Authentication Credential Policy

Introduction

An authentication credential is essentially a key that "opens the door" to information systems and the data stored within them. Credential management is a practical approach to protecting judiciary information and its associated information technology (IT) infrastructure by ensuring that access to data is protected in a consistent manner commensurate with the risk of harm to judiciary operations in the event of a data breach. The United States District Court and Probation Office for the Northern District of Mississippi (MSND/MSNP) has created this policy to ensure all users and information systems within its purview manage credentials consistently across their life cycle.

Purpose

The purpose of this policy is to ensure that MSND/MSNP's information systems and data are protected against unauthorized access and misuse and that all users of MSND/MSNP resources are aware of their obligations to create, protect, and securely manage credentials across their life cycle.

Scope

This Policy applies to all IT assets owned, leased, or operated on behalf of MSND/MSNP and in the MSND/MSNP system boundary that require passwords for authentication. All MSND/MSNP employees, contractor personnel, interns, visitors, and other non-government employees are obligated to comply with this policy.

Policy

MSND/MSNP's information systems and the users of these resources must comply with the credential management standards as set forth in this policy. The Operations Manager for IT ensures a comprehensive credential management process is developed ensuring procedures are documented in a credential management plan with guidance on general credential use; system administrator, application developer, and end user accounts; training and awareness; and credential compromise. IT staff are assigned roles and responsibilities for implementing credential management procedures.

General Credential Use

The following general standards apply to all MSND/MSNP's local court information systems, in accordance with the Guide, Vol. 15, Ch.3, § 390 Identification and Authentication, and the Guide, Vol. 15, Ch. 3 § 330.80 Voice Mail System Security:

- Users must never provide anyone their credentials, nor should anyone other than the authorized user make use of remote access to judiciary networks.
- MSND/MSNP has adopted the JENIE password standards. Where applicable, JENIE authentication via single sign-on will be used instead of local accounts and password policies.
- Default passwords are changed on all information systems before operational deployment.
- Administrative accounts are assigned to individuals who are responsible for maintaining, operating, and securing systems.
- All devices (e.g., Surface Pros, desktops, laptops, smart phones, flash drives, servers, network equipment) that access, store, transmit, or process sensitive judiciary information are password-protected when capable.

- Where supported, MSND/MSNP systems automatically require passwords to be changed every 180 days. If automated means to force a password change are unavailable, users are notified via email, bi-annually to manually change their password.
- Where supported, MSND/MSNP systems maintain a password history so that a password that is one of the four most recently used passwords cannot be reused.
- All remote access to the Data Communications Network (DCN) and the local MSND/MSNP networks will only be facilitated with the national solution for remote access which incorporates two-factor authentication for the virtual private network (VPN), in accordance with the Guide, Vol. 15, Ch. 3, § 330.60.30 Virtual Private Network.
- The number of attempts that a user can enter an incorrect password is three times before the account is automatically disabled for 30 minutes.
- All information systems, with the technical capability, enforce the local password policy to ensure compliance.
- Password recovery and reset requests must be submitted to the MSND/MSNP Help Desk for staff that have locked their accounts, lost their passwords, or whose passwords have been compromised.
- Secure password storage practices are implemented to prevent intruders with physical or unauthorized system access from gaining access to the passwords, in accordance with the Guide, Vol. 11, Ch. 6, § 660 Access Restrictions.
- Passwords transmitted over internal and external networks are encrypted or transmitted in a hashed format for capable systems.
- MSND/MSNP information contained on mobile devices such as iPhones, iPads, laptops, and other portable devices is encrypted, and access to these devices are password protected in accordance with the Password Policy Resource Packet (RP).
- Passwords are not hardcoded during application development and are encrypted when stored.
- Multi-factor authentication (MFA) is enabled on all non-shared workstations. Users may use either a Personal Identity Verification-Interoperable (PIV-I) card or a national system providing multi-factor authentication services (e.g., DUO) as a second-factor when logging into the workstation.

For national systems and applications, the password complexity and security are enforced by those systems.

System Administrator Accounts

As noted in the Password Policy Resource Packet (RP), system administrators have privileged access to information systems where they can change operational and security settings. Therefore, it is critical that their accounts meet more stringent security standards than those of the typical end user. In accordance with the Password Policy Resource Packet (RP), all administrative accounts meet the following standards:

- Activities performed by an administrator are attributable only to that individual administrator.
- Role management provisions are in place so that one administrator can take over the functions of another without having to know the other's password.

- The minimum password length for administratively controlled devices (e.g., network devices, servers) is twelve (12) characters, which contain numbers, special symbols, and upper and lowercase letters.
- Accounts with system-level privileges (for example "root" accounts) require passwords that are different from all other accounts assigned to that user.

End User Accounts

The following password requirements for end users ensure that access to systems is protected in a secure and consistent manner.

All end user accounts meet the following standards in accordance with the Password Policy Resource Packet (RP) and the Guide, Vol. 15, Ch. 3 § 330.80 Voice Mail System Security:

- End users are immediately forced to change passwords issued by the system administrator during the user's first login session.
- Users are required to create strong passwords that include a minimum of eight characters, which include three of the following categories on all systems which support complex passwords. Where possible, administrators will configure systems to require such complex passwords.
    - Uppercase characters (A-Z)
    - Lowercase characters (a-z)
    - Numbers (0-9)
    - Special symbols: ! @ # $ % ^ & * ( ) _ + | ~ - = \ ` { } [ ] : " ; ' < > ? , / (NOTE: some characters may not be supported on all Judiciary systems).
- End user access codes for voice mail systems are defined by the National Internet Protocol Telephone offering implemented at all MSND/MSNP locations.
- Users are required to securely manage their passwords to include:
    - Changing their passwords every 180 days.
    - Changing default passwords on assigned IT equipment, portable electronic devices, mobile phones, etc. in accordance with the Guide, Vol. 15, Ch. 3, § 330.10.25 Default Settings.
    - Not sharing their username and passwords with anyone (e.g., supervisors, co-workers, family, etc.). If users must share their passwords with the Help Desk due to extenuating circumstances (e.g., the Help Desk cannot access users' systems remotely to assist them), the password must be reset by the user after the need has been resolved.
    - Passwords to websites should not be stored in such a way as to bypass the authentication process.

When practical, single sign-on, self-service password reset, and secure password manager technologies will be incorporated into MSND/MSNP's operational environment to help users securely manage multiple passwords.

IT Security Training and Awareness

It is important to properly train users of their obligations to securely manage their credentials in accordance with the Guide, Vol. 15, Ch. 3, § 340 IT Security Training and Awareness and How to Build an Effective IT Security Training and Awareness Program Resource Packet (RP).

Credential training and awareness are integrated into the content of MSND/MSNP's initial, annual, and refresher IT training and awareness efforts for users and includes:

- Training users on creating and protecting strong passwords across their life cycle.
- Ensuring users are aware of MSND/MSNP's local incident reporting procedures.
- Ensuring users know to password-protect their mobile devices.
- Ensuring users understand they are responsible for activity performed with their user-IDs and credentials.
- Ensuring users understand special precautions that may be needed when working from home or on a public terminal.

Credential Compromise

Consistent with MSND/MSNP's local incident response procedures, the following actions are taken when a credential compromise is suspected:

- User or system credentials are immediately disabled to avoid the possibility of unauthorized activity being attributed to an authorized user.
- MSND/MSNP's Computer Incident Response Team (CIRT) personnel notify the user or system owner of the suspected compromise.
- A thorough investigation is performed to gauge the possible level of exposure.
- Corrective measures are performed immediately to eradicate the cause of the compromise and to prevent the attacker from compromising new credentials in the same manner. For example, if the attacker used a keystroke logger to capture the user's password, the malicious software is removed before the user establishes a new one.
- Users are advised to change the passwords on all systems that used the same password as the compromised system.

References

Guide to Judiciary Policy

- Vol. 11, Ch. 6, § 660 Access Restrictions
- Vol. 15, Ch. 3, § 330.10.25 Default Settings
- Vol. 15, Ch. 3, § 330.60.30 Virtual Private Network
- Vol. 15, Ch. 3 § 330.80 Voice Mail System Security
- Vol. 15, Ch. 3, § 340 IT Security Training and Awareness
- Vol. 15, Ch.3, § 390 Identification and Authentication

How to Build an Effective IT Security Training and Awareness Program Resource Packet (RP)

MSND/MSNP Help Desk

Password Policy Resource Packet (RP)

Authentication Credential Policy Agreement

By signing this agreement, I acknowledge that I have read and agree to abide by the Authentication Credential Policy.

References

Authentication Credential Policy

_____ _____

Signature Date