अखिल भारतीय आयुर्वेद संस्थान

(आयुष मंत्रालय, भारत सरकार के अंतर्गत स्वायत्त संस्थान)

ALL INDIA INSTITUTE OF AYURVEDA (AIIA)
(An Autonomous Organization under the
Ministry of AYUSH, Govt. of India)

IT POLICY FOR USER

गौतमपुरी, सरिता विहार, मथुरा रोड, नई दिल्ली -110076
Gautampuri, Sarita Vihar, Mathura road, NEW DELHI-110076
E-mail: aiianewdelhi@gmail.com Phone: 011-29948658
Fax: 011-29948660

IT POLICY FOR USER

All India Institute of Ayurveda (AIIA) New Delhi provides IT resources to enhance efficiency and productivity. These resources are meant as tools to access and process information related to their areas of work. These resources help to remain well informed and carry out their functions in an efficient and effective manner.

1. **Purpose**: The policy aims at providing secure and acceptable use of IT Resources / client systems. The term 'IT Resources' includes desktop devices, portable and mobile devices, networks including wireless networks, Internet connectivity, external storage devices and peripherals like printers and scanners and the software associated therewith.
2. **Scope**: This policy is applicable to ALL the users of All India Institute of Ayurveda (AIIA) for handling/accessing information. The objective of this policy is to ensure proper access to and usage of AIIA's IT resources and prevent their misuse by the users. Use of resources provided by AIIA implies that the user's agreement to be governed by this policy
3. **Exception Management**: For any exception / deviation, the user shall take approval from the competent authority of AIIA.
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 take approval from the competent authority of AIIA and shall contact the In-charge IT.

4.1.4 User shall use account with limited privileges on client system and shall not use administrator privileges.

4.1.5 Backup of important files shall be taken by the user at regular intervals.

4.1.6 System / media containing official information shall be physically secured.

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.

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 In-charge IT.

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/Govt. of India rules.

4.1.11 User shall report security incident to the In-charge IT.

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.

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 In-charge IT.

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.

4.2.2 User shall ensure that anti-virus software and the virus pattern files are up-to-date.

4.2.3 User shall ensure that anti-virus scan is configured to run at regular intervals.

4.2.4 In case a virus does not get cleaned, incident shall be reported to the In-charge IT.

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.

4.3.2.3 Latest available service packs, patches and drivers are installed.

4.3.2.4 Booting from removable media is disabled.

4.3.2.5 Auto-run on all removable drives is disabled.

4.3.3 User shall allow the installation of service packs and patches provided by the patch server.

4.4 E-mail Use

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

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

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

4.4.3.1 Distribution of messages anonymously

4.4.3.2 Misusing other user's E-mail address

4.4.3.3 Using a false identity

4.4.3.4 Sending messages to harass or intimidate others

4.4.4 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. However, the User shall ensure the following:

4.5.2.1 Passwords are enabled on BIOS and System login.

4.5.2.2 Auto-logon feature on the client system is disabled.

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 In-charge IT

4.6 Portable Storage Media

4.6.1 By default USB ports are blocked.

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

4.6.3 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.

4.7.3.4 To ensure information security, users should not connect their devices to unsecured wireless networks.

4.7.4 Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security

4.8 Client System Log

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

4.9 Filtering and blocking of sites:

4.9.1 Institute may block content over the Internet which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or which may pose a security threat to the network.

4.9.2 Institute may also block content which, in the opinion of the organization concerned, is inappropriate or may adversely affect the productivity of the users.

4.10 Access to Social Media Sites from Government Network

4.10.1 Use of social networking sites by Government organizations is governed by “Framework and Guidelines for use of Social Media for Government Organizations” available at http://meity.gov.in.

4.10.2 User shall comply with all the applicable provisions under the IT Act, 2000 etc., while posting any data pertaining to the Government on social networking sites.

4.10.3 User shall adhere to the “Terms of Use” of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.

4.10.4 User shall report any suspicious incident as soon as possible to the competent authority.

4.10.5 User shall always use high security settings on social networking sites.

4.10.6 User shall not post any material that is offensive, threatening, and obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.

4.10.7 User shall not disclose or use any confidential information obtained in their capacity as an employee/contractor of the organization.

4.10.8 User shall not make any comment or post any material that might otherwise cause damage to the organization’s reputation.

4.11Deactivation

4.11.1 In case of any threat to security of the Government systems or network from the resources being used by a user, the resources being used may be deactivated immediately by the In-charge IT.

4.11.2. Subsequent to such deactivation, the concerned user and the competent authority of that organization shall be informed.

4.12 Use of IT Devices

IT devices issued by the Institute to a user shall be primarily used for Institute related purposes and in a lawful and ethical way and shall be governed by the practices defined in the document “Guidelines for Use of IT Devices on Government Network” available at http://www.meity.gov.in.The aforesaid document covers best practices related to use of desktop devices, portable devices, external storage media and peripherals devices such as printers and scanners.

5. **Review**: This Security Policy shall be reviewed at the time of any change in the IT environment or as deemed necessary 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 / Govt. of India rules and regulations.