HPDTA
IT Acceptable Use Policy

Document Control

Document Name	IT Acceptable Use Policy
Document Reference Number	HPDTA/ISMS/ITAUP
Classification	Internal
Version Number	D1.1
Date	23-06-2017
Reviewed by	
Approved by	

Revision History

Date	Version	Description	Created by
15-06-2017	D1.0	Draft Release	ISMS Team
23-06-2017	D1.1	Revised Draft	ISMS Team

Distribution

- E-Mail
- HIMKOSH

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 on Intranet Portal is the controlled copy.

Related documents

S. No.	Document Reference Number	Document Name	Version

Acronyms and Abbreviations

Term	Description
HPDTA	Himachal Pradesh Directorate of Treasuries Accounts and Lotteries
HOD	Head of Department
DTO	District Treasury Officer

TABLE OF CONTENTS

1. Introduction

Purpose

The purpose of this policy is to establish the appropriate use of computing and telecommunication networks, computing equipment, and technology resources. These resources are provided primarily to enable/facilitate the official duties and responsibilities of the intended users. This policy sets out the responsibilities and limitations on the use of the organization's computer systems and the intention is to avoid any unauthorized use which may cause damage to the system, loss of data or criminal and/or civil liability for the user and/or the organization.

HPDTA's intention to publish the IT Acceptable Use Policy is not to impose restrictions that are contrary to the organization's established culture of openness, trust and integrity. HPDTA is committed to protect its employees, partners, clients and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly. Hence it is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Scope

This policy applies to employees, contractors, consultants, trainees, and other workers at HPDTA, including all personnel affiliated with third parties providing services to HPDTA.

2. Intended Audience

This policy is intended for use by all the users of its IT services (Computing and telecommunication networks, computing equipment, and technology resources) including employees, contractors, consultants, trainees, and other workers (Housekeeping, Security etc.) at HPDTA, including all personnel affiliated with third parties within the organization.

3. Description

3.1. General Use and Ownership

- HPDTA shall be sole proprietor of any information stored in HPDTA's Information Processing Facilities and its protection needs to be ensured by the users.
- Under no circumstances, users can engage in any activity that is illegal under law of the land by using information processing facilities of HPDTA.
- Theft, loss or unauthorized disclosure of HPDTA's proprietary information shall be promptly reported to the Security Incident Response Team (SIRT) at Treasuries HQ through a designated phone number and/or email id.
- HPDTA reserves the right to audit networks and systems, of the users of its services, on a periodic basis to ensure compliance with this policy.
- Important data, which needs protection, must reside on server (in NIC Cloud) itself and in order to ensure its coverage under backup procedure, user must seek clarification from NIC.
- All workstation, printers and other desks must be cleared of all redundant and non-usable documents before leaving for the day.
- Disposing of information should take place in a safe manner, to prevent information leakage.
- Use of IT facilities and services for purpose other than official work is prohibited.
- Providing information about or lists of HPDTA employees to parties outside HPDTA is not allowed.
- Do not send any official data/information to internal/external users for non-business related purpose.
- Do not create, circulate, forward, distribute, store and/or download any material or make any statements
    - Which may cause offence to any person to whom it is addressed
    - Which may be considered to infringe the organization's equal opportunities policy or be in any way be discriminating or harassing (whether sexually, racially or otherwise).
    - Of a pornographic, sexual or obscene nature, defamatory which may result in financial or legal liability or which may damage the reputation of the organization.

3.2. Desktop/PC/Workstation

- Desktops have been provided to employees of HPDTA to carry out their official work.
- Physical movement of desktops or any other hardware equipment shall be only done by the authorised personnel of department with assistance from IT-Support Team of the office/department.
- Individual workstations must be shut down and switched off before leaving the office everyday (unless required otherwise for official reasons).
- Users shall not save the data in the same drive where the OS is installed (generally the C drive) but in any other drive on the system (other than C).
- Hardware configuration of workstations after first time installation should not be changed and any requirements from users to upgrade hardware configuration must be routed to the Cyber Treasuries department, Shimla, subject to approval from concerned department head.

- Use of pirated software is absolutely prohibited on any computer system of HPDTA.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws is illegal and shall not be attempted by any user.
- No user shall try to access or copy data from systems to which they are not allowed access.
- User shall not install/uninstall any software on/from the HPDTA's computers without the prior approval from the IT-Support Team of the office/department.
- Users are precluded from installing, removing or editing scripts, which affects system configuration.
- Users shall not leave computers logged in and unattended for long durations. Ideally whenever you are leaving your PC unattended then either it must be logged off or it must be locked using (CTRL+ALT+DEL).
- Any unauthorized deliberate action that causes a system to malfunction or disrupts the normal performance of the system and /or the connected terminals is a security violation, irrespective of the system location or time duration.
- If media needs to be sent for repair, ensure that it does not carry any sensitive information, which It shall be erased before sending.

3.3. Secure Printer Usage

- Printers should be used for business purposes only and any bulk printing of manuals, e-books etc., if necessary, must be done in duplex mode to save paper.
- Confidential documents printed shall be collected from the printer immediately.
- Computer printout of confidential documents shall be kept in secured place.
- In case a printout is not correct/usable, it should be properly disposed-off by tearing or shredding.

3.4. User Access Management – Application

- Unique User-IDs shall be issued to each user of the IFMS Applications as per the policy by NIC. User shall be solely responsible for all actions conducted by using that User-id.
- Users shall not attempt to gain unauthorized access to restricted files or networks, or damage or modify computer equipment or software.
- All Users shall respect the privacy of other users, and shall refrain from attempting to view or read information being used by others.

3.5. Password Control and Usage

- Temporary/default passwords provided by the respective DTOs or NIC (as the case may be) shall be changed at the first log-on.
- To enhance security, password complexity shall be enabled on application, user workstation and servers. Before selecting a password following guidelines should be referred:
    - Password shall be of minimum 8 characters.
    - Password shall contain characters from three of the following four categories:
        - English uppercase characters (A through Z)
        - English lowercase characters (a through z)

        - Base 10 digits (0 through 9)
        - Non-alphabetic characters (for example,!, $, #, %)
    - Passwords used in 3 previous cases shall not be used again.
    - Passwords shall be easy to remember but at the same time shall not be based on something one could easily guess or obtain using user-related information, e.g. names, telephone numbers, date of birth, etc.
- User account shall be locked in case of 3 unsuccessful retries to log-on and shall need Administrator's intervention to revive.
- Maximum password age shall be 30 days. However, it is recommended to change user passwords frequently and whenever there is any indication of possible system or password compromise.
- As user is responsible for activities performed using his/her user-ids, sharing of passwords with others is NOT RECOMMENDED.
- Avoid keeping a paper record of passwords. User shall not divulge passwords to other users. Authorized users are responsible for the security of their passwords.
- Do not include passwords in any automated log-on process, e.g. stored in a macro or function key.

3.6. System and Network Activities

- The following activities are strictly prohibited:-
    - Unauthorized copying of proprietary/copyright material.
    - Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
    - Revealing your account password to others or allowing use of your account by others. This includes family and other household members when working from home.
    - Accessing data, a server or an account for any purpose other than official work or designated duty, even for users having authorized access.
    - Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of assigned work. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
    - Port scanning, security scanning or executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's assigned duty.
    - Circumventing user authentication or security of any host, network or account.
    - Interfering with or denying service to any user.

- User shall log-off from applications or network services, when no longer needed.
- To ensure security and avoid the spread of viruses, users accessing the Internet through a computer attached to organization's network must do so through an approved Internet

firewall or other security device. Bypassing Company's computer network security by accessing the Internet directly by modem, CDMA, GPRS or other means is strictly prohibited. If this is required for official reasons, then the permission must be sought explicitly from the concerned office/department head.

- Installation of any wireless (Wi-Fi LAN etc.) equipment in the company premises or its close proximity is not allowed without the prior permission of the IT-Support Team of the office/ department.

3.7. E-Mail

- Emails shall be configured for all HPDTA employees by the NIC.
- Depending on hierarchy, different mailbox spaces shall be provided to the users.
- In case of mailbox getting full, users shall contact NIC.
- When communicating on official email system, utmost care shall be taken as well as high professional standards must be followed because the users are representing HPDTA while sending or replying on official mail id.
- No personal email id shall be used to interact for official reasons with (including but not limited to) vendors, customers, service providers or partners. Only official email id must be used to do any official email correspondence except for emergency cases when the HPDTA's mail service is not available.
- Employee should not use official mail id for excessive personal use. It is employee's responsibility to discourage excessive personal mails on official email id.
- Employees shall use extreme caution when opening e-mails and specifically attachments received from unknown senders, which may contain viruses, worms or Trojan horse code.
- Forging of email headers is prohibited. Similarly sending emails from someone else's PC without the prior approval of that user shall not be allowed.
- Postings by employees from an HPDTA email address to newsgroups is discouraged. In case such a posting is done then it shall contain a disclaimer stating that the opinions expressed are strictly the user's own and not necessarily those of HPDTA, unless posting is in the course of business duties and with specific permission from HPDTA Management.
- Users who have emails configured in their Smartphone and/or laptop shall protect their devices by using authentication.
- Size of outgoing mails is limited to 25 MB. E-mail server shall be configured not to accept mails greater than this size.
- On receipt of any mail, suspected to be containing Malware (virus, worms, etc) it must be reported to the Security Incident Response Team (SIRT) at Treasuries HQ through a designated phone number and/or email id and further be deleted from the system.
- HPDTA policy strictly prohibits creating, circulating, distributing, storing and/or downloading (internally or externally) any:
    - Chain letters
    - Religious, political or business solicitations which do not relate to the user's duties as an employee of the organization;
    - Any files (including games, screen savers, .jpg or .wav or .mp3 or .scr or .bin or .zip files or other software and shareware) which are not business related.

3.8. Internet

- Different levels of Internet access is provided to employees depending on the job responsibility and other parameters. Using someone else's password to gain different level of internet access is prohibited and users must stick to the level of access allowed to them.
- Use of Internet connectivity service provided by ISPs (Internet Service Providers) other than the connectivity being provided by the office shall not be allowed in general. It may be allowed by the Head of the office/department only under exceptional circumstances where the office is unable to provide satisfactory quality of internet connectivity to the user/s. In such cases the IT-Support Team of the office/ department shall be kept involved and appropriate information security precautions shall be taken.
- Internet shall not be used for illegal activity, to access illegal materials, or to access materials that are obscene/pornographic/sexually explicit.
- Downloading software from the Internet without prior permission from the IT-Support Team of the office/ department, is prohibited.
- Downloading copyright protected material from the Internet is prohibited.
- Personal chatting on Internet is disallowed. In special cases, where chatting with external client is required, permission must be sought from the IT-Support Team of the office/ department together with approval from the concerned department head.
- No online storage accounts like Yahoo Briefcase, Dropbox, Google Drive, etc. shall be used to store official information.

3.9. Use of Removable Devices

- When a removable media is connected to desktop/laptop, it shall be scanned by anti-virus software before using it.
- User shall take utmost care for security of any official data kept in removable media like CD/DVD/USB hard disk /Pen Drive etc.
- Data shall be completely erased from the removable media, like USB/Hard Disk/Pen Drive, before discarding it. CD/DVD containing data shall be destroyed before its disposal.
- The use of removable devices like Infrared and Bluetooth devices, Data Access Cards etc., which plug into the USB (Universal System Bus) port of the desktop is prohibited in general. Only under exceptional circumstances, when connecting to an external ISP is permitted by the Head of the office/ department (ref second para of section 3.8), use of Data Access Cards may be allowed.

3.10. Privacy Control

HPDTA has full respect for individual's privacy and rights. However, users should not have any expectation of privacy in respect of their usage of organization's IT resources. The organization's IT resources are the backbone for running the organization's business and it is vital that nothing is done to compromise this in any way even if this is unintentional. Please note that HPDTA/NIC may monitor or keep a record of communications (at any time with or without notice) either directly or via an external agency and/or record an individual's use of the IT Resources in order to (including, but not limited to):

- To detect/investigate any unwanted elements like virus etc which might be destructive in nature
- Detect and/or prevent crime
- Ascertain and/or demonstrate whether the user and/or the organization are complying with the organization's rules and policies (including, but not limited to, this policy) and also with legal and/or regulatory obligations which the user and/or the organization are subject to
- Ascertain whether communications are relevant to the organization's business
- Ascertain and/or demonstrate whether HPDTA is providing appropriate standards of customer service
- HPDTA shall, in conducting such monitoring activities, use all reasonable endeavours to comply with regulatory guidelines and to respect individual's privacy and that of third parties using the IT Resources.

Annexure A

Declaration towards compliance to HPDTA's Acceptable IT Use Policy					
I have read the Acceptable IT Use Policy of HPDTA (Para 3.1 to Para 3.10) and agreed to comply with it fully including any updates or revisions published in future. I understand that my access to HPDTA's data and information processing facilities is for the sole purpose of carrying out my official responsibilities. I understand that misuse of HPDTA's data and information processing facilities and any violation of the HPDTA's Acceptable IT Use Policy (Para 3.1 to Para 3.10) are liable for appropriate action by HPDTA management.					
Name of the user:		**Email Address:**			
Designation:		**Contact Number:**		**Date:**	__/__/____
Department:		**Signature:**			