Daisy No- 1954 / e-Gov IT Cell
-1- 11.11.2016.

Haryana Government
Electronics & Information Technology Department
Secretariat For Information Technology

Notification

The 4th November, 2016

No. Admn/432/1SIT/4080-The Governor of Haryana is pleased to notify a comprehensively policy on use of IT Resources of Government in the State, copy of which is attached at Annexure 'X'.

ACSSE
CFMS No. 4438 Date 9-11-16
Mark to DSE
AD-I 10.11.16
AD II 10.11.16

Devender Singh
Principal Secretary to Govt., Haryana
Electronics & Information Technology Department

Endst. No. Admn/432/1SIT/4081 Chandigarh: Dated, the 04.11.2016

A copy is forwarded to the Accountant General (Haryana) for information.

Sr. Administrative Officer
for Principal Secretary to Govt., Haryana
Electronics & Information Technology Department

Circulate & upload on website.

Endst. No. Admn/432/1SIT/4082 Chandigarh: Dated, the 04.11.2016

A copy is forwarded to the Controller, Printing & Stationery Department, Haryana, Chandigarh with the request that the above notification may please be published in Haryana Government (Extra ordinary) gazette immediately and 20 copies thereof be supplied to the department.

10/11

Sr. Administrative Officer
for Principal Secretary to Govt., Haryana
Electronics & Information Technology Department

Endst. No. Admn/432/1SIT/4083 Chandigarh: Dated, the 04.11.2016

A copy, alongwith its enclosure, is forwarded to all the Administrative Secretaries to Government Haryana for information and necessary action.

11/11/16

Sr. Administrative Officer
for Principal Secretary to Govt., Haryana
Electronics & Information Technology Department

CC: Sh. Rajinder Bist, AGM (Hartron) for placing on website.

Enclosure: - Annexure 'X'.

ANNEXURE'X'

GOVERNMENT OF HARYANA.

Policy on use of IT Resources of Government of Haryana

ELECTRONICS & INFORMATION TECHNOLOGY DEPARTMENT.

Table of Contents

- Policy on use of IT Resources of the Government-

1. Introduction

1.1 Government provides IT resources to its employees to enhance their efficiency and productivity. These resources are meant as tools to access and process information related to their areas of work. These resources help Government officials to remain well informed and carry out their functions in an efficient and effective manner.

1.2 For the purpose of this policy, 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.

1.3 Misuse of these resources can result in unwanted risk and liabilities for the Government. It is, therefore, expected that these resources are used primarily for Government related purposes and in a lawful and ethical way.

2. Scope

This policy governs the usage of IT Resources from an end user's [1] perspective. This policy is applicable to all employees of State Government and employees of those State/UT Governments that use the IT Resources of the Government and also those State/UT Governments that choose to adopt this policy in future. The policy shall also cover employees of PSUs/Boards/Corporations and agencies. The policy shall also cover Contractual/consolidated/casual workers or any other workers drawing wages from the public exchequer.

3. Objective

The objective of this policy is to ensure proper access to and usage of Government's IT resources and prevent their misuse by the users. Use of resources provided by Government of India (GoI) and State Government implies the user's agreement to be governed by this policy.

4. Roles and Responsibilities

The following roles are required in each organization [2] using the Central/State/UT Government IT resources. The official identified for the task shall be responsible for the management of the IT resources deployed for the use of entire user base under their respective domain.

4.1 Competent Authority [3] as identified by each organization.

4.2 Designated Nodal Officer [4] as identified by each organization.

4.3 Implementing Agency [5]: The overall responsibility for Information Security will be that of the respective organization. In the interest of security of the network services, it is recommended that the organizations should use the GoI network services provided by NIC, in which case NIC would be the Implementing Agency (IA) for security of network services on behalf of the concerned organization. In organizations not using NIC network services, the respective organization will be the Implementing Agency.

In organizations using SWAN and other state Government network services, the state designated Implementing Agency and state Nodal Agency for SWAN shall be responsible for security of core Network services. However, respective organizations shall be responsible for security of Local Area Networks (LANs) and devices connected to these LANs with in their premises.

4.4 The Nodal Agency [6] for managing all IT Resources except network services shall be the respective organization.

5. Access to the Network

5.1 *Access to Internet and Intranet*

a) A user shall register the client system and obtain one time approval from the competent authority before connecting the client system to the Government network.

b) It is strongly recommended that sensitive offices shall maintain two independent networks, i.e. Internet [7] and Intranet [8]. Both the networks

shall not have any physical connection/devices between them. Users in such deployments shall have two access devices, i.e. desktops. One shall be connected to the internet and the other to the intranet. End point compliance [9] shall be implemented on both the networks to prevent unauthorized access to data.

c) 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.

5.2 Access to Government Wireless Networks

For connecting to a Government wireless [10] network, user shall ensure the following: -

a) A user shall register the access device and obtain one time approval from the competent authority before connecting the access device to the Government wireless network.

b) Wireless client systems and wireless devices shall not be allowed to connect to the Government wireless access points without due authentication.

c) To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

5.3 Filtering and blocking of sites:

a) IA 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.

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

6. Monitoring and Privacy:

6.1 IA shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy.

6.2 IA/Nodal Agency, for security related reasons or for compliance with applicable laws, can access, review, copy or delete any kind of electronic communication or files stored on Government provided devices under intimation to the user. This includes items such as files, e-mails, and Internet history etc.

6.3 IA may monitor user's online activities on Government network, subject to such Standard Operating Procedures as the organization may lay down in this regard.

7. E-mail Access from the Government Network

7.1 Users shall refrain from using private e-mail servers from Government network.

7.2 E-mail service authorized by the Government and implemented by the IA shall only be used for all official correspondence. For personal correspondence, users may use the name-based e-mail id assigned to them on the Government authorized e-mail Service.

7.3 More details in this regard are provided in the "E-mail Policy of the Government".

8. Access to Social Media Sites from Government Network

8.1 Use of social networking sites by Government organizations is governed by "Framework and Guidelines for use of Social Media [11] for Government Organizations" available at http://deity.gov.in.

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

8.3 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.

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

8.5 User shall always user high security settings on social networking sites.

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

8.7 User shall not disclose or use any confidential information obtained in their capacity as an employee/contractor [12] of the organizations.

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

9. Use of IT Devices Issued by the Government.

9.1 IT devices issued by the Government to a user shall be primarily used for Government 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"**. 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.

9.2 Each Government agency shall maintain its own asset register with details of software/Hardware and other IT resources which are operation/ non-operational at their offices. A standard template to maintain such a register is given at **Annexure - A**

10. Responsibility of User Organizations

10.1 Policy Compliance

a) All user organizations shall implement appropriate controls to ensure compliance with this policy by their users. Implementing Agency shall provide necessary support in this regard.

b) A periodic reporting mechanism to ensure the compliance of this policy shall be established by the competent authority of the organization.

c) Nodal Officer of the user organization shall ensure resolution of all incidents related to the security aspects of this policy by their users. Implementing Agency shall provide the requisite support in this regard.

d) Competent Authority of the user organization shall ensure that training and awareness programs on use of IT resources are organized at regular intervals. Implementing Agency shall provide the required support in this regard.

e) User organization shall not install any network/security device on the network without consultation with the IA.

10.2 Policy Dissemination

a) Competent Authority of the user organization should ensure proper dissemination of this policy.

b) Competent Authority may use newsletters, banners, bulletin boards etc. to facilitate increased awareness about this policy amongst their users.

c) Orientation programs for new recruits shall include a session on this policy. (A step by step implementation approach is given at **Annexure - B**)

11. Security Incident Management Process

11.1 A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of Government data.

11.2 IA reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the competent authority of that organization.

11.3 Any security incident[13] noticed must immediately be brought to the notice of the Indian Computer Emergency Response Team (ICERT) and the IA, ISMO Haryana.

12. Scrutiny/Release of logs

12.1 Notwithstanding anything in the above clause, the disclosure of logs relating to or contained in any IT Resource, to Law Enforcement agencies and other organizations by the IA shall be done as per the IT Act, 2000 and other applicable laws.

12.2 IA shall neither accept not act on the request from any other organization, save as provided in this clause, for scrutiny or release of logs.

13. Intellectual Property

Material accessible through the IA's network and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual

property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use the Government network and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

14. Enforcement

14.1 This policy is applicable to all employees of Central /State Governments as specified in clause 2 of this document. It is mandatory for all users to adhere to the provisions of this policy.

14.2 Each organization shall be responsible for ensuring compliance with the provisions of this policy. The implementing Agency would provide necessary technical assistance to the organizations in this regard.

15. Deactivation

15.1 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 IA.

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

16. Audit of Government Network Infrastructure

The security audit of State Government network infrastructure shall be conducted periodically by an organization approved by Deity/State IT Department.

17. Review

Future changes in this Policy, as deemed necessary, shall be made by Deity with approval of the Minister of Communication & IT after due inter-ministerial consultations with DeiTY/NIC and other stakeholders.

GLOSSARY

Sr No.	Term	Definition
1	**Users**	Refers to Government/State/UT employees /contractual employees who are accessing the Government services.
2	**Organization**	Ministry/Department/Board/Corporation/Agency Statutory body/Autonomous body under Central or State Governments.
3	**Competent Authority**	Officer responsible for taking and approving all decisions relating to this policy in his Organization, which will typically be the Principal Secretary or HoD of the organization. e.g. Any orders for compliance shall be issued by the competent authority.
4	**Nodal Officer**	Officer responsible for all matters relating to this policy who will coordinate on behalf of the Organization. This can be any competent officer designated as Nodal Officer by the Competent authority. e.g. Any cyber security issue will be communicated by the nodal officer to ISMO/CERT-in /NIC after approval of competent authority.
5	**Implementing Agency (IA)**	A Body which will be responsible for ensuring compliance with this policy with reference to network services including power to take precautionary and penal actions as specified in this policy. (HARTRON/NIC for SWAN/NICNET) and concerned department for LAN and devices.
6	**Nodal Agency**	Respective organization responsible for ensuring

		compliance with this policy with respect to use of It resources except network services. (Each organization for its IT assets whereas electronics and IT department Haryana shall be overall nodal agency for the State.)
7	**Internet**	Internet is a network of the interlinked computer networking worldwide, which is accessible to the general public. These interconnected computers work by transmitting data through a special type of packet switching which is known as the IP or the Internet Protocol
8	**Intranet**	An intranet is a private network that is contained within an organization. For the purpose of this policy, computers connected to an intranet are not allowed to connect to internet.
9	**End point compliance**	End point compliance is an approach to network protection that requires each computing device on a network to comply with certain standards before network access is granted. Endpoints can include desktops, laptops, smart phones, tablets etc.
10	**Wireless**	Any type of computer network that uses wireless data connections for connecting network nodes. For the purpose of this policy, all the GoI / GoH wireless networks will be deployed in a secure manner.

11	**Social Media**	Applies to social networking sites, blogs, electronic newsletters, online forums, social networking sites, and other services that permit users to share information with others in a contemporaneous manner.
12	**Contractor/contractual employees**	An employee who works under contract for GoI or State Government. A contract employee is hired for a specific job or assignment. A contract employee does not become a regular addition to the GoI staff and is not considered a permanent employee of GoI or State Government.
13	**Security Incident**	Any adverse event which occurs on any part of the government data and results in security threat/breach of the data.

Annexure - 'A'		
Asset Identification Questionnaire		
Name		
Position		
Division Name		
Location		
Name		
The objective of this Information Asset Register is to gather information about the assets (physical, software, information, services, people, paper) within office locations and respective divisions/sections		
The Information Asset Register should be filled up by respective Asset Owners (personnels accountable) or by Asset Custodians (personnels responsible) with inputs from the Asset Owner.		
You are requested to fill up individual worksheets for each individual asset under the ownership/custody of the division/section.The explanations to the format are provided below however,the Asset Register worksheet will also have ready examples		
Explanations to the format		
Name	**Brief description**	**Values/ Examples**
Sl No.	Serial Number	
Asset ID	Identification	
Location	Location of the Assets. i.e. The physical location where the asset has been installed. Which should provide room no, floor,	

	building name etc.	
Office/Branch Name	The name of the Branch/Office within the asset owner organisation where the Asset is being used.	
Asset Name	Name of the asset	
Asset Type 1	Asset type can be either Software Asset, Physical Asset	Windows 10, MS Office 2013, SQL server, PC, Laser Printer etc.
Asset Make	Name of the manufacturing company	HP, Dell, Cisco etc.
Asset Sr No	Sr No. mentioned on the asset	
Date aquired	Date on which the organization acquired the asset.	
Asset Value	Price of the asset at the time of purchase	
Asset Owner	Owner of the Asset will generally mean the Accountability and may generally be the organisation head	
Asset Custodian	Person with delegated responsibility for protecting an asset which generally will be the section/branch head	
Asset Criticality Value	Asset may be rated on 1 to 5 on criticality value. The most critical asset should be rated as 5 and least critical asset as 1.	e.g. Server may be rated as 5. where as a small printer can be rated as 1.
Remarks	One Line on asset description	

Annexure – 'A'

Sl No	Asset ID	Location	Office/ Branch name	Asset Name	Asset Type	Asset Make/ Company	Asset Sr No	Date on which acquired	Asset Value	Asset Owner	Asset Custodian	Asset Criticality Value	Remarks, if any

Annexure – 'B'

Procedure for implementation of "Use of IT resources of the Government"

1. **Adoption and implementation of the policy**

   After approval of the IT PRISM, the policy shall become applicable to all Haryana Government organizations. Each organization will start the process of policy compliance by following the steps given below.

2. **Designate a Competent Authority:**

   Each Government organization will designate the Head of organization as a "Competent Authority". The officer designated as "Competent Authority". For Government Departments, the Principal Secretary of the department should be designated as Competent Authority and for Boards, Corporations, Agencies, the Managing Director or Chairman of the organization should be designated for the purpose of any approvals and decisions related to this policy.

3. **Designate a Nodal Officer:**
   Each origination will designate a senior departmental officer of the level of Additional Director, as a Nodal Officer who will be responsible for coordinating all activities related to the policy.

4. **Define a n escalation matrix for various issues.**
   Each organization will have a clearly defined escalation matrix for any issues related to IT resources.
   a. For organizations connected to NICNET/NKN, Network Division, NIC Haryana will be point of contact for network related issues.
   b. For SWAN connectivity HARTRON will be the point of contact.
   c. NIC and HARTRON shall designate officers as nodal officers for NICNET and SWAN respectively.
   d. For all issues related to LANs within the organization, the nodal officer along with a technical team of the organization will be point of contact.
   e. For Hardware and Software, each organization should have contact numbers and details of vendors who are responsible for maintenance of the equipment.
   This escalation matrix should be displayed in each office/branch of the organization

5. **List and record all IT assets.**

   Each organization will create an asset register as per the format given as **Annexure - A.**

6. **Conduct Training and awareness workshops**

Each organization may conduct a workshop for its employees about the policy. NIC / HARTRON / ISMO will help in organizing such workshops which can also be held in batched of 4-5 departments.

7. Act on cases of non compliance

The competent authority of each organization shall decide on action to be taken on defaulters within the organization who are found to be misusing the IT assets or are found to be guilty of non-compliance of policy directives.

Repeated offences may attract higher penalties as per decision of the competent authority. In severe cases the authority may recommend action as per Indian IT Act 2000.

Annexure – 'C'

"Guidelines for use of IT Devices on Government Networks"

1. Introduction:

Government has formulated the **"Policy on Use of IT Resources"**. This document supports the implementation of this policy by providing the best practices related to use of desktop devices, portable devices, external storage media and peripheral devices such as printers and scanners.

2. Desktop Devices

2.1 Use and Ownership

Desktops shall normally be used only for transacting government work. Users [1] shall exercise their own good judgment and discretion towards use of desktop devices for personal use to the minimum extent possible.

2.2 Security and Proprietary Information

a. User shall take prior approval from the competent authority [2] of their respective organizations [3] to connect any access device to the Government network.

b. User shall keep their passwords secure and not share their account details. Users shall keep strong and secure passwords as per the password policy.

c. All active desktop computers shall be secured with a password-protected screensaver which should be set with automatic activation at 10 minutes or less, or log-off when the system is unattended.

d. Users shall ensure that updated virus-scanning software is running in all systems. Users shall exercise due caution when opening e-mail attachments received from unknown senders as they may contain viruses, e-mail bombs, or Trojan horse code. Preferably a central antivirus software will be used on all systems which are connected to Government Networks. This central antivirus software shall be managed by the Implementing Agency which will keep the Antivirus Server updated with latest software updates and shall ensure to implement policies centrally.

e. User shall report any loss of data or accessories to the competent authority of their respective organization.

f. User shall obtain authorization from the competent authority before taking any Government issued desktop outside the premises of their organization.

g. Users shall properly shut down the systems before leaving the office.

h. In case an organization does not have two networks, as recommended in the Policy on "Use of IT Resources" Classified/ sensitive data shall not be stored on the desktop connected to the internet.

i. Users shall encrypt all sensitive information while storing it on the desktop. If no licensed encryption software is available, any Open Source (FOSS) shall be used for encryption. The IA shall recommend suitable FOSS for encryption of data.

j. By default all interfaces on the client system shall be disabled and those interfaces that are required are enabled.

k. Booting from removable media shall be disabled.

l. Users shall be given an account with limited privileges on the client systems. User shall not be given administrator privileges.

m. Users shall abide by instructions or procedures as directed by the IA [4] /Nodal agency [5] from time to time.

n. If users suspect that their computer has been infected with a virus (e.g. it might have become erratic or slow in response), it should be reported to the IA/Nodal Agency for corrective
action.

o. The Annual Maintenance Contract with service providers should include a clause that Hard Disk should be retained by the Organization, even if it is faulty. While disposing the Hard disk it should be destroyed so that data cannot be retrieved.

2.3 Use of software on Desktop systems

a. Users shall not copy or install any software on their own on their desktop systems, including privately owned shareware and freeware without the approval of the competent authority.

b. A list of allowed software shall be made available by the IA. Apart from the Software mentioned in the list, no other software will be installed on the client systems. Any addition to the list by the respective organizations should be done under intimation to IA.

c. New Government computer systems should preferably be purchased with pre loaded operating system with sufficient maintenance support from the vendor.

d. If no licensed software is available for common office applications, FOSS as recommended by the IA should be used on Government systems.

2.4 Sharing of data

Users shall not share their account(s), passwords, security tokens (i.e. smartcard), Personal Identification Numbers (PIN), digital signatures certificate or similar information or devices which is used for identification and authorization purposes.

2.5 Use of network printers and scanners

a. User shall use a strong administrator password on the device to help defend against attacks and to prevent re-configuration by an unauthorized user.

b. Where the device supports Access Control Lists (ACLs), the devices shall be configured to block all traffic from outside the Organization's IP range.

c. FTP and telnet server on the printer shall be disabled.

d. User shall disable any protocol or service not required.

3. Use of Portable devices

Devices covered under this section include Government issued laptops, mobiles, iPads, tablets, PDAs etc. Use of the devices shall be governed by the following:

a. User shall be held responsible for any unauthorized usage of their Government issued access device by a third party

b. Users shall keep the Government issued devices with them at all times or store them in a secured location when not in use. User should not leave the devices unattended in public locations (e.g. airport lounges, meeting rooms, restaurants, etc.).

c. User shall ensure that the portable devices are password protected and auto lockout enabled. The password used should be as strong as the device may support and should be as per the password policy available in "Password Policy" notified by the Government.

d. User shall ensure that remote wipe feature is enabled on the Government issued device, wherever technically feasible. Users shall not circumvent security features on their devices.

e. The concerned nodal officer of the organization shall ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User. Firewalls shall be enabled, if possible. As indicated **2.2 d,** central antivirus should preferably be used.

f. Users shall wipe or securely delete data from the device before returning/ disposing it off.

g. Lost, stolen, or misplaced devices shall be immediately reported to the IA/Nodal agency and the competent authority of the organization.

h. Data transmissions from devices to the services on the Government network shall be over an encrypted channel.

i. When installing software, user shall review the application permissions to ensure that unwanted information regarding the user is not shared with the application provider.

4. External Storage Media:

Devices covered under this section include Government issued CD/DVD's, USB storage devices etc. Use of these devices shall be governed by the following:

a. Use of external storage [6] media, by default shall not be allowed in the Government network. If the use of external storage is necessary, due approval from the competent authority of that respective organization shall be taken.

b. Blocking access to external storage on a Government issued access devices like desktop/laptop etc shall be implemented at all organizations within the Government. Users authorized by the competent authority of the organization to use the external storage will be allowed as per the policies configured by the IA/Nodal agency.

c. Users shall use only the media issued by the organization for all official work. The user shall be responsible for the safe custody of devices and contents stored in the devices which are in their possession.

d. Classified data shall be encrypted before transferring to the designated USB device. The decrypting key shall not exist on the same device where encryption data exists.

e. Classified/ sensitive information shall be stored on separate portable media. User shall exercise extreme caution while handling such media.

f. Unused data on USB devices shall be cleaned through multiple pass process (like wipe/eraser software)

g. Users shall not allow USB device belonging to outsiders to be mounted on Government systems.

4.1 Use of External storage media by a visitor

a. Competent authority shall ensure that process is in place that visitors to an organization shall not be allowed to carry any portable media without permission.

b. If it is necessary to allow the visitor to use a USB memory device for any reason, it shall be used only on designated systems meant for presentation purpose. Under no circumstances the USB device belonging to visitors shall be mounted on systems that are connected and belong to the Government network.

4.2 Authority issuing External storage devices of each organization shall adhere to the following:

a. Competent Authority of an organization shall ensure that process is in place to maintain records for procurement, issue, return, movement and destruction of the storage devices

b. All obsolete USB devices shall be physically destroyed to avoid misuse.

c. Self-certification for verification of USB devices by individuals at regular intervals of 6 months shall be carried out by issuing authority to ensure that devices issued to them are under their safe custody.

GLOSSARY

S.no	Term	Definition
1	**Users**	Refers to Government/State/UT employees who are accessing the Government services.
2	**Competent Authority**	Officer responsible for taking and approving all decisions relating to this policy in his organization.
3	**Organization**	For the purpose of this policy, organization refers to all ministries/departments/offices/statutory bodies/autonomous bodies, both at the Central and State level. Government organizations offering commercial services are not included.
4	**Implementing Agency (IA)**	A Body which will be responsible for ensuring compliance with this policy with reference to network services including power to take precautionary and penal actions as specified in this policy.
5	**Nodal agency**	Respective organization responsible for ensuring compliance with this policy with respect to use of It resources except network services.
6	**External Storage**	In computing, external storage comprises devices that temporarily store information for transporting from computer to computer. Such devices are not permanently fixed inside a computer
7	**FOSS**	Free and Open Source Software

Annexure - 'D'

Name of the Document		*Password Policy*	
Classification	*Restricted*	**Audience**	*NICNET Administrators, Users and Application Developers*
Version	*2.1*	**Data of last change**	*September 01, 2009*

Password Policy

1.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of the passwords.

2.0 Scope

The scope of this policy includes all end-users and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system/service in the NIC domain. These include personnel with their designated desktop systems. The scope also includes designers and developers of individual applications.

3.0 Policy

3.1 Policy Statements

3.1.1 For users having accounts for accessing systems/services

3.1.1.1 Users shall be responsible for all activity performed with their personal user IDs. Users shall not permit others to perform any activity with their user IDs or perform any activity with IDs belonging to other users.

3.1.1.2 All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed periodically (at least once every three months). Users shall not be able to reuse previous passwords.

3.1.1.3 Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers and characters.

3.1.1.4 Passwords shall not be stored in readable form in batch files, automatic logon scripts, Internet browsers or related data communication software, in computers without access control, or in any other location where unauthorized persons might discover or use them.

3.1.1.5 All access codes including user ID passwords, network passwords, PINs etc. shall not be shared with anyone, including personal assistants or secretaries. These shall be treated as sensitive, confidential information.

3.1.1.6 All PINs (Personal Identification Numbers) shall be constructed with the same rules that apply to fixed passwords.

Name of the Document		*Password Policy*	
Classification	*Restricted*	**Audience**	*NICNET Administrators, Users and Application Developers*
Version	*2.1*	**Data of last change**	*September 01, 2009*

3.1.1.7 Passwords must not be communicated though email messages or other forms of electronic communication such as phone to anyone.

3.1.1.8 Passwords shall not be revealed on questionnaires or security forms.

3.1.1.9 Passwords of personal accounts should not be revealed to the controlling officer or any co-worker even while on vacation unless permitted to do so by designated authority.

3.1.1.10 The same password shall not be used for each of the systems/applications to which a user has been granted access e.g. a separate password to be used for a Windows account and an UNIX account should be selected.

3.1.1.11 The "Remember Password" feature of applications shall not be used.

3.1.1.12 Users shall refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site.

3.1.1.13 First time login to systems/services with administrator created passwords, should force changing of password by the user.

3.1.1.14 If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.

3.1.1.15 The password shall be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

3.1.2 For designers/developers of applications/sites

3.1.2.1 No password shall be traveling in clear text; the hashed form of the password should be used. To get around the possibility of replay of the hashed password, it shall be used along with a randomization parameter.

3.1.2.2 The backend database shall store hash of the individual passwords and never passwords in readable form.

3.1.2.3 Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers and characters.

3.1.2.4 Users shall be required to change their passwords periodically and not be able to reuse previous passwords.

3.1.2.5 For Password Change Control, both the old and new passwords are required to be given whenever a password change is required.

Name of the Document		*Password Policy*	
Classification	*Restricted*	**Audience**	*NICNET Administrators, Users and Application Developers*
Version	*2.1*	**Data of last change**	*September 01, 2009*

3.2 Policy for constructing a password

All user-level and system-level passwords must conform to the following general guidelines described below.

3.2.1 The password shall contain more than eight characters.
3.2.2 The password shall not be a word found in a dictionary (English or foreign).
3.2.3 The password shall not be a derivative of the user ID, e.g. <username>123.
3.2.4 The password shall not be a slang, dialect, jargon etc.
3.2.5 The password shall not be a common usage word such as names of family, pets, friends, co-workers, fantasy characters, etc.
3.2.6 The password shall not be based on computer terms and names, commands, sites, companies, hardware, software.
3.2.7 The password shall not be based on birthdays and other personal information such as addresses and phone numbers.
3.2.8 The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc. or any of the above spelled backwards.
3.2.9 The password shall not be any of the above preceded or followed by a digit (e.g., secret1, 1secret).
3.2.10 The password shall be a combination of upper and lower case characters (e.g. a-z, A-Z), digits (e.g. 0-9) and punctuation characters as well and other characters (e.g., !@# $%^&*()_+|~-=\`{}[]:";'<>?,./).
3.2.11 Passwords shall not be such that they combine a set of characters that do not change with a set of characters that predictably change.

3.3 Suggestions for choosing passwords

Passwords may be chosen such that they are difficult-to-guess yet easy-to-remember. Methods such as the following may be employed :

3.3.1 String together several words to form a pass-phrase as a password.
3.3.2 Transform a regular word according to a specific method e.g. making every other letter a number reflecting its position in the word.
3.3.3 Combine punctuation and/or numbers with a regular word.
3.3.4 Create acronyms from words in a song, a poem, or any other known sequence of words.

Name of the Document		*Password Policy*	
Classification	*Restricted*	**Audience**	*NICNET Administrators, Users and Application Developers*
Version	*2.1*	**Data of last change**	*September 01, 2009*

3.3.5 Bump characters in a word a certain number of letters up or down the alphabet.
3.3.6 Shift a word up, down, left or right one row on the keyboard.

4.0 Responsibilities

4.1 All individual users having accounts for accessing systems/services in the NIC domain, and system/network administrators of NIC servers/ network equipments shall ensure the implementation of this policy.
4.2 All designers/developers responsible for site/application development shall ensure the incorporation of this policy in the authentication modules, registration modules, password change modules or any other similar modules in their applications.

5.0 Compliance

5.1 Personnel authorized as Internal Audit shall periodically review the adequacy of such controls and their compliance.
5.2 Personnel authorized as Application Audit shall check respective applications for password complexity and password policy incorporation.