1. Introduction.

1.1 Overview. The Court establishes this policy to explain the acceptable use of the Court's computer systems and equipment by any authorized users. Use of these systems and equipment is a privilege, and individuals who are granted this privilege must use these systems and equipment in an appropriate, ethical and lawful manner. Unauthorized access is prohibited and all activity, authorized or not, may be monitored and reported to the appropriate director or proper authorities. 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.

1.2 Terms. This policy uses the following defined terms:

(a) *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.

(b) *Personal Equipment*. Any technology-related equipment or devices owned by a user and not the Court.

(c) *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.

(d) *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.

2. Acceptable Use.

2.1 Court Business. The Court's computer systems and equipment are to be used for Court business. Users must comply with the directives of the Court including the Code of Judicial Conduct and any Court policies, standards, procedures, contracts and licenses. Users shall comply with all applicable federal, state and local laws and regulations.

2.2 Personal Use.

(a) Except as stated otherwise by this policy, incidental personal use of the Court's computer systems and equipment is permitted if the use does not consume more than a trivial amount of resources that could otherwise be used for Court business, does not

interfere with the productivity of other users, does not interfere with Court business activities and does not cause distress, moral or legal problems for other users.

(b) Court email is to be used for Court business exclusively.

(c) Storing personal data and information unrelated to Court business — such as documents, photos, music or video — on the Court's computer systems and equipment is prohibited.

(d) Loading personal software on to the Court's computer systems and equipment is prohibited without prior authorization by the Division of Technology Services; unapproved software may be removed without prior notice to the user.

(e) Personal equipment may not connect to the Court's network without prior authorization by the Division of Technology Services. Users may use personal equipment to access web-based Court applications while not connected to the Court's network. Any user who conducts Court business on personal equipment assumes sole responsibility for the security and confidentiality of Court information.

2.3 No Expectation of Privacy. Users have no expectations of privacy when using the Court's computer systems and equipment. Any data or messages created on, stored within or transmitted by the Court's computer systems and equipment is the property of the Court and is subject to access, audit, review, deletion or disclosure by authorized Court personnel. The Court may monitor use of its computer systems and equipment at any time, including email, Internet use and any electronically stored information. Users must cooperate with any search or inspection by the Division of Technology Services.

2.4 User Access. Access to the Court's computer systems and equipment is granted by the Division of Technology Services according to each user's job duties and responsibilities.

3. Unacceptable Use.

3.1 General. Users are strictly prohibited from illegal, unauthorized, inappropriate or disruptive use of the Court's computer systems and equipment.

3.2 Examples. Some examples of unacceptable use are listed below. This is not an exclusive list.

(a) Disruptive or improper use as determined by the Division of Technology Services that could cause congestion, disruption of normal service or unnecessary additional Court expense.

(b) Unauthorized disclosure of confidential or personal information.

(c) Any use not related to official Supreme Court duties that could cast the Court or its employees in a negative light, such as the transmission, retrieval, storage or display of defamatory, obscene, sexist, sexually explicit, racist, violent, offensive, slanderous, harassing or illegal content.

(d) Hacking or attempting unauthorized entry into any other electronic resource in violation of the Federal Electronic Communications Privacy Act or any other applicable federal, state or local law.

(e) Falsely representing yourself or another person, real or fictional, to acquire system or resource access, or for any other reason.

(f) Using access for personal financial gain or to solicit others for activities unrelated to official Court business, including, but not limited to, solicitations for personal, political, or religious causes, or to operate or support a personal business.

(g) Tampering with, circumventing or disabling security mechanisms or access control measures for the Court's computer systems and equipment.

(h) Installing any software on the Court's computer systems and equipment without prior authorization of the Division of Technology Services.

(i) Altering, relocating or removing any hardware or software without prior authorization of the Division of Technology Services.

(j) Intentionally destroying, damaging, disrupting or impairing any of the Court's computer systems and equipment.

(k) Violating this policy or any other policy of the Division of Technology Services.

4. Security and Confidentiality.

4.1 Security. Users are expected to observe basic security measures and must adhere to the following:

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

(b) When you step away from your computer, secure it by locking the user account (Windows + L key) or logging out.

(c) Users assigned mobile devices such as phones, laptops and tablets must take adequate precautions to ensure the security of such devices, especially when traveling. Laptops distributed since September 2018 are configured with encryption that will protect against unauthorized access to systems.

(d) All equipment should be kept in a secure environment.

(e) Any unauthorized changes to data should be reported immediately to your supervisor and to the Service Desk. This includes any loss of data or programs, whether electronic or paper.

(f) Notify the Service Desk immediately if a virus or other infection is suspected on the Court's computer systems and equipment.

4.2 Confidential Information. Confidential information — such as Social Security numbers, dates of birth, addresses and phone numbers — is stored on the Court's computer systems and equipment. Some information regarding parties who appear in court (such as minors) is also confidential. Access to confidential information is restricted according to need. Users are expected to safeguard confidential information by complying with the following measures:

(a) All Court business must be conducted through the Court's email and not through third-party email providers such as Google, Yahoo, etc.

(b) Accounts must be protected from unauthorized access by ensuring accounts are not shared or left active and unattended.

(c) Display screens for computers used to handle confidential information must be positioned so that individuals who are not authorized to access confidential information cannot view it easily.

(d) Passwords, encryption keys and other security-related information must be entered in such a way that others cannot readily see what is being typed.

5. Proprietary Material.

(a) For purposes of this policy, proprietary material includes literature, software and graphics protected by copyright, trademark, patent or trade secret laws. The Court enters into legal agreements called licenses to use such proprietary material, usually for a fee. These licenses related to the Court's computer systems and equipment are managed by the Division of Technology Services.

(b) All use of proprietary material must comply with the terms of the relevant license. Users may be permitted access to or use of proprietary material such as software but are not permitted to download or disseminate it for non-Court use. No proprietary information shall be copied, transmitted, posted or distributed in violation of the Court's licenses. Users should not remove trademark or copyright notices from proprietary material.

(c) When a user is no longer employed by or affiliated with the Court, all Court-owned hardware, licenses, software and media remain the property of the Court.

6. Equipment and Data Management.

6.1 Supreme Court Guest Network. Where available, certain individuals such as vendors or representatives of other state entities, may be provided with access to the Supreme Court Guest Network, if approved by the Division of Technology Services.

6.2 Internet Access Control. The Court may, at its discretion, restrict or block access to certain Internet sites and restrict or block the downloading of certain file types that are likely to cause network service degradation such as streaming video. Court employees are permitted to view work-related webcasts.

6.3 Relocation/Removal of Equipment. Users may not remove the Court's computer systems and equipment from Court facilities without prior authorization by the Division of Technology Services. Users are permitted to remove mobile devices such as phones, laptops and tablets, except that no such device may leave the continental United States without prior authorization by the Division of Technology Services.

6.4 Storing and Archiving Data. The Court maintains archival procedures to ensure the safe retention of electronic data. Archived copies of electronic files and messages are and remain Court property and may be used by the Court for any business purpose. The deletion of messages or data does not provide privacy with regard to such messages or data. Archived data may be maintained indefinitely.

6.5 Data Encryption. Only authorized encryption tools (both software and hardware) may be used in connection the Court's computer systems and equipment.