SUPREME COURT OF APPEALS OF WEST VIRGINIA

User Password Policy
Technology Services Division

1. Introduction.

1.1 Overview. The Court establishes this policy to explain the standards for creation, protection and rotation of passwords. Breaches of this policy may result in disciplinary or other corrective action. Any questions regarding this policy should be addressed to the Director of the Division of Technology Services. Any exceptions to this policy shall be reviewed on a case-by-case basis.

1.2 Terms. This policy uses the following defined terms:

(a) *Alphanumeric*. A set of characters that includes letters, numbers and special characters such as punctuation marks.

(b) *Court's Computer Systems and Equipment*. All technology-related hardware, software, databases and case management systems owned or supported by the Court 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.

(c) *Credentials.* Unique Court-provided account username and password assigned to each user by the Division of Technology Services to enable access to the Court's computer systems and equipment.

(d) *Password*. A secret word, phrase or string of characters used to gain full or partial access to the Court's computer systems and equipment.

(e) *Service Desk*. Communication center providing a single point of contact for resolution of technology issues, managed by the Division of Technology Services. Users can contact the Service Desk by email at ServiceDesk@courtswv.gov.

(f) *Users*. Court employees and other authorized persons using the Court's computer systems and equipment. Other authorized persons include non-Court employees with a courtswv.gov user account, or other persons pre-approved to access the Court's computer systems and equipment.

(g) *Workstations*. All technology-related hardware having operating systems that are supported by the Court such as desktop computers, laptop computers, tablets, mobile devices, and any other technology-related devices.

Effective Date:	2019 03-11
Revision Date:	2019 03-11
Review Date:	2019 03-11

2. Password Maintenance.

2.1 First Login. Each user is responsible for changing the assigned password upon first login or when requesting a password reset.

2.2 Password Creation.

(a) The password must be at least twelve (12) alphanumeric characters.

(b) The password must contain at least one of each of the following:

- uppercase character (ex: ABC)
- lowercase character (ex: abc)
- number (ex: 123)
- special character (ex: ! @ # $ % ? & *)

(c) Users should set passwords that are not common words, familiar dates or names.

2.3 Password Rotation.

(a) Users must change their password at least every one-hundred twenty (120) days. Users must change passwords on secondary devices such as laptops, tablets, and other mobile devices at the same time to avoid being locked out.

(b) Each password cannot be identical to any of the previous twelve (12) passwords.

2.4 Password Protection. Users are required to maintain a high standard of care regarding password management including, but not limited to, the following:

(a) Do not share accounts or passwords with any other person. Safeguard your password so that it cannot be easily discovered.

(b) Manually lock workstations when unattended (Windows Key + L key).

(c) Notify the Service Desk immediately if credentials are compromised.

3. Additional Access Controls.

3.1 The Division of Technology Services reserves the right to enhance credential security through the use of tools such as encryption, tokens and biometrics, as necessary.