



**Northern District of Mississippi  
(MSN)**

**Password Policy**

**October 2015**

---

Prepared for the  
Northern District of Mississippi  
911 Jackson Ave.  
Oxford, MS 38655

---

## **Introduction**

A password is essentially a key that "opens the door" to information systems and the data stored within them. Password management is a practical approach to protecting judiciary information and its associated 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 *Northern District of Mississippi's (MSN)* has created this Password Policy to ensure all users and information systems within its purview manage passwords consistently across their life cycle.

### **1. Purpose**

The purpose of this Password Policy is to ensure that *MSN's* information systems and data are protected against unauthorized access and misuse and that all users of *MSN* resources are aware of their obligations to create, protect, and securely manage passwords across their life cycle.

### **2. Scope**

This Policy applies to all IT resources owned, leased, or operated on behalf of *MSN* that require passwords for authentication. All *MSN* personnel, contractor personnel, interns, visitors, and other non-government employees are obligated to comply with this policy.

### **3. Policy**

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

#### **3.1 General Password Use**

The following general standards apply to all *MSN's* local court information systems:

- Default passwords are changed, or services are disabled, on all information systems before operational deployment.
- Administrative accounts are assigned to individuals and not groups, who are responsible for maintaining, operating, and securing systems.
- All devices (e.g., desktops, laptops, smart phones, flash drives, servers, network equipment) that access, store, transmit, or process sensitive judiciary information are password-protected. Where supported, *MSN* systems automatically require passwords to be changed every six months.
- All remote access solutions require passwords before granting access to sensitive information on the Data Communications Network (DCN) and the local *MSN* networks.

- The number of attempts that a user is allowed to enter an incorrect password is ten times for low/moderate risk systems<sup>1</sup> and six times for high risks systems before the account is automatically disabled for 30 minutes if the system supports this function
- Workstation sessions are locked after 30 minutes of inactivity and retained until the user re-authenticates to the session.<sup>2</sup>
- Password history is set to four (4) used passwords per user. Minimum password aging is set to seven days to prevent users from immediately changing their passwords.
- All information systems, with the technical capability, enforce the local password policy to ensure compliance.
- Password recovery and reset procedures are established to support users who 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.
- Passwords transmitted over internal and external networks are encrypted or transmitted in a hashed format.
- Passwords are not hardcoded during application development and are encrypted when stored.
- Web applications implement safeguards, such as RADIUS<sup>3</sup> with LDAP<sup>4</sup> security to help ensure only authorized users access *MSN* networks and only the resources for which they are allowed.

### 3.2 System Administrator Accounts

System administrators have privileged access to information systems where they have the ability to change operational and security settings. Therefore, it is critical that their accounts meet more stringent security standards than those of the typical end user. All administrative accounts meet the following standards:

- Activities performed by an administrator are attributable only to that individual administrator.
- The minimum password length for administratively controlled devices (e.g., network devices, servers) is twelve 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.

### 3.3 Application Developer Accounts

---

<sup>1</sup> For information on categorizing the risk level of information systems, see the [Guide to Implementing the Judiciary Information Security Framework](#), section 2.1 How to Categorize Information System Risk.

<sup>2</sup> [AC-11: Session Lock](#)

<sup>3</sup> RADIUS, Remote Authentication Dial In User Service, a network protocol for computers that connect remotely to networks, and provides centralized Authentication, Authorization, and Account management.

<sup>4</sup> LDAP, Lightweight Directory Access Protocol, an application protocol for the access and maintenance of directory services via the Web.



Application developers, similar to system administrators, have to abide by more rigorous password management standards than those of a typical end user, since they have the ability to manipulate application code. All application developer accounts meet the following standards:

- Application developer passwords are a minimum of twelve characters, which contain numbers, special symbols, and upper and lowercase letters.
- Accounts support authentication of individuals not groups, so that the developer's actions are attributed to a specific individual.

### **3.4 End User Accounts**

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:

- End users are immediately forced to change passwords issued by the system administrator during the user's first login session, where systems allow.
- 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, and etc.
  - Not sharing their username and passwords with anyone (e.g., supervisors, co-workers, family, Help-Desk personnel). 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 Help-Desk staff will reset users' passwords immediately after providing assistance, to force users to change their passwords upon re-login.

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

### **3.5 IT Security Training and Awareness**

It is important to properly train users of their obligations to securely manage their passwords. Password training and awareness are integrated into the content of *MSN'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 *MSN'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 passwords.

- Ensuring users understand special precautions that may be needed when working from home or on a public terminal.

### **3.6 Password Compromise**

Consistent with *MSN's* local incident reporting procedures, the following actions are taken when a password compromise is suspected:

- Notify IT staff.
- User or system passwords are immediately disabled to avoid the possibility of unauthorized activity being attributed to an authorized user.
- *MSN's* IT 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 to prevent the attacker from compromising new passwords 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.

## **4. Policy Review**

*MSN's* IT Security Officer reviews this Policy annually to ensure the policy statements set forth remain effective and adhere to industry best practices and/or standards. Performance of this review is documented in a memorandum to the Chief Deputy of Administrative Services.

## **5. Exceptions**

Exceptions to this policy are formally granted, documented, and periodically reviewed for on-going legitimacy in accordance with *MSN's* IT security policy exception procedures.<sup>5</sup>

---

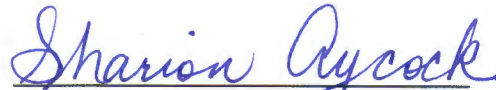
<sup>5</sup> *MSN's* IT security policy exception procedures were developed in accordance with the [Guide to Judiciary Policy, Vol. 15, Ch. 3, Section 380: Security Policy Exceptions](#)

## 6. Policy Authorization

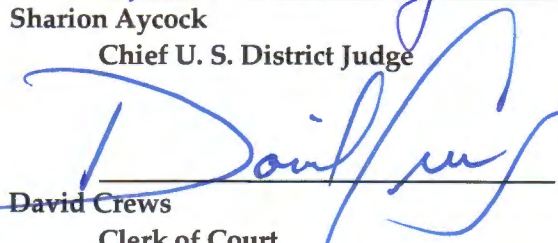
This policy was reviewed and approved by the CUEs, Chief Judge, and all Judges from the *Northern District of Mississippi* on October 30, 2015.

### Effective Date:

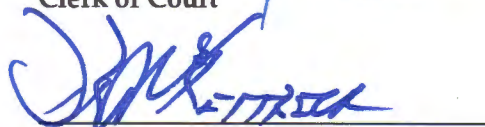
This *Policy* is effective beginning on the 6<sup>th</sup> day of November, 2015.



Sharion Aycock  
Chief U. S. District Judge



David Crews  
Clerk of Court



Danny McKittrick  
Chief U. S. Probation Officer

## Appendix A: Tips on Creating “Hard to Guess” but “Easy to Remember” Passwords

It is important for users to learn to create *hard to guess* but *easy to remember* passwords. A few options are listed below.

### OPTION 1

**Step 1:** Use a two or three word phrase.

- the bull
- my dog sam

**Step 2:** Use character substitution by replacing certain letters with numbers. This should be easy to remember because the shape of the numbers is similar to the shape of the letters.

- O = 0 (zero)
- L = 1
- S = 5
- A = 4
- E = 3

Using the above examples, the passwords would become.

- the bull = **th3 bu11**
- my dog sam = **my d0g 54m**

**Step 3:** Replace all spaces with special symbols (e.g., ! @ # \$). In the examples, spaces will be replaced with \$.

- **th3\$bu11**
- **my\$d0g\$54m**

**Step 4:** Add uppercase characters at the beginning, middle or end of the phrase.

- **Th3\$bu11** or **th3\$Bu11**
- **my\$d0g\$54M** or **my\$d0G\$54m**

The passwords may look strange (that's the *hard to guess* part), but the phrase is familiar and converted with a simple substitution method (that's the *easy to remember* part).

### OPTION 2

Use the same familiar phrase method as in Option 1, but use numbers in place of any words that sound like numbers.

- one = 1
- to = 2
- for = 4

Substitute single letters for words that sounded like a single letter and drop all spaces.

- be, bee = **b**



- gee = g
- tee = t

The password phrase, To be or not to be, becomes: **2b0rn0t2b**

### OPTION 3

Use the phrase method to create a core password, **th3\$Bu11**. Use that core to create multiple passwords by adding uppercase characters to identify the system being accessed.

- **th3\$Bu11LN** for Lotus Notes
- **th3\$Bu11HR** for Human Resources
- **th3\$Bu11T** for Testing
- **th3\$Bu11F** for Finance



## **Password Policy Agreement**

By signing this agreement, I acknowledge that I have read and agree to abide by the Password Policy for the Northern District of Mississippi.

---

Signature

---

Date