1. Introduction.

1.1. Overview. The Court establishes this policy to explain the standards for account credentials. 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. Authority. The Court establishes this Policy pursuant to its inherent powers and administrative authority, as set forth in Article 8, Section 3 of the Constitution of the State of West Virginia.

1.3. Terms. This policy uses the following defined terms:

a) **"Court's Computer Systems and Equipment"** is 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.

b) **"Credentials"** means the 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.

c) **"Multifactor Authentication ("MFA")"** is the layer of protection added to the sign-in process that requires Users to provide two authentication methods that authenticate:

- something you know, such as a password, or a pin number,
- something you have, such as a hardware token, a certificate, or a code from an authenticator application,
- and/or something you are, such as biometrics (fingerprint or facial recognition scan).

d) **"Password"** is 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"** is the 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"** means all Court employees and other authorized persons using the Court's computer systems and equipment. Other authorized persons include judicial officers, 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"** are 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.

2. Account Credentials Maintenance.

2.1. Account Username. Each user shall be issued a unique username derived from his/her legal first name and legal last name. A middle initial shall be appended to the legal first name when any conflict occurs due to an existing username. Nicknames and preferred names may be considered on a case-by-case basis. Such requests must be submitted in writing to the Director of the Division of Technology Services for review.

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

2.3. Password Creation.

a) The password must be at least sixteen (16) 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.

2.4. Password Rotation.

a) Users must change their password at least every one-hundred twenty (120) days.

b) Users must change passwords on secondary devices such as laptops, tablets, and other mobile devices at the same time to avoid being *locked out.*

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

3. **Session Timeout.** Tampering with session timeouts on any of the Court's Computer Systems and Equipment is strictly prohibited.

4. **Additional Access Controls.** 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.

4.1. Password Rotation When MFA is Required.

a) Users are not required to rotate their passwords when MFA is required.

The details of this policy and all Court policies are subject to modification by the Court at any time as situations, standards, and legal requirements may change. The Court will ensure that all employees are notified of any such modification in a timely fashion.