

Section x	IS Security Policies	mm/dd/yy	-Effective
Policy x.xx	Password	mm/dd/yy	-Revised
		Information Services	-Author

Introduction

User authentication is a means to control who has access to an Information Resource system. Controlling the access is necessary for any Information Resource. Access gained by a non-authorized entity can cause loss of information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to [AGENCY].

Three factors, or a combination of these factors, can be used to authenticate a user. Examples are:

- Something you know – password, Personal Identification Number (PIN)
- Something you have – Smartcard
- Something you are – fingerprint, iris scan, voice
- A combination of factors – Smartcard and a PIN

Purpose

The purpose of the [AGENCY] Password Policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the [AGENCY] user authentication mechanisms.

Audience

The [AGENCY] Password Policy applies equally to all individuals who use any [AGENCY] information resource.

Section x	IS Security Policies	mm/dd/yy	-Effective
Policy x.xx	Password	mm/dd/yy	-Revised
		Information Services	-Author

Definitions

Information Resources (IR): any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM): Responsible to the State of Minnesota for management of the agency's information resources. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Minnesota to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Commissioner or Director, and this person is responsible for adhering to the duties and requirements of an IRM.

Information Security Officer (ISO): Responsible to the IRM for administering the information security functions within the agency. The ISO is the agency's internal and external point of contact for all information security matters.

Information Services (IS): The name of the agency department responsible for computers, networking and data management.

Password: A string of characters which serves as authentication of a person's identity, which may be used to grant, or deny, access to private or shared data.

Strong Passwords: A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically the longer the password the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about you such as a birth date, social security number, and so on.

Section x	IS Security Policies	mm/dd/yy	-Effective
Policy x.xx	Password	mm/dd/yy	-Revised
		Information Services	-Author

Password Policy

- All passwords, including initial passwords, must be constructed and implemented according to the following [AGENCY] IR rules:
 - ❖ it must be routinely changed
 - ❖ it must adhere to a minimum length as established by [AGENCY] IS
 - ❖ it must be a combination of alpha and numeric characters
 - ❖ it must not be anything that can easily tied back to the account owner such as: user name, social security number, nickname, relative's names, birth date, etc.
 - ❖ it must not be dictionary words or acronyms
 - ❖ password history must be kept to prevent the reuse of a password
- Stored passwords must be encrypted.
- User account passwords must not be divulged to anyone. [AGENCY] IS and IS contractors will not ask for user account passwords.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with [AGENCY].
- If the security of a password is in doubt, the password must be changed immediately.
- Administrators must not circumvent the Password Policy for the sake of ease of use.
- Users cannot circumvent password entry with auto logon, application remembering, embedded scripts or hardcoded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the [AGENCY] ISO. In order for an exception to be approved there must be a procedure to change the passwords.
- Computing devices must not be left unattended without enabling a password-protected screensaver or logging off of the device.
- IS Helpdesk password change procedures must include the following:
 - ❖ Authenticate the user to the helpdesk before changing password
 - ❖ Change to a strong password
 - ❖ the user must change password at first login
- In the event passwords are found or discovered, the following steps must be taken:
 - ❖ Take control of the passwords and protect them
 - ❖ Report the discovery to the [AGENCY] Help Desk
 - ❖ Transfer the passwords to an authorized person as directed by the [AGENCY] ISO

Section x	IS Security Policies	mm/dd/yy	-Effective
Policy x.xx	Password	mm/dd/yy	-Revised
		Information Services	-Author

Password Guidelines

- Passwords must be changed at least every 60 days.
- Passwords must have a minimum length of 8 alphanumeric characters
- Passwords must contain a mix of upper and lower case characters and have at least 2 numeric characters. The numeric characters must not be at the beginning or the end of the password. Special characters should be included in the password where the computing system permits. The special characters are (!@#\$%^&* _+=?/~`.;:<>|).
- Passwords must not be easy to guess and they:
 - must not be your Username
 - must not be your employee number
 - must not be your name
 - must not be family member names
 - must not be your nickname
 - must not be your social security number
 - must not be your birthday
 - must not be your license plate number
 - must not be your pet's name
 - must not be your address
 - must not be your phone number
 - must not be the name of your town or city
 - must not be the name of your department
 - must not be street names
 - must not be makes or models of vehicles
 - must not be slang words
 - must not be obscenities
 - must not be technical terms
 - must not be school names, school mascot, or school slogans
 - must not be any information about you that is know or is easy to learn (favorite - food, color, sport, etc.)
 - must not be any popular acronyms
 - must not be words that appear in a dictionary
 - must not be the reverse of any of the above
- Passwords must not be reused for a period of one year
- Passwords must not be shared with anyone
- Passwords must be treated as confidential information

Section x	IS Security Policies	mm/dd/yy	-Effective
Policy x.xx	Password	mm/dd/yy	-Revised
		Information Services	-Author

Creating a strong password

- Combine short, unrelated words with numbers or special characters. For example: eAt42peN
- Make the password difficult to guess but easy to remember
- Substitute numbers or special characters for letters. (But do not just substitute) For example:
 - livefish - is a bad password
 - L1veF1sh - is better and satisfies the rules, but setting a pattern of 1st letter capitalized, and i's substituted by 1's can be guessed
 - !!v3f1Sh - is far better, the capitalization and substitution of characters is not predictable

Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of [AGENCY] Information Resources access privileges, civil, and criminal prosecution.

Section x	IS Security Policies	mm/dd/yy	-Effective
Policy x.xx	Password	mm/dd/yy	-Revised
		Information Services	-Author

Supporting Information

This Security Policy is supported by the following Security Policy Standards

Reference # Policy Standard detail

- 1 IR Security controls must not be bypassed or disabled.

- 2 Security awareness of personnel must be continually emphasized, reinforced, updated and validated.

- 3 All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.

- 4 Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the custodian or owner department management.

- 5 Access to, change to, and use of IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service.

- 9 On termination of the relationship with the agency users must surrender all property and IR managed by the agency. All security policies for IR apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.

- 16 Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.

Section x	IS Security Policies	mm/dd/yy	-Effective
Policy x.xx	Password	mm/dd/yy	-Revised
		Information Services	-Author

References

Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
IRM Act Standard 16