SECURITY POLICY FOR USER

1. **Purpose:** The policy aims at providing secure and acceptable use of client systems.

2. **Scope:** This policy is applicable to the employees in the Ministry / Department / Subordinate office of Government of India for handling of unclassified information.

3. **Exception Management:** For any exception / deviation, the user shall take approval from the Chief Information Security Officer (CISO).

4. **Policy**

4.1 Acceptable Use of Client Systems

4.1.1 User shall be responsible for the activities carried out on the client system, using the accounts assigned to him / her.

4.1.2 User's network access shall be subjected to monitoring / filtering for malicious / unauthorized activities.

4.1.3 For any administrative activities on the client system, user shall adhere to Security Policy for System Administrator.

4.1.4 User shall use account with limited privileges on client system and shall not use administrator privileges. (refer: Limited User Account Creation Procedure)

4.1.5 Backup of important files shall be taken by the user at regular intervals. (refer: Data Backup and Restoration Procedure)

4.1.6 System / media containing official information shall be physically secured. (refer: Security Guidelines for User)

4.1.7 User shall not leave system unattended. The user shall lock out his / her system before leaving the system. Additionally, system idle timeout shall be configured on the client system. (refer: System Idle Timeout Configuration Procedure)

4.1.8 Maintenance or rectification of faults in the client system shall be carried out under close supervision of the user.

4.1.9 User shall check that the system time is as per IST. Any variation shall be reported to the System Administrator / Network Security Administrator.

4.1.10 User shall not engage in any of the following activities:

4.1.10.1 Circumventing security measures

4.1.10.2 Unauthorized access to Systems / Data / Programs

4.1.10.3 Harassing other users by accessing or modifying their data / resources on the system

4.1.10.4 Creating, accessing, executing, downloading, distributing, storing or displaying any form of anti-national, offensive, defamatory, discriminatory, malicious or pornographic material

4.1.10.5 Making copies of software / data for unauthorized use

4.1.10.6 Impersonation

4.1.10.7 Phishing

4.1.10.8 Social engineering

4.1.10.9 Unauthorized use of software license

4.1.10.10 Providing official e-mail address on Internet mail groups / bulletin boards for personal use

4.1.10.11 Any activity that is in violation of Central Civil Services (Conduct) rules

4.1.11 User shall report security incident to the System Administrator / Network Security Administrator. (refer: Security Incident Management Process)

4.1.12 User shall ensure that unauthorized Peer to Peer file sharing software is not installed.

4.1.13 User shall ensure that the system is configured as follows:

4.1.13.1 User shall not share client system with anyone, by default. However, if necessary for any specific reason (such as client system used in shift-duty), following shall be ensured:

4.1.13.1.1 Explicit approval of competent / designated authority is taken for each client system and every user accessing it.

4.1.13.1.2 Every user on the shared client system has a separate account.

4.1.13.1.3 File / Folder access permission is limited to meet functional requirement of the user.

4.1.13.2 User shall not share hard disk or folders with anyone, by default. However, if necessary, only the required folders shall be shared with specific user. (refer: Hard Disk / Folder Sharing Procedure)

4.1.13.3 Client System has Client System Security (CSS) implemented as per Client System Security Guidelines.

4.1.13.4 By default all interfaces on the client system are disabled and only those interfaces which are required are enabled. For configuration user shall contact the System Administrator.

4.2 Virus and Malicious Code (adware, spyware, malware)

4.2.1 User shall ensure that client system is configured with the authorized anti-virus software. *(refer: Anti-Virus Management Procedure)*

4.2.2 User shall ensure that anti-virus software and the virus pattern files are up-to-date. (refer: Anti-Virus Management Procedure)

4.2.3 User shall ensure that anti-virus scan is configured to run at regular intervals. (refer: Anti-Virus Management Procedure)

4.2.4 In case a virus does not get cleaned, incident shall be reported to the System Administrator / Network Security Administrator. (refer: Security Incident Management Process)

4.3 Hardware, Operating System and Application Software

4.3.1 User shall use only the software / hardware which are authorized by the Department.

4.3.2 The following activities shall be carried out by the System Administrator. However, the User shall ensure the following:

4.3.2.1 Operating System and other software is installed using authorized source / Original Equipment Manufacturer (OEM) media with valid license.

4.3.2.2 While installing the Operating System and other software packages, only the required utilities are installed / enabled. (refer: Operating System Hardening Guidelines).

4.3.2.3 Latest available service packs, patches and drivers are installed. (refer: Patch Installation Procedure and Patch Verification Procedure)

4.3.2.4 Booting from removable media is disabled. (refer: Removable Media Boot-up Disable Procedure)

4.3.2.5 Auto-run on all removable drives is disabled. (refer: Auto-Run Disable Procedure)

4.3.3 User shall allow the installation of service packs and patches provided by the patch server. (refer: Patch Installation Procedure and Patch Verification Procedure)

4.4 E-mail Use

4.4.1 Only the E-mail account provided by the Department shall be used for official communication.

4.4.2 Official E-mail shall not be forwarded to personal E-mail account.

4.4.3 E-mail password shall not be shared even for official purpose.

4.4.4 User shall not attempt any unauthorized use of E-mail services, such as:

4.4.4.1 Distribution of messages anonymously

4.4.4.2 Misusing other user's E-mail address

4.4.4.3 Using a false identity

4.4.4.4 Sending messages to harass or intimidate others

4.4.5 Password used for online forms / services / registrations / subscriptions shall not be the same as the password of official E-mail account.

4.5 Password Security

4.5.1 Selection of password shall be done as per the Password Management Guidelines.

4.5.2 The following activities shall be carried out by the System Administrator. However, the User shall ensure the following:

4.5.2.1 Passwords are enabled on BIOS, System login and Screensaver levels. *(refer: Password Enabling Procedure)*

4.5.2.2 Auto-logon feature on the client system is disabled. (refer: Auto-Logon Disable Procedure)

4.5.2.3 User account is locked after a predefined number of failed login attempts.

4.5.3 User shall not share or reveal passwords.

4.5.4 Passwords shall be changed at regular intervals as per the Password Management Guidelines.

4.5.5 If a password is suspected to have been disclosed / compromised, it shall be changed immediately and a security incident shall be reported to the System Administrator / Network Security Administrator (refer: Security Incident Management Process).

4.6 Portable Storage Media

4.6.1 User shall use officially issued portable storage media only.

4.6.2 User shall return the portable storage media, if it is no longer a functional requirement or in case of damage / malfunctioning.

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

4.6.4 User shall ensure that the execution of software from portable storage media is not done.

4.7 Network Access Policy applicable for the user

4.7.1 User shall take prior approval from the competent authority to connect the client system to the network.

4.7.2 A client system authorized to connect to one network shall not connect to any other network.

4.7.3 For wireless connectivity, user shall ensure the following:

4.7.3.1 By default, the wireless interfaces are disabled.

4.7.3.2 Client system does not connect to wireless networks / devices without approval from the competent authority.

4.7.3.3 If permitted, the wireless interface of the client system is enabled to connect to authorize wireless network only.

4.8 Client System Log

4.8.1 User having administrative privilege shall not disable / delete the audit trails / logs on the client system.

5.Review: This Security Policy shall be reviewed at the time of any change in the IT environment or once every year, whichever is earlier. The review shall be carried out for assessing the following:

5.1 Impact on the risk profile due to, but not limited to, the changes in the deployed technology / network security architecture, regulatory and / or legal requirements**.**

5.2 The effectiveness of the security controls specified in the policy. As a result of the review, the existing policy may be updated or modified.

6.Enforcement: Violation of this policy shall amount to misconduct under CCS Conduct rules.