सत्यमेव जयते

आयुष मंत्रालय
MINISTRY OF
AYUSH

IT SECURITY POLICY

Ministry of AYUSH, GOI

20th July, 2020

(Version 3.0)

ABBREVIATIONS

BCP	Business Continuity Planning
DR	Disaster Recovery
MOA	Ministry of Ayush, Government of India
NIC	National Informatics Centre
MeitY	Ministry of Electronics and Information Technology
CSIT	Cyber Security Implementation Team, MOA
GOI	Government of India
Information	Throughout this document information shall mean Digital Information

Table of Contents

1 INTRODUCTION

The purpose of this document is to define the IT security policy of the Ministry of Ayush, Government of India. It also caters to the organization and framework required to communicate, implement and support the policy. Information is an asset which has significant value to the ministry and requires to be protected from unauthorized access. The IT security policy is an evolving framework and provides an overview of what it takes to effectively protect information, information systems & networks for creating secure computing environment.

Information security is a critical component that is required to enable and ensure the availability, integrity, and confidentiality of data, network, and processing resources. This policy document has been developed to establish and uphold the minimum requirements that are necessary to protect information and information assets against unavailability, unauthorized or unintentional access, modification, destruction or improper disclosure. This document applies to all full, part-time employees and consultants, contractors or vendors who work on the ministry’s premises and it is their responsibility to adhere to this policy and the management has all rights to take action in case of its violation in accordance with defined process. The Management commits itself to supporting implementation and maintaining compliance to this policy.

This policy also serves as an umbrella framework for defining and guiding the actions related to IT security of the various organizations of the ministry. It therefore enables the individual organizations under this ministry in designing appropriate IT security policies to suit their needs.

1.1 Vision

Make timely informed decisions with practical security mechanisms for the protection of information of the Ministry of Ayush by building a secure and resilient ICT ecosystem.

1.2 Mission

To protect information and ICT infrastructure, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

1.3 Objectives

a) To create a secure IT ecosystem in the ministry, generate adequate trust & confidence in IT systems and thereby enhance adoption of IT in all organizations of the ministry.

b) To enhance and create mechanisms for obtaining information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.

c) To ensure effective information security within the ministry with clearly laid down roles and responsibilities.

2 INDIVIDUAL USE

2.1 Purpose

This section provides users with relevant guidance concerning use of various information and information assets in the ministry.

2.2 General Requirements

a) Users are responsible for exercising good judgment regarding appropriate use of ministry's resources in accordance with Government policies, standards, and guidelines. Government resources may not be used for any unlawful or prohibited purpose.

b) For security, compliance, and maintenance purposes, authorized personnel shall monitor and audit equipment, systems, and network traffic.

c) Devices that interfere with other devices or users on the Government network may be disconnected.

d) The ownership assigned to the user of the information assets and information processing facilities will be approved and reviewed regularly, in specifics the owner will follow the government policy and procedure.

e) Users must not purposely engage in activity that may degrade the performance of Information Resources, circumvent Government computer security measures.

f) Government Information Resources must not be used for personal benefit.

g) Administrator login credentials shall not be used / shared to general users only authorized by competent authority.

2.3 Password Use

a) Users will not keep copy of password in any written form or electronic form. If required, passwords of critical user accounts shall be maintained securely.

b) Users will change passwords whenever there is any indication of possible system orpassword compromise.

c) Users will change passwords at regular intervals as per defined policy.

d) Users will avoid reusing or cycling old passwords.

e) Users will change temporary passwords at first logon.

f) Users must not include password in any automated logon process, e.g.: stored in amacro or function key.

g) Users will not share their passwords with anyone.

h) Users shall use their credentials to logon to an information asset even in cases where an information asset is being shared by more than one user.

i) Users will ensure that nobody is watching when the password is being entered.

2.4 Password construction

a) Users will choose passwords that are easy to remember but difficult to guess. Some of the guidelines for password constructions are:

- Quality password with sufficient minimum length 8 characters long
- Easy to remember

- Not based on anything, somebody else could easily guess or obtain using persons related information (e.g.: Names, Telephone No's, Date of Birth, Company Name, Spouse Name, etc.)
- Not vulnerable to dictionary attack (i.e. do not consists of words included in dictionaries)
- Free of consecutive identical, all---numeric or all alphabetic characters

b) Do not use word or number patterns like aaabbb, qwerty, 123321, etc.

c) Not use the same password for ministry and non-ministry purposes.

d) Strong passwords would have a minimum length of 8 characters and can be constructed through a mix of numerals (1,2,3 etc.), special characters (!,@,#,$ etc) and capital letters (A,B,C etc).

e) One way to create complex but easy to remember passwords is to take a known word or phrase and convert it using numerals, special characters and capital letters.

2.5 Unattended User Equipment, Clear Desk and Clear Screen

a) All users are responsible for implementing security procedures for protecting unattended systems.

b) Sensitive or critical business information, e.g.: on electronic storage media, will be locked away (ideally in a safe or specialized cabinet or other forms of security furniture) when not required, especially outside the normal working hours.

c) Computers and terminals will be left logged off or protected with a screen and keyboard locking mechanism controlled by a password when unattended.

d) Unauthorized use of photocopiers and other reproduction technology like scanners, digital cameras, will be prevented.

e) Documents containing sensitive or classified information will be removed from printers immediately.

f) System administrators shall ensure that the active directory system is configured to automatically lock systems, which are inactive for more than 5 minutes.

2.6 Information exchange Policies and Guidelines

a) Appropriate controls will be implemented for protection against malicious code, when transmitting information electronically.

b) Sensitive information will be protected using encryption, password or any other suitable method especially when being sent as an attachment in an email.

c) Disposal procedures will be followed to destroy sensitive information.

d) Users will :

- Not leave sensitive information unattended at Scanners, printers etc.
- Not auto forward mails to external mail ids.
- Not reveal sensitive information in public.
- Not leave sensitive messages on answering machines.
- Check the recipients email ID before sending an email respectively.

2.7 Reporting Information Security Incidents and Weaknesses

a) All users will be aware or made aware of their responsibility to report any information security incidents and/or weaknesses in systems or services.

b) All users shall report Information security related events and weaknesses through the quickest mode to the ICT unit through a defined reporting procedure.

2.8 Prevention of misuse of information processing facilities

a) All users will use the information processing facilities for business purposes only.

b) Any use of these facilities for non-business purposes without management approval or for any unauthorized purposes, will be regarded as improper use of facilities or breach of confidentiality. The unauthorized activity may be identified by monitoring or other means.

c) Intrusion detection, intrusion prevention, content inspection, and other monitoring tools shall be used to detect and prevent misuse of information processing facilities.

2.9 Anti-Virus

a) All workstations and laptops will have anti-virus installed, running and updated. A corporate anti--virus will be implemented in the ministry. NIC’s anti-virus policy shall be followed in the ministry.

b) Users will not change the anti-virus settings.

c) Users will not disable the installed anti-virus agent or change its defined settings during installation. This includes settings for daily virus scan; anti---virus server address and signature update schedules.

d) Users will not disrupt the auto virus scan scheduled on their desktop. If the scan is affecting system performance, users will contact NIC helpdesk for resolution.

e) All external media will be used only after authorization and subjection to anti-virus scan and users are advised to run anti-virus scan when any external media is used.

f) Users will report any virus detected in the system to System NIC helpdesk.

g) Users must exercise extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse codes.

h) Users will exercise caution when copying files. They shall only download from reputable sites and carry out a virus check on the file.

i) User shall not disrupt the periodic updates of all necessary security patches and hot fixes for the operating system and applications installed on their desktop/laptop.

2.10 Internet Usage

a) Users shall not use or access the Internet for non-business purposes and restrict personal use to minimum - limited to educational, knowledge and news sites. Users will strictly avoid visiting non-business, offensive and unethical sites which violate security policies.

b) Users will not use Internet facilities to:

- Download or distribute malicious software or tools or to deliberately propagate any virus.
- Violate any copyright or license agreement by downloading or distributing protected material.

- Upload files, software or data belonging to the ministry to any internet site without authorization of the owner of the file, software or data.
- Share any confidential or sensitive information of the ministry with any internet site unless authorized by a Superior.
- Post any ministry's proprietary information on Internet share drives/briefcase, public forums, newsrooms or bulletin boards. This is strictly prohibited and any violation will be subject to disciplinary process.
- Post remarks that are offensive, aggressive, insulting, obscene or not in line with ministry's policy on the subject.
- Conduct illegal or unethical activities including gambling, accessing obscene material or misrepresenting the ministry.

c) In case such misuse of the Internet access is detected, authorized personnel shall take disciplinary action.

d) Users will ensure that they do not access websites by clicking on links provided in emails or in other websites. When accessing a website where sensitive information is being accessed or financial transactions are done, it is advisable to access the website by typing the URL address manually rather than clicking on a link.

e) Users shall be aware that their information systems (computer, internet, email, messenger and telephone conversations), their usage and information exchanged are not private and the ministry reserves the right to monitor and audit these on ongoing basis and during or after any security incident.

f) Users must be aware that the ministry accepts no liability for their exposure to offensive material that they may access via the Internet.

g) Users will ensure that security is enabled on the Internet browser as per guidelines given below:

- Configure browser not to remember web application passwords.
- Set browser security setting to medium.

h) The ministry reserves the right to monitor and review Internet usage of users to ensure compliance to this policy. Any such monitoring will be authorized by competent authority.

2.11 User Privacy

a) Users will have no expectation of privacy while using ministry owned or leased equipment. Information passing through or stored on ministry equipment can and will be monitored as and when required for security and compliance reasons.

2.12 Email Usage

a) Email is a business communication tool and users must use this tool in a responsible, effective and lawful manner.

b) Users shall comply with ministry's email policy on proper and effective use of email. NIC's email policy shall be followed in the ministry.

c) Users will protect their email account through strong password and will not share their password or account with anyone else.

d) Users shall conduct the necessary housekeeping of his/her email at regular intervals.

e) Users will promptly report all suspected security vulnerabilities or problems that they notice with the email system to NIC helpdesk.
f) The ministry has the authority to intercept, disclose or assist in intercepting or disclosing email communications.
g) Users will not use any email account other than the one provided by the ministry for transmitting official information.
h) Confidential information will be secured before being sent through email by way of compression, password protection or other advanced cryptographic means.
i) Language used will be consistent with other forms of business communications.
j) Users will treat electronic email messages with sensitive or confidential information as 'Confidential'.
k) Users shall avoid opening mail from unknown users/sources and also avoid opening suspicious attachments or clicking on suspicious links.
l) The ministry shall restrict attachments size on the email system.
m) The ministry reserves the right to monitor email messages and may intercept, disclose or assist in intercepting or disclosing email communications to ensure that email usage is as per this policy.
n) Users shall avoid sending or forwarding unsolicited email messages; "chain letters","Jocks", "junk mail", etc. from other internal users and external networks or other advertising material to individuals who did not specifically request such material (email spam).
o) Users will avoid using "reply to all" for messages that are sent to large distribution groups, especially when the reply only concerns only a few recipients.
p) Users shall avoid any form of harassment via email whether through language, frequency or size of messages.
q) Users shall avoid unauthorized use, or forging, of email header information.

2.13 Laptop Security

a) Laptop users will take additional responsibility for the security of their laptop and the information it contains. Users will adopt the following measures and consult NIC helpdesk for any clarification:
   - Ensure that laptop is configured as per the secure configuration. Do not install unlicensed or doubtful software or applications.
   - All sensitive data on laptop will be secured either through password protection or by using encryption.
   - Whenever connecting to the LAN, ensure that the anti-virus agent is installed with latest signatures on the laptop.
   - Log off laptops when not working for extended periods and enable a screen saver with password for protection during short periods of inactivity.
   - Take adequate measures for physical protection of laptop including, but not limited to, not leaving laptops unattended in public places or while travelling.
   - Personal Digital Assistant (PDAs) devices, laptops, wireless phones and miniature hard drives will not be connected to the LAN without prior permission from the reporting manager and NIC helpdesk. Users having personal internet connectivity facility are recommended to have

a personal firewall installed to prevent unauthorized access to their laptop while connected to Internet.

- Loss of laptop will be reported immediately to NIC helpdesk, superior. If the laptop contains sensitive information, necessary steps need to be taken by the NIC helpdesk to control damage.

b) In case any laptop is connected to the ministry network without authorization, the ministry shall take appropriate action against the user.

2.14 User level best practices.

a) Always use genuine software avoid pirated s/w.
b) Always access Internet as a standard user but not as ADMIN.
c) Disable file and printer sharing.
d) Be wary of storing personal information on various social media platforms.
e) Do not share financial details, e-wallets details or banking details with anyone.
f) Do not share UN, passwords etc. with any one anonymously.
g) Do not provide information about yourself that may allow user to answer any secret security question
h) Check and verify email sender ID and weblinks before opening.
i) Be cautious of any tiny URLs.
j) Do not open attachments with extensions: VBS, U64, SHS, PIF, SCR.
k) Protect against social engineering attacks. Phishing emails and SMS are used to get user credentials like UN, PWS CC PIN etc.

3 ORGANIZATION SUPPORT

3.1 Purpose

This section ensures an effective information security management framework within the ministry with clearly laid down roles and responsibilities. In a large Government organization, a cross-functional forum of management representatives from relevant parts of the organization is necessary to coordinate the implementation of information security controls.

3.2 Management commitment to information security

a) The ministry shall designate a member of senior management, as Chief Information Security Officer (CISO), responsible for IT security efforts and initiatives. Refer section “Governance Framework” for details about the required committees to implement this policy.
b) CISO shall head a Cyber Security Implementation Team to assist the ministry in implementing this policy. CISO shall be responsible and oversee the implementation ofthis policy.
c) Earmark a specific budget for implementing IT security initiatives and for meeting emergency response arising out of cyber incidents.
d) Provide fiscal schemes to install, strengthen and upgrade information infrastructure with respect to cyber security.
e) CISO shall review the information security policy at least once a year or on a need basis.
f) Prepare the ministry’s Cyber Crisis Management Plan in line with the National Cyber Crisis Management Plan.

g) Implement the defined Cyber Crisis Management Plan for dealing with cyber related incidents.
h) CISO conducts cyber security meetings at least twice a year to review the effectiveness of the implementation of this security policy.
i) CISO shall ensure adequate resources are allocated for information security initiatives.
j) CISO shall coordinate the implementation and maintenance of information security controls.

3.3 Information security coordination

a) The Cyber Security Implementation Team (CSIT) shall take overall responsibility for Information security and drive Information Security initiatives in the ministry.
b) CSIT shall be suitably staffed with wide representation of departments across the ministry.
c) CSIT shall be responsible for assigning roles, responsibilities, drafting all the Security Policies in the ministry for due approval of competent authority.
d) CSIT shall meet once every quarter to review the policies and minutes of these meetings shall be maintained as records.
e) CSIT shall ensure that security activities are executed in compliance with this policy.
f) CSIT shall assess and review risk management at least twice a year or whenever there is a change.
g) CSIT shall ensure periodic information security education, training and awareness of users.
h) CSIT in quarterly meetings shall review, evaluate information security incidents and recommend appropriate corrective or preventive actions.
i) CSIT shall ensure internal audits are conducted at least once a year to ensure that the information security policies, procedures are implemented and to assess the effectiveness of the policies.
j) CSIT shall also ensure CERT-In audits as defined in the ministry's Cyber Crisis Management Plan.
k) CSIT shall ensure all ICT assets are listed with an identified owner. CSIT shall ensure the responsibility of asset owners are defined, documented and communicated to the asset owners.
l) The asset owners along with CSIT shall be responsible for identifying and assessing the risks to the assets on need basis or at least once a year.
m) CSIT shall ensure all users are briefed on their information security roles and responsibilities prior to being granted access to sensitive information or information assets.

3.4 Independent review of IT security

a) The ministry shall conduct yearly external audit by a STQC/STQC empanelled agency of the implementation of this policy.
b) CSIT shall ensure recommendations for improvements are implemented within one month's time where applicable.
c) CSIT shall ensure the results of the external audit shall be discussed in their meetings. These records shall be maintained.

3.5 Identification of risks

a) CSIT shall conduct risk assessment and implement risk management processes to reduce the risk of disruption and improve the security posture.

b) CSIT shall identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.

c) CSIT shall review the risks from third party access once every year.

d) CSIT shall evaluate information regarding security risks from external parties getting access to critical information or information assets, before deciding the engagement of external parties by the ministry.

e) Based on the criticality of the system or process involved, CSIT shall reassess the risks and service levels whenever there is a requirement to change external party services.

3.6 Organization level best Practices

a) Implement application white listing to ensure would only approved applications can be executed on user machines.

b) Enforce Multi factor Authentication to prevent phishing attacks that steal email credentials.

c) Enable network segregation to contain malicious activity and prevent successful propagation of malware.

d) Install anti-phishing software that can run on mail server and examine emails for any hyperlink containing phishing websites/malware. This will prevent credential loss.

e) Ensure PATCH Management, done on regular basis especially on servers where unpatched remote desktop software if present could lead to cyber-attacks. Else remove unused o0r unpatched software from computers.

f) Ensure password policy in the organization to ensure that a minimum strength of password is compiled with across the network. This will help prevent brute force attack.

g) Periodical audit of IT systems.

h) Educate staff on phishing attacks and email compromise frauds.

i) Use firewall access control list to restrict direct network access to user machines so only approved devices are allowed to connect to them.

j) Perform regular backups to allow quick restoration of impacted devices.

3.7 Remedial measures in case the system is compromised

a) Disconnect the infected systems from LAN/internet immediately.

b) Remove unused or non-updated software’s from the computers.

c) Change password of all email and online services from another secure computer.

d) Format HDD of infected computer after taking backups.

e) Backup data to be scanned for virus before restoring it.

4 INFORMATION ASSET MANAGEMENT

4.1 Purpose

This section deals with the maintenance of appropriate protection of Information and Information assets. Information and information assets are identified, classified and adequately protected by the owners of these assets. It will also ensure that boundaries of acceptable use are clearly defined for anyone that accesses any of the information assets.

4.2 Inventory of ICT assets

a) CSIT shall ensure inventory of all important ICT assets are drawn and maintained with each department.

b) The information asset inventory shall be updated and reviewed once every year.

c) The asset inventory shall include type of asset, owner, location, backup information, manufactured date, purchase date, license information and the asset value (type of assets are hardware, software, information, service).

d) The asset inventory shall note all the critical information to be recovered in case of a disaster.

4.3 Acceptable use of assets

a) Rules for the acceptable use of information and information assets will be identified and documented CSIT.

b) CSIT shall ensure all users follow information assets acceptable usage guidelines.

c) CSIT shall be responsible for communicating acceptable usage guidelines to all users at the time of joining the ministry and on periodically.

4.4 Classification guidelines

a) CSIT shall ensure that a procedure for defining, allocating and reviewing classification of information is documented.

b) Users shall classify information as per the information classification procedure.

c) Users shall ensure access is based on need to know basis (Read, write access based on individual role).

4.5 Information labelling and handling

a) The ICT and Administrative Team shall ensure all assets are labelled using asset tags.

b) Users shall be made aware of their responsibilities regarding handling of sensitive information.

c) All critical information shall be securely protected; files shall be password protected and critical information shall be encrypted.

d) Removable media with confidential information shall be physically labelled.

e) The ICT and Administrative Team shall be responsible for disposing media securely using media destroyers.

f) Removable media shall be stored in lock and key at all times.

g) Backup media shall be labelled and stored in locked fireproof cabinets.

h) Removable media in transit shall be securely stored using bubble wrap or boxes.

4.6 Network security management

a) Networks will be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. The NIC policy to maintain the network and access to the network shall be strictly followed in the ministry.

b) Overall responsibility for network activity will be clearly assigned to an individual (i.e. the network 'owner'). Responsibilities for key tasks will be assigned to one or more individuals who are capable of performing them.

c) CSIT shall ensure that sufficient technology controls are implemented by NIC and regularly monitor the services.

d) Wireless router (if used) will be tested prior to implementation. All access to wireless networks shall have strong authentication mechanisms to prevent unauthorized users.

5 BUSINESS CONTINUITY MANAGEMENT

This section talks about a well-defined and tested business continuity plan to ensure timely resumption of the ministry's critical information assets in the event of disasters, long term outages and disruptions due to security failures.

A practical and well-defined Business Continuity Plan will be prepared to ensure that adequate procedures are in place to recover from disasters and resume normal business operations. Recovery teams will be formed with clear, defined roles and responsibilities. CSIT shall identify critical functions, emergency response team with contact details and ensure that a BCP is in place. The plan must be maintained current and tested / exercised regularly.

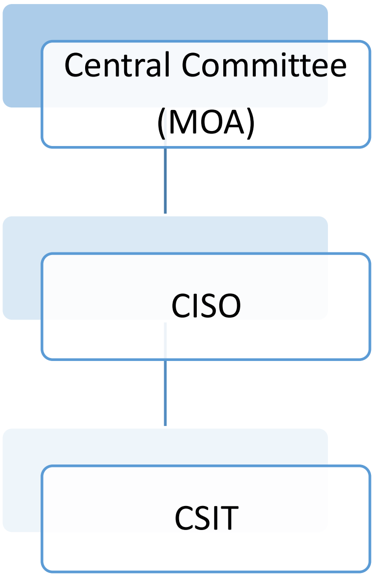
6 GOVERNANCE FRAMEWORK

6.1 Purpose

This section provides the governance framework required to implement this policy.

6.2 Organization & Management

The effective implementation of this security policy will depend upon the availability of resources to purchase and license the required security hardware / software and adequate staffing to manage infrastructure, train users and conduct routine security audit procedures. A central committee shall be formulated and staffed with appropriate level of officers of the ministry. This committee shall meet at least once a year to provide leadership and governance for IT security. CSIT shall be constituted by this committee. CSIT shall report to this committee. The chart below highlights the reporting structure required to implement this policy



6.3 Monitoring & Evaluation

Senior officers shall approve and oversee the implementation of this policy to ensure the protection of information assets against unauthorized or unintentional access, modification, destruction or disclosure.

7 LEGAL AND FINANCE REVIEWS

Due consultations / reviews with the Legal and Internal Finance departments shall be followed to ensure all applicable rules and regulations have been adhered to in this policy prior to approval by competent authority.

8 CONCLUSION

The purpose of this policy is to ensure that all the users in the ministry understand the importance of IT Security as defined in this policy. This IT security policy sets out the Ministry's approach to information security management. It focuses on the three main principles: confidentiality, integrity and availability of information. This comprehensive policy provides guidance for acceptable use and organization of information, information asset management, communication and operational management.