6.1 Information Systems Passwords

OVERVIEW

Passwords are an important aspect of information security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Legislative Branch's entire network. Therefore, all Montana Legislative Branch employees, contractors, and vendors with access to the network are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

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.

SCOPE

The scope of this policy includes all Montana Legislative Branch employees, Legislators, contractors, vendors, or others who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides in the Legislative Branch network.

POLICY

All Montana Legislative Branch information systems, including desktop computers, laptop computers, personal digital assistants (PDAs), wireless capable cell phones, or any other memory capable device that may connect to the Montana Legislative Branch network or store State of Montana information, must restrict access to the device by use of a unique user ID (username) and password.

When appropriate, password restrictions must be employed at the operating system level (initial logon) and at the application level (access to sensitive data).

6.1.1 User Responsibilities

The Legislative Branch shall implement strong password and access authentication procedures for both internal and external users.

Passwords

All platforms and services permitting access must use *strong passwords*.

User account passwords must contain a minimum of eight characters. All passwords must consist of at least one upper case alphabetic character, one lower case alphabetic character, one numeric character, and one special character. (ex: gr1sRUL!, Byzdroo1!)

<u>Password Protection</u>

Users are not allowed to share Legislative Branch passwords. All passwords are to be treated as sensitive information. Users may not write down passwords for storage. Additionally, users should not store unencrypted passwords in any file on any computer system (including PDAs or similar devices). There will be standard Legislative Branch password management software with (storage and transmission) encryption made available to staff, which is the only authorized method of recording passwords for storage/transmission of passwords.

<u>Passwords Construction</u>

Strong passwords provide the first line of defense against improper access and compromise of sensitive information. Strong passwords typically exhibit the following best practice characteristics:

Are at least eight characters in length

Contain both upper and lower case alphabetic characters (e.g., a-z, A-Z)

Contain numeric characters (e.g., 0-9)

Contain special characters (e.g.,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

No more than two sequential characters

Are not words in any language, slang, dialect, jargon, etc.

Are not based on personal information, names of family, etc.

Are not written down or stored in plain text online

Should be easily remembered

Should never be a null password

Should never be passwords that are the same as user ID

<u>Password Expiration</u>

Passwords require a maximum expiration age of 60 days. Previously used passwords may not be reused.

<u>Account Management</u>

Users shall not use the same passwords from personal accounts as state system passwords. Passwords must be different between state accounts and non-state accounts to ensure a compromise of a personal password does not endanger a state system.

Failed logon attempts will be limited to three before the system or application initiates a *lockout*. Contact the Legislative Branch IT Helpdesk to unlock the account and/or reset the password.

All systems should be configured for automatic screen saver activation within a 15-minute period of inactivity. Users are required to use the manual lock feature whenever the system is left unattended. This action should invoke a password protected screen saver and overrides the 15-minute automated setting.

Users are required to log off and shut down their systems prior to leaving for the day.

Automatic Login Actions

Users shall refuse all opportunities presented by applications and/or Internet sites to use automatic login capabilities.

Password Compromise

If a user account or password is suspected of being compromised, the user should immediately change the password and report the incident to the Legislative Branch Information Security Officer (ISO).

6.1.2 System and Network Administrators

Access Rights

Information custodian and business process owners shall determine appropriate individual access to Legislative Branch information resources (systems, applications, data, etc.).

System and network administrators are responsible for ensuring that each user ID requested for a specific access is an authorized user ID and for validating any change to access rights associated with that user ID.

Account Assignment/User Identification

System and network administrators are required to assign each Legislative Branch "user" with a unique user ID for each information system and network account requiring access. Each user ID must be composed of at least six characters based on a nonidentifiable system (i.e., not first initial of last name, last name, work area, etc.) and bound to a unique password.

Group accounts should not be authorized, unless absolutely required for system specific issues.

A user ID should be deactivated ONLY when the appropriate information custodian or business process owner specifies a change to the appropriate system and network administrator. System or network administrators will deactivate any account that has not been active for a 90-day period.

No user accounts will be deleted without the direction of the Legislative Branch ISO or prior to the ISO informing the respective director.

Password Generation/User Authentication

All services permitting access must use *strong passwords*.

User account passwords must contain a minimum of eight characters. All passwords must consist of at least one upper case alphabetic character, one lower case alphabetic character, one numeric character, and one special character. (ex: gr1sRUL!, Byzdroo1!)

Password Expiration

All end user passwords should have a maximum expiration age of 60 days. Automated password expiration prompts should be implemented at least 7 days prior to remind users when to change their passwords. Previously used passwords may not be reused.

Password Administration/Account and Password Resets

Administrators/IT helpdesk personnel may not ask for the user's password. Administrators/IT helpdesk personnel may never retain or document user passwords except to notify the user of a temporary password for an account that requires a password change upon initial logon or as directed by the Legislative Branch ISO.

Automated password resets must generate a temporary password, and the system must require the user to immediately change the user's password upon next logon.

All operating system default passwords must be replaced with strong passwords prior to that machine's delivery for use or entry onto the Legislative Branch network.

Failed logon attempts must be limited to three before the system or application initiates a *lockout*. Contact the Legislative Branch IT Helpdesk to unlock the account and/or reset the password. **Documented procedures must be in place and followed to authenticate users on password reset requests.**

All preconfigured passwords must be encrypted or otherwise obfuscated from the user's view. **Passwords must be stored and transmitted using encryption.**

Password Protection

Administrators are restricted from sharing Legislative Branch admin passwords with anyone. All passwords are to be treated as sensitive information.

Administrators may not write down passwords for storage, except when authorized by the Legislative Branch ISO for use in conjunction with certain business continuity processes. Additionally, administrators should not store unencrypted passwords in any file on any computer system (including PDAs or similar devices) without the express authorization of the Legislative Branch ISO. There will be standard Legislative Branch password management software with (storage and transmission) encryption made available to staff, which is the only authorized method of recording passwords for storage/transmission of passwords.

Passwords for Different Accounts

Administrators should differentiate passwords between their admin, service, and user accounts. Administrators will not use their elevated admin accounts for normal day-to-day business. Admin accounts are only to be used when required for administrative purposes only. The use of admin accounts for anything other than administrative purposes is prohibited. Administrators should not use admin passwords for other Legislative Branch accounts and non-Legislative Branch accounts (i.e., personal ISP account, interagency access, etc.).

Account Management

Contractual provisions between the Legislative Branch and any externally connected entity must be established in which the externally connected entity accepts responsibility for the acts or omissions of its users and assumes all liability for managing access to the Legislative Branch data through the entity's accounts.

Account Log Management

All applications, computing platforms, and network components that support account logging must have account logging enabled.

- Review of the *account log files* for security relevant events must be conducted on a regular basis.
- Audit trails should be retained as specified in the Records Retention Policy.

Any inconsistencies or security relevant events identified in the audit log should be reported to the Legislative Branch ISO.

Password Compromise

If an admin password is suspected of being compromised, the administrator should immediately change the password and report the incident to the Legislative Branch ISO.

If personnel changes occur, which affect admin password confidentiality, the admin password must be changed no later than the last duty day for the affected personnel.

If a service account password is suspected of being compromised, the administrator should immediately change the password, start the password change management process, and report the incident to the Legislative Branch ISO.

Compliance Testing

The Legislative Branch ISO or representative will perform periodic, random password audits via automated tools. The Legislative Branch ISO is responsible for conducting a quarterly review and report of all active user IDs and their associated access rights.

6.1.3 Management Responsibilities

Business Processes

Management shall ensure education and awareness training is conducted prior to implementation.

Management shall provide all tools necessary to ensure users are able to comply with this policy prior to implementation.

Password Protection

Management shall ensure that Legislative Branch personnel are treating passwords as sensitive information.

Passwords for Different Accounts

Management shall promote information protection efforts by requiring users to use different passwords between Legislative Branch accounts and non-Legislative Branch accounts (i.e., personal ISP account, agency access, etc.).

Password Compromise

If any password is suspected of having been compromised, management should immediately change the password and report the incident to the Legislative Branch ISO.

REFERENCES

MT ITSD ENT-SEC-063
2-15-114, MCA
2-17-534, MCA