APPENDIX 1

Judicial Branch Information Technology Standard
Acceptable Use of Information Technology Resources Policy

1.0 Purpose and Benefits

Appropriate organizational use of information and information technology (IT) resources and effective security of those resources require the participation and support of the organization's workforce (users). Inappropriate use exposes the organization to potential risks, including virus attacks, compromise of network systems and services, and legal issues.

2.0 Authority

Neb. Ct. R. § 1-1201 et seq. requires compliance with this Appendix.

3.0 Scope

This policy applies to users of the Judicial Branch's (Branch) information or physical infrastructure regardless of its form or format, created or used to support the Judicial Branch for the State of Nebraska. It is the user's responsibility to read and understand this policy and to conduct activities in accordance with its terms. In addition, users must read and understand the organization's Information Security Policy and its associated standards.

4.0 Information Statement

Except for any privilege or confidentiality recognized by law, individuals have no legitimate expectation of privacy during any use of the Branch IT resources or in any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed, or captured in any manner, including in real time, and used or disclosed in any manner by authorized personnel without additional prior notice to individuals. Periodic monitoring will be conducted of systems used, including but not limited to: all computer files; and all forms of electronic communication (including email, text messaging, instant messaging, telephones, computer systems and other electronic records). In addition to the notice provided in this policy, users may also be notified with a warning banner text at system entry points where users initially sign on about being monitored and may be reminded that unauthorized use of the organization's IT resources is not permissible.

The Branch may impose restrictions, at the discretion of the Supreme Court, on the use of a particular IT resource. For example, the Branch may block access to certain websites or services not serving legitimate business purposes or may restrict user ability to attach devices to the Branch's IT resources (e.g., personal USB drives, phones, etc.).

Users accessing the organization's applications and IT resources through personal devices must only do so with prior approval or authorization from the Branch.

4.1 Acceptable Use

All uses of information and information technology resources must comply with Branch policies, standards, procedures, and guidelines, as well as any applicable license agreements and laws, including federal, state, local, and intellectual property laws.

Consistent with the foregoing, the acceptable use of information and IT resources encompasses the following duties:

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information;
- Protecting Branch information and resources from unauthorized use or disclosure;
- Protecting personal, private, sensitive, or confidential information from unauthorized use, disclosure, or destruction;
- Observing authorized levels of access and utilizing only approved IT technology devices or services; and
- Immediately reporting suspected information security incidents or weaknesses to the appropriate manager and the Information Security Officer (ISO)/designated security representative. In certain instances, security incidents may need to be reported to local law enforcement. For example, if a laptop is stolen, the Branch user may be asked to file a police report.

4.2 Unacceptable Use

The following list is not intended to be exhaustive, but is an attempt to provide a framework for activities that constitute unacceptable use. Users, however, may be exempted from one or more of these restrictions during their authorized job

responsibilities, after approval from division or Branch management, in consultation with organization IT staff (e.g., storage of objectionable material in the context of a disciplinary matter).

Unacceptable use includes, but is not limited to, the following:

- Unauthorized use or disclosure of personal, private, sensitive, and/or confidential information;
- Unauthorized use or disclosure of Branch information and resources;
- Distributing, transmitting, posting, or storing any electronic communications, material, or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate, except when the material is part of court proceedings;
- Attempting to represent the Branch in matters unrelated to official authorized job duties or responsibilities;
- Connecting Information Technology systems or devices not specifically purchased or authorized by the Branch's Chief Information Officer (CIO) to the Branch's local or remote network or any IT resource. This includes, but is not limited to, software applications, software as a service, all external media (i.e., thumb drives, external hard drives, cameras), and all hardware such as PCs, laptops, mobile computing devices, phones, scanners, printers, and "smart devices";
- Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with organizational policies. Use of pirated or illegally obtained software on any Branch information system is strictly prohibited.
- Connecting to commercial email systems (e.g., Gmail, Hotmail, Yahoo) without prior management approval (organizations must recognize the inherent risk in using commercial email services as email is often used to distribute malware);
- Using an organization's IT resources to circulate unauthorized solicitations or advertisements for non-Branch purposes, including religious, political, or not-for-profit entities;

- Providing unauthorized third parties, including family and friends, access to the Branch's IT information, resources, or facilities;

- Using Branch IT information or resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);

- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using Branch IT resources;

- Disabling, uninstalling, or otherwise circumventing Branch or third-party IT security controls;

- Disabling or uninstalling security software, settings, or configurations on Branch owned equipment; and

- Peer-to-Peer (P2P) software/service connections (where a computer or server acts as a sharing device for users outside the Branch's network) are strictly prohibited.

4.3 Occasional and Incidental Personal Use

Occasional, incidental, and necessary personal use of IT resources is permitted, provided such use: is otherwise consistent with this policy; is limited in amount and duration; and does not impede the ability of the individual or other users to fulfill the organization's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization. Exercising good judgment regarding occasional and incidental personal use is important. The Branch may revoke or limit this privilege at any time.

4.4 Individual Accountability

Individual accountability is required when accessing all IT resources and Branch information. Everyone is responsible for protecting against unauthorized activities performed under their user ID. This includes locking your computer screen when you walk away from your system and protecting your credentials (e.g., passwords, tokens, or similar technology) from unauthorized disclosure. Credentials must be treated as confidential information and must not be disclosed or shared.

To the extent possible, computer monitors will be positioned to eliminate viewing by unauthorized personnel. When computer monitors cannot be positioned to

eliminate viewing by unauthorized personnel, a privacy screen, which allows viewing only from direct line of site, should be used.

Branch users shall ensure any IT related work or maintenance performed on any computing device, system, or network is completed by authorized Branch IT personnel. Express approval from an authorized Branch IT employee is required prior to removing any stationary computing components and should not be removed without the express approval of the CIO. Branch users are expected to notify their immediate supervisor of anyone not complying with this procedure.

4.5 Restrictions on Off-Site Transmission and Storage of Information

Users must not transmit restricted organization, nonpublic, personal, private, sensitive, or confidential information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct Branch business unless explicitly authorized. Users must not store restricted organizational, nonpublic, personal, private, sensitive, or confidential information on a nonorganizational issued device or with a third-party file storage service that has not been approved for such storage by the organization.

Devices that contain organizational information must be attended at all times or physically secured and must not be checked in transportation carrier luggage systems.

4.6 User Responsibility for IT Equipment

Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to the Branch and must be immediately returned upon request or at the time an employee is separated from the organization. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the organization. Should IT equipment be lost, stolen, or destroyed, users are required to provide a written report of the circumstances surrounding the incident. Users may be subject to disciplinary action that may include repayment of the replacement value of the equipment. The Branch has the discretion to not issue or re-issue IT devices and equipment to users who repeatedly lose or damage IT equipment.

4.7 User Responsibility for Electronic Communication

A. Judicial Branch email shall be used for authorized Branch purposes. Branch users must exercise common sense, good judgment, and propriety in using the Branch's electronic communication technologies.

B. All Branch users shall use only a Judicial Branch issued email address and account when conducting Branch business. Use of personal email accounts, accounts of other governmental subdivisions, or email addresses appearing to be for judicial branch purposes using a nonbranch issued email account are strictly prohibited by the Nebraska Supreme Court.

C. Branch users should not expect privacy or confidentiality when using a Branch issued email account and/or Branch email system(s). For technical issues, investigative purposes, or public records requests, Branch email accounts or system(s) may be subject to review without notice. Such technical issues or investigations include, but are not limited to, email or email account restoration, troubleshooting email client issues (i.e., Microsoft Outlook), IT security investigations, Human Resource investigations, and/or law enforcement investigations. Such reviews will be handled in accordance with appropriate policies and laws. In addition, email may be subject to disclosure as part of a public records request under Neb. Rev. Stat. § 84-712 et seq.

D. Electronic mail messaging shall be used in accordance with the following guidelines:

1. Auto-forwarding of email messages to addresses outside the Branch network is strictly prohibited.

2. When emails contain sensitive Branch data, emails must be appropriately encrypted using Microsoft Outlook encryption methods.

3. Misrepresenting, obscuring, or suppressing a user's identity in the "From:" line of an email message or information system is prohibited. The username, email address, organizational affiliation, and related information included with an email message or posting must reflect the actual originator of the message or posting. This does not include deleting information within the body of an email when replying or forwarding information.

4. To ensure the integrity of the Branch's email communication system, employees shall not intercept or assist in intercepting email communication unless authorized to do so by the Branch CIO.

5. Message Content – All messages shall be conducted in a professional manner and the messaging shall not:

a. contain profanity, obscenities, or derogatory remarks;
b. contain obscene, pornographic, or sexually suggestive materials;
c. be used to discriminate against any person or group on the basis of race, national origin, gender, age, sexual orientation, religion, socioeconomic status, or disability, or as discrimination is defined in other statutes and rules governing Branch users;
d. be used to harass and/or threaten others;
e. be used to intimidate others or to interfere with a person's ability to perform his or her job duties;
f. involve the creation and exchange of advertisements, solicitations, chain letters, or other unsolicited email;
g. involve the creation and exchange of information in violation of any copyright laws; or
h. be used to promote personal, political, and/or self-interests.

The restrictions above do not prohibit Branch users from alerting supervisors or Branch IT of emails containing prohibited content under the above sections.

E. Care should be taken interacting with email. Branch users should carefully examine emails before clicking on links, opening attachments, or responding. If the email message looks suspicious, the Branch user should not interact with the message and report it as Phishing in Outlook. The message will be moved to the user's deleted items. If the Branch user continues to receive suspicious email from the sender, the local IT Support Technician should be contacted to provide necessary information to the Branch's ISO.

F. It is necessary for authorized Branch IT staff to use software to monitor the activity of user IDs. It may also be necessary for technical support personnel to review the content of an individual employee's communications during problem resolution, or to ensure the ongoing availability and reliability of the email system(s). Under no circumstances, however, may technical support personnel review the content of an individual employee's communications except to enforce provisions of this policy.

G. Branch IT security personnel is distinct from technical support personnel and has been authorized by the Nebraska Supreme Court to review the content of Branch user's communications as necessary and appropriate for purposes of preventing cyber security threats and incidents.

4.8 Use of Social Media

The use of public social media sites to promote Branch activities requires written preapproval from the Administrative Office of the Courts and Probation (AOCP).

Approval is at the discretion of the AOCP and may be granted upon demonstration of a business need, and a review and approval of service agreement terms by Branch's Counsel's Office. Final approval by the AOCP should define the scope of the approved activity, including, but not limited to, identifying approved users.

Unless specifically authorized, the use of Branch email addresses on public social media sites is prohibited. In instances where users access social media sites on their own time utilizing personal resources, they must remain sensitive to expectations that they will conduct themselves in a responsible, professional, and secure manner with regard to references to the Branch and staff. These expectations are outlined below.

A. Use of Social Media Within the Scope of Official Duties

The AOCP, or designee, must review and approve the content of any posting of public information, such as blog comments, tweets, video files, or streams, to social media sites on behalf of the Branch. However, AOCP approval is not required for postings to public forums for technical support, if participation in such forums is within the scope of the user's official duties, has been previously approved by his or her supervisor, and does not include the posting of any sensitive information, including specifics of the IT infrastructure. In addition, AOCP approval is not required for postings to private, Branch-approved social media collaboration sites (e.g., Microsoft SharePoint external sites). Blanket approvals may be granted, as appropriate.

Accounts used to manage the organization's social media presence are privileged accounts and must be treated as such. These accounts are for official use only and must not be used for personal use. Passwords of privileged accounts must follow information security standards, be unique on each site, and must not be the same as passwords used to access other IT resources.

B. Guidelines for Personal Use of Social Media

Staff should be sensitive to the fact that information posted on social media sites clearly reflects on the individual and may also reflect on the individual's professional life. Consequently, staff should use discretion when posting information on these sites and be conscious of the potential perceptions of and responses to the information. It is important to remember that once information is posted on a social media site, it can be captured and used in ways not originally intended. It is nearly impossible to retract, as it often lives on in copies, archives, backups, and memory cache.

Users should respect the privacy of the Branch's staff and not post any identifying information of any staff without permission (including, but not limited to, names, addresses, photos, videos, email addresses, and phone numbers). Users may be held liable for comments posted on social media sites.

If a personal email, posting, or other electronic message could be construed to be an official communication, a disclaimer is strongly recommended. A disclaimer might be: "The views and opinions expressed are those of the author and do not necessarily reflect those of the Branch."

Users should not use their personal social media accounts for official business, unless specifically authorized by the Branch. Users are strongly discouraged from using the same passwords in their personal use of social media sites as those used on Branch devices and IT resources, to prevent unauthorized access to resources if the password is compromised.

5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time upon approval of the Nebraska Supreme Court.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the Information Security Officer's exception process.

6.0 Acknowledgment

A. Branch users who require or need to establish access to Branch information systems shall read, review, and understand the Information Systems Security Rule and Information Systems Security Policy.

B. Branch users shall as a condition of access to any Branch information system sign an Acknowledgment of the Information Systems and Security Rule and Policy form, found as Appendix 2 to Neb. Ct. R. § 1-1201 et seq.

7.0 Revision History

This policy shall be reviewed at least once every year to ensure relevancy.

Date	Description of Change	Reviewer