


**JUDICIARY OF GUAM
POLICY AND PROCEDURES
ADMINISTRATIVE POLICY NO. UJ20-03**

 Judiciary of Guam	Division: ADMINISTRATIVE OFFICE OF THE COURTS
TITLE: PASSWORD MANAGEMENT POLICY	EFFECTIVE DATE: <i>5/6/2020</i>
REVISED DATE:	APPROVED BY: <i>Kristina L. Baird</i> Kristina L. Baird, Administrator of the Courts

A. PURPOSE

The Judiciary of Guam (“Judiciary”) establishes this Password Management Policy to set standards for the creation, protection and rotation of passwords used to access technology-related hardware, software, databases, case management systems, and Enterprise resource systems owned or supported by the Judiciary and third party vendors. Any questions regarding this policy should be addressed to the Management Information Services (MIS) Administrator. Any exceptions to this policy must be reviewed and approved by the Administrator of the Courts on a case-by-case basis.

B. APPLICATION

The Judiciary has a responsibility to reasonably ensure that proprietary data, confidential data, and licensed applications are accessed and used appropriately. It is the MIS Administrator’s or his/her designee’s responsibility to manage the authentication process and the duty of Judiciary employees and other authorized persons, and third-party vendors to reasonably ensure the confidentiality of their unique user authentication.

C. DEFINITIONS

1. **Computer Systems and Equipment.** All technology-related hardware, software, databases, case management systems, and Enterprise resource systems owned or supported by the Judiciary such as desktop computers, laptop computers, tablets, monitors, printers, scanners, servers, copiers, video conference units, telephones, mobile devices, flash drives, storage devices and any other technology-related devices.
2. **Password.** A secret word, phrase or string of characters used to gain full or partial access to the Judiciary’s Computer Systems and/or Equipment.
3. **Users.** Judiciary employees and other authorized persons using the Judiciary’s Computer Systems and Equipment. Other authorized persons include non-Judiciary employees with a

guamcourts.org user account, or other persons pre-approved to access the Judiciary's Computer Systems and Equipment.

D. POLICY GUIDELINES AND GENERAL RESPONSIBILITIES

1. Passwords are not to be issued or generated without appropriate authorization and approval to access Judiciary Computer Systems and Equipment.
2. Users must be assigned initial passwords, which are unique to each individual user. Following initial login, the user is required to change the password to a strong password only known to the user.
3. To prevent password guessing attacks, the number of consecutive attempts to access the system or an application using an incorrect password will be limited by the system.
4. User passwords will not be reset or changed unless the user is able to uniquely identify him- or herself (via phone or in person). If the user is unable to uniquely identify him- or herself, the MIS Administrator or his/her designee, or the user's Division Manager must approve a password reset.
5. Best practices provide that user IDs associated with a password must be automatically disabled or locked after a specified period of account inactivity.
6. Best practices provide that system design must prohibit or obfuscate the password display during entry of clear text passwords.

E. USER RESPONSIBILITY

1. Intentionally sharing user passwords is a violation of Judiciary security policies and is subject to disciplinary action, up to and including dismissal.
2. All users will be required to change passwords at least once every one hundred eighty (180) days or sooner if the specific application dictates. If users do not change their password within one hundred eighty (180) days, they may be denied access to Judiciary Computer Systems and Equipment, and a password reset will be required.
3. Writing down passwords is prohibited.
4. Passwords must always be encrypted when stored or transmitted over networks including the Internet.

F. PASSWORD REQUIREMENTS

1. Passwords cannot be personally identifiable (i.e., birth date, spouse's name, child's name, etc.) and will be at least eight characters consisting of alpha numeric characters including upper and lower case alpha characters, at least one number, and one special character.
2. Upon a password being changed, that same password cannot be reused for five (5) iterations (i.e., the user cannot use the same password that has been used within the last five (5) password changes).

3. Users are prohibited from self-assigning a fixed password by combining a set of characters that do not change, with a set of characters that predictably change (i.e., characters which change are typically based on a month, a department, a project, or some other easily guessed factor; e.g., passwords such as "X34JAN" in January, "X34FEB" in February, etc.).
4. A password must not be the same as the user ID with which it is associated.

G. OTHER

1. Passwords may be reset or disclosed to an appropriate party authorized by the Judiciary needing emergency access to Judiciary Computer Systems and Equipment where the user is unavailable to log on. Following the conclusion of the emergency, the account will be disabled until the user is available to reset his/her password.
2. All vendor-supplied default passwords will be changed before any computer or communications system is activated.
3. On all multi-user Judiciary Computer Systems and Equipment, system software or locally developed software will be used to maintain an encrypted history of log on requests.
4. Whenever Judiciary Computer Systems or Equipment has been compromised, the MIS Administrator or his/her designee must require users to immediately change all of the users' passwords associated with the compromised Judiciary Computer Systems or Equipment. If the users are not available to change their passwords, access will be disabled until such time as the passwords can be changed.
5. Unless approved by the MIS Administrator, the use of shared passwords associated with a generic user ID to access files, databases, computers and other system resources is prohibited.
6. For assistance, please contact:

MIS Division
Judiciary of Guam
671-472-9710 (office phone)
671-787-9101 (cell phone)
jmannion@guamcourts.org (email address)

H. VIOLATIONS

Any Judiciary employee or other authorized person found to have violated this policy may be subject to disciplinary action, up to and including termination.

I. REFERENCES

1. Administrative Policy No. UJ20-02 - Interim Laptop and Mobile Device Policy

