensure that the required evidence is collected as per the legal requirement and it is stored securely so that it cannot be tampered.
- While collecting evidence following things are needed to be considered:
  - **Rules for evidence** – to have adequate evidence to support an action against the user(s)
  - **Admissibility of evidence** – complying with any standard or code of practice for the production of admissible evidence
  - **Quality and completeness of evidence** – to achieve quality and completeness of the evidence, a strong evidence trail is needed

27. Compliance

Policy : *"Compliance with legislative, regulatory and contractual security requirements for the design, operation, use, and management of information systems shall be ensured."*

28.Tasks

28.1. Compliance with Legal and Contractual Requirements

28.1.1. List of Applicable Legislation and contractual requirements

The authorized personnel identify all legislation and Government guidelines applicable to HPDTA in order to meet the requirements for their type of business.
The specific controls and individual responsibilities to meet these requirements are defined and documented.
The applicable legislations include but are not limited to the following:

- IT Act 2000/2008 Amendment;
- National Cyber Security Policy;
- Information Security related Guidelines provided from time to time by Department of Electronics & IT (DeitY), Min. of Comm. & IT, Department of Internal Security, Min. of Home Affairs (MHA).

28.1.2. Intellectual Property Rights

Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licenses.

- The legal uses of software and information products are defined.
- Software is acquired through only known and reputable sources for ensuring compliance of Copyright Act.
- HPDTA maintains the proof and evidence of ownership of licenses.
- HPDTA ensures that software license agreements are complied with.
- Controls are implemented to ensure that software installed in various devices is within the purchased license quantity only.
- HPDTA ensures that only authorized software and licensed products are installed.
- Copying in full or in part, books, articles, reports or other documents is not permitted as per copyright law.

28.1.3. Protection of Records

- The protection of organization's record is based on classification of records. Organizational records needed to meet statutory, regulatory or contractual requirements, including support of essential business activities are retained securely. Appropriate destructions of records after the retention period are done.
- Handling procedures are implemented in accordance with manufacturer's recommendations when information is stored in media.

28.1.4. Privacy and Protection of Personally Identifiable Information

- Appropriate management controls exist to ensure privacy and protection of personally identifiable information.
- Awareness in regard to handling of personally identifiable information is ensured in the organization.
- Appropriate technical and organizational measures are implemented to protect personally identifiable information.
- The collection, processing and transmission of personally identifiable information are done as per the applicable legislation and regulations.

28.2. Information Security Reviews

28.2.1. Independent Review of Information Security

- Internal Information Security Audits are conducted on behalf of management twice a year or when significant changes take place.
- Internal IS Audits ensures the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security.
- The results of the Internal IS Audit are recorded and reported to the CISO.
- Corrections and Corrective actions are implemented in case of any non-conformances identified in the internal IS audits.

28.2.2. Compliance with Security Policies and Standards

Managers prepare the procedure for review of information security requirements as defined in policies, standards and other applicable regulations.
In case of non-compliance found in the review, below mentioned points are followed:-

- Identify the causes of the non-compliance;
- Evaluate the need for actions to achieve compliance;
- Implement appropriate corrective action;
- Review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses;

28.2.3. Technical Compliance Review

- Technical compliance reviews (e.g. Penetration Testing, Vulnerability Assessment, etc. of IT infrastructure) are planned, documented and repeatable and carried out by competent, authorized personnel;
- Penetration tests through external IP addresses are conducted by third-party service providers;
- Vulnerability Assessments of servers and systems are done by third-party service providers;
- The periodicity of Penetration testing and Vulnerability Assessment is at least once in a year;
- Appropriate corrective actions as recommended in the reports of PT and VA are taken.

Annexure 1 – Annual Audit Programme Template

ANNUAL AUDIT PROGRAMME (for Period: (Year))

Audit Number:					**Audit Number:**				
Month		**Scope**		**Remarks**	**Month**		**Scope**		**Remarks**
Planned	Actual	Planned	Actual		Planned	Actual	Planned	Actual	

CISO

Annexure 2- Audit Plan Template

S.No	Project/ Function	Areas to be covered	Auditee(s)	From	To	Auditor	Location
Date							

Annexure 3 - Examples of Security Events and Weaknesses

The following incidents are classified as security events:

- Unauthorized use of User ID/ Password compromise
- Theft of any Information Asset
- Unauthorized disclosure or amendment or corruption of information
- Loss of Departmental, clients', personal information
- External or internal hacking of network
- Unforeseen effects of change (e.g. change in system configuration)
- Fraud related to Information security
- Improper use of Internet/email
- Accidental or deliberate damage to information asset
- Unauthorized attempt to gain information
- Website defacement
- Physical intrusion
- Unauthorized logical access
- Theft or espionage of information or physical assets
- Denial of service
- Malicious software (virus, worms etc.)
- Unexplained system behavior
- Unauthorized access to secure areas
- Unauthorized movement of equipment and any other physical assets
- Detection of fire/smoke in the premises
- Malfunctions of hardware or software

The following are possible security weaknesses which may lead to security incidents:

- Applications used in the organization not tested for security
- Event logs are not write-protected
- Housekeeping staff not trained for security awareness

Annexure 4 - Information Security Event/Incident/Weakness Report Form

Form to report Events/Incidents or Weakness			
For official use only:		Tracking Number : ISMS-xxxxxxxxx	
☐Event	☐Incident	☐Weakness	
1. Reported By:			
Name:	Department:	Employee ID:	Designation:
2. Date and Time Incident/Event/Weakness reported:			
Date:	Time:		
3. When and How was the Event/Incident/Weakness detected?			
4. Physical Location of Affected Computer/ Network/Server/Appliance			
5. Is the affected system/network critical to the organisation's mission? (Yes / No). Details.			
6. Information of Affected System:			
IP Address:	Computer/ Host Name:	Operating System (incl. Ver./ release No.):	Last Patched/ Updated:	Hardware Vendor/ Model:

7. Description of Event/Incident/Weakness:				
8. Any Unusual behaviour/symptoms				
9. Has this problem been experienced earlier? If yes, details.				
10. ISSC notified(Yes/No)				
11. Any Other information available:				

Annexure 5 – Typical Security Incident Log contents

Security Log Content	Description
Serial Number	Running serial number
Security Incidence Number	SI + Running serial number
SI Date	Security Incidence reported date
Incident/ Weakness Description	Detail of the security incident
Classification	Whether it is an incident or a weakness
Severity Level	This can be 1, 2 or 3. Criteria of marking this are: **1 – Criticality Level is Low:** Minor system vulnerability / critical equipment failure not resulting in system downtime / log-on credential sharing. **2 - Criticality Level is Medium**: Unavailability / Failure of critical resources resulting in system downtime. Mal-functioning of critical equipment / Theft / Inappropriate data protection in application **3 - Criticality Level is High:** High impact on business / unauthorized forceful access (physical & logical).
Date Reported On	Date on which incident in reported
Reported By	Name of the person who reported the security incidence
Status	Status of the reported security incidence. These can be: Open: SI received but not allocated Allocated: SI received is allocated to the resolving person Close: The reported SI is closed, action complete.
Unit/ Department Name	Name of the Unit or Department of the person reporting the security incidence
Area / Equipment Affected	Current Identified Areas. For example: Access Control Air Conditioner

	DG E-mail Fire Alarm Infrastructure Internal Application Internet Access Logical Access Control Physical Security These can be changed from time to time
Location	Location where the reported security incidence occurred
Assigned To	The ISMS Administrator assigns the incident to the relevant authority for immediate action. SI is assigned based on the nature of SI. Some of the identified Assignees are: ADMIN IT SW DEV.
Allocation Date	Date of allocation of the reported security incidence
Expected Closure Date	Expected Closure Date of the reported security incidence
Resolved By	Name of the person who has finally resolved the reported security incidence. This person can be different than the "assigned to"
Actual Closure Date	Actual date of closure of the reported security incidence
Action Taken	Corrective Actions taken on the reported security incidence

Annexure 6A

IPAO-DDO-Login Request Letter

Date:

Letter Ref No.:

From: _____

_____

_____

_____ (DDO's office address)

To: _____

_____

_____

_____ (DTO/TO's office address)

Subject: Request for issue of new User ID / Password to the Office of DDO code _____.

Sir/Madam,

This is to request allocation of Login credentials for Mr./Ms. _____ ,

who has joined/working in our office as _____ w.e.f. _____ and his/her Login Request Form is attached herewith.

He/she may be provided with account privileges appropriate for DDO / Dealing Assistant (strike-out whichever is not appropriate).

Appreciate if his/her HIMKOSH account Password could be securely sent to my office at your earliest convenience.

Yours faithfully,

_____

_____

IPAO-DDO-Login Request Form

(To be filled by DDO)

Date of Request :

Treasury Code :

DDO Code :

IP No. of the DDO/Dealing Assistant (strike out whichever not appropriate):

Office Address :

Office Email :

Office Phone :

(To be filled by the Treasury)

Date of Allotment

User ID for DDO/Dealing Assistant (strike out whichever not appropriate):

User Name

Password

Instructions:

1. User ID is IP No. as provided by the Treasury.
2. You are requested to change the password on first Login and thereafter at regular intervals.
3. Your application web address will be http://himkosh.hp.nic.in/esalary

Annexure 6B

Covering Letter for sending Password to DDO

Date:

Letter Ref No.:

From: _____

_____

_____

_____ (DTO/TO's office address)

To: _____

_____

_____

_____ (DDO's office address)

Subject: Issue of new Password to the Office of DDO code _____.

Sir/Madam,

Kindly refer to your office letter number _____ dated _____ on subject cited above.

Please find enclosed herewith the PASSWORD for Mr./Ms. _____ .

He/she has been provided with account privileges appropriate for DDO / Dealing Assistant (strike-out whichever is not appropriate).

Enclosure: Filled-in Request Form for Login credentials for Mr./Mrs._____

_____.

Yours faithfully,

_____

_____

Annexure 7 – Change Request Form template

CHANGE REQUEST FORM			
Short Description of Change			
Change Request #:		**Change Request Date:**	
Proposed Change Date:		**Proposed Change Time:**	
Initiator's Name:		**Implementer's Name:**	
Implementation Date:		**Change Impact Category:**	**Major / Minor**
Approver's Name:		**Rollback Plan Duration:**	
Change Impact Analysis			
Detailed Description of Change (task lists with time estimates)			

Rollback Plan Description (task list with time estimates)			
Review (Post Change Implementation)			
Actual Start Time:		**Actual Finish Time:**	
Review's Name:		**Review Date:**	
Did the change go as planned? :			
If not, why not? Was the rollback plan used? Was the rollback plan successful?			
Initiator's Signature:	**Approver's Signature:**	**Implementer's Signature:**	**Reviewer's Signature:**