NOTICE OF COMMENT PERIOD

The Nebraska Supreme Court is considering a new rule, Neb. Ct. R. § 1-1201, regarding technology and new Appendixes 1 and 2 governing the Judicial Branch's Information Systems, and it seeks public comment on the proposed new rule and appendixes.

The Nebraska Supreme Court invites interested persons to comment on the new rule and appendixes. Anyone desiring to submit a public comment for the Supreme Court's consideration should do so via email to wendy.wussow@nebraska.gov, with the following text listed in the email subject line: **Neb. Ct. R. § 1-1201. Technology**. Comments will be accepted until **9 a.m. on June 26, 2023**.

The full text of the proposal is available below. To obtain a paper copy, please call the Clerk's Office at 402-471-3731.

CHAPTER 1: ADMINSTRATIVE OPERATIONS

. . . .

Article 12: Technology.

§ 1-1201. Information Systems and Security Rule.

(A) The Nebraska Supreme Court, pursuant to the general administrative authority over all courts in the state set forth in Neb. Const. art. V, § 1, and by adoption of this rule, authorizes creation and implementation of an Information Systems and Security Policy ("policy") found as Appendix 1, to protect the Nebraska Judicial Branch ("Judicial Branch") information technology systems from potential threats, vulnerabilities, and data loss. This rule further provides clarification as to applicability of Appendix 1 to users of Judicial Branch information technology systems.

(B) Applicability and Scope:

(1) The rule shall apply to all Judicial Branch users of information technology systems. Judicial Branch users are defined as persons who have access to and utilize any Judicial Branch information technology systems, networks, hardware, and/or software, regardless of title, employment, volunteer position, or contract status. This includes, but is not limited to, judges, judicial branch employees covered by and those who are excepted

from the Nebraska Supreme Court Personnel Policies and Procedures, elected clerks of the district court, county court employees who are Branch users, contract workers, interns, volunteers, and business partners.

(2) All Judicial Branch users shall, to the fullest extent reasonably possible, comply with all requirements of Appendix 1 or face potential disciplinary and/or remedial action as determined by the Nebraska Supreme Court and set forth in section (D).

(C) Acceptable Usage. Appendix 1 shall outline the acceptable use of information technology systems, networks, hardware, and/or software by Branch users. The Nebraska Supreme Court requires all Branch users to sign an acknowledgment that the user has received and read this rule and Appendix 1 as a condition of access to any Branch information system. This Acknowledgment of the Information Systems and Security Rule and Policy is set forth in Appendix 2.

(D) Disciplinary and Remedial Action. Violations of this rule by willful noncompliance with Appendix 1 may result in disciplinary action, loss of access to information technology systems, networks, hardware, and/or software by the violator, or other remedial or corrective action as determined by the Nebraska Supreme Court. Specific disciplinary and remedial authority is set out as follows:

(1) The ultimate disciplinary authority for judges in the State of Nebraska rests in the provisions of Neb. Const. art. III, § 17, and art. V, § 30. Willful noncompliance with Appendix 1 may be cause for disciplinary action as provided by the constitution, Nebraska statutes, and/or Neb. Ct. R. § 5-101 et seq.

(2) Disciplinary authority for judicial branch employees covered by the Nebraska Supreme Court Personnel Policies and Procedures rests in the disciplinary provisions contained therein. Willful noncompliance with Appendix 1 may be cause for disciplinary action as provided by the Personnel Policies and Procedures.

(3) For Judicial Branch employees excepted from the Nebraska Supreme Court Personnel Policies and Procedures, willful noncompliance with Appendix 1 may be cause for remedial or corrective action as determined by the Nebraska Supreme Court.

(4) For elected clerks of the district court and county employees who are Judicial Branch users in the district courts of the state, willful noncompliance with Appendix 1 may be cause for loss of access to information technology systems, networks, hardware, and/or software by the violator.

(5) For contract workers, interns, volunteers, and business partners, willful noncompliance with Appendix 1 may be cause for loss of access to information technology systems, networks, hardware, and/or software by the violator, may be a breach of contract, or may result in early termination of the internship or volunteer opportunity as determined by the Nebraska Supreme Court or the Administrative Office of the Courts and Probation.

(E) Any violation of Appendix 1 that gives rise to potential criminal activity shall be reported to the appropriate authorities.

(F) Administration of Appendixes 1 and 2 shall be by the Nebraska Judicial Branch Chief Information Officer as directed by the Nebraska Supreme Court.

(G) The Nebraska Supreme Court may require Judicial Branch Education for all Judicial Branch users on information systems and security. Specific education shall be provided by Judicial Branch Education as directed by the Nebraska Supreme Court.

Appendix 1

Information Systems and Security Policy

I. Purpose.

The purpose of the Information Systems and Security Policy is to protect the Nebraska Judicial Branch ("Branch") information technology (IT) systems from potential threats, vulnerabilities, and data loss, allow for current and future oversight of IT resources, and provide direction regarding the security, operation, and permissible use of the Branch's network, hardware, and software.

II. Applicability & Scope.

A. The Nebraska Supreme Court has adopted by rule that this Information Systems and Security Policy (policy) shall apply to and govern actions of all Judicial Branch users of IT systems including judges, elected clerks of the district court, bailiffs and court staff employed by counties who utilize Branch Information Technology Systems. To the extent the following persons have access to Branch Information Technology Systems, it shall apply to contract workers, volunteers, business partners, and internship positions. When a position is governed by a contract or agreement and involves use of IT systems, networks, hardware, or software, the parties shall agree to be bound by this Policy as a term of the contract.

B. This policy covers accessing and using the Branch's electronic computing technologies, including but not limited to:

1. The Branch's network, which is any network circuit used to exchange information within the Branch or externally and includes hardware and software necessary to use the network.

2. Hardware--including but not limited to desktop computers, laptops, mobile computing devices, remote and centralized servers, network equipment, and telephone equipment.

3. Software applications--including software developed in-house and/or purchased commercially.

III. Policy.

The security and availability of the Branch's information systems and data--in any media or format--is vital to the success of the Branch's constitutional and statutory duty to provide court and probation services to the State of Nebraska. Therefore, the Supreme

Court shall establish and maintain a comprehensive Branch-wide information systems security policy detailing acceptable use and behavior necessary to protect the Branch's IT infrastructure, personnel, and data assets.

IV. Definitions.

A. "Authorized Branch IT personnel" means Judicial Branch IT personnel, Executive Branch IT personnel, county IT personnel, or IT contractor hired by the Judicial Branch to perform IT work on behalf of the Branch.

B. "Branch users" means persons who have access to and utilize any Branch Information Technology or Systems including all judicial officers, employees of the Judicial Branch, Clerks of the District Court, Bailiffs, county court employees working in the district courts, contract workers, volunteers, business partners, and interns.

C. "Cloud" or "Cloud computing" is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

D. "Computing device(s)" means any laptop, desktop, mobile device, network equipment, and servers hosted on premises or in the Cloud.

E. "Password manager" means a program that stores usernames and passwords for multiple applications in a secure, encrypted format. Individual username and passwords stored within the password manager can be accessed using a single master password.

F. "Sensitive information" includes, but is not limited to, personal identifiable information (PII), criminal justice information (CJI), payment card information (PCI), mental health records, and healthcare records.

G. "Electronic communication technologies" includes email, videoconferencing systems, case management systems of courts and probation, Nebraska.gov portals, and any administrative, court, or probation record keeping system(s)

V. Information Security Requirements.

A. The Branch shall implement security controls, internal technology policies, and guidelines to protect information systems and data from individual and environmental threats.

B. Branch users accessing the Branch network, computing devices, or external storage media must make every effort to protect Branch information systems and devices within their control in their work areas and any equipment used when working remotely.

Equipment must be properly safeguarded and protected to reduce risks from environmental threats and hazards, as well as opportunities for unauthorized access, use, or removal.

C. Electronic communication technologies shall be used for business-related purposes with limited personal use. Any use of the Branch's Case Management System (CMS) must be related to users' performance of their job duties. The CMS includes all Branch information systems designed to capture, monitor, and track court and probation content, including filings, events, calendar events, documents, and financial information in a case; all Nebraska.gov portals; or any other electronic court and probation record-keeping system. Users are strictly prohibited from using the CMS to access information for which they have no business purposes, including information related to court cases or probation records.

D. Except for the CMS, court-authorized service provider portals, or any other electronic court and probation record keeping systems, limited personal use of the Branch's electronic communication technologies is permissible when it does not interfere with network bandwidth, employee productivity, conflict with this policy's goals or any other Branch policy, or preempt any business-related activity, in accordance with the Nebraska Supreme Court Personnel Policies and Procedures.

E. Branch users shall utilize strong, non-offensive passwords and have a professional responsibility to protect system passwords by not sharing passwords with anyone or writing them down. Branch users shall change passwords per prescribed schedule or immediately if a password is discovered to be compromised. Passwords shall always be secured from unauthorized access. It is highly recommended employees use a secure password manager approved by the Branch Information Security Officer. Enabling the "Save Password Option" is strictly prohibited.

F. Branch users are required to lock their computing device when the device is no longer within line of sight. At the end of the workday, Branch users must log off their workstations. The Branch will employ computing device locking controls to protect against unauthorized use of Branch information systems.

G. 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.

H. 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 IT. Branch users are expected to notify their immediate supervisor of anyone not complying with this procedure.

I. Information technology systems or devices not specifically purchased or authorized by the Branch's Chief Information Officer (CIO) are prohibited from being connected to the Branch's local and remote network or any other Branch information system. This includes, but is not limited to, software applications, software as a service, all external media (i.e., zip drives, thumb drives, external hard drives, CD burners), and all hardware such as PCs, laptops, mobile computing devices, scanners, printers, and "smart devices."

J. In situations where there is a business need to connect external media to a computing device or information system, Branch users shall take precautionary measures to ensure the computing device and information system(s) are properly secured. Precautionary measures shall include, at a minimum, ensuring the device that external media will be connecting to has malware protection installed. Business situations that may require connecting unencrypted external media to a computing device or information system may include the following but is not limited to:

1. Large exhibits or evidence on external media for court proceedings;

2. Case review for probation supervision purposes; or

3. Training materials that are required to be distributed using external media.

K. Branch users who have access to or store Branch data shall ensure the data is protected from the risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

L. When Branch sensitive information is no longer needed or exceeds established retention policies or laws, the information and/or hardware storing the sensitive information shall be destroyed by a method rendering it unreadable, undecipherable, and irretrievable.

M. Software Licensing: All software installed on computing devices shall be approved and installed by authorized Branch IT personnel. Personally owned software on any Branch information system must be approved by authorized Branch IT personnel before use. Use of pirated or illegally obtained software on any Branch information system is strictly prohibited. To ensure compliance with software copyright and licensing agreements, IT staff are authorized to conduct computer audits. Authorized Branch IT personnel has the authority to remove or disable any unapproved or pirated software found.

N. All devices that connect to any Branch information system, either on site or from a

remote location, shall be updated with the latest security patches and malware protection as they are distributed. Users shall not disable, uninstall or override any security software, settings, or configurations on Branch owned equipment.

O. Remote access (VPN) to the Branch's network is permitted only with the use of Multi-Factor Authentication and through approved software/services authorized by the Branch's CIO.

P. 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.

Q. A security review shall be performed by IT for any computing device, network, wireless, or server equipment purchased using local funds, and if approved, installed by authorized IT personnel.

R. Wireless network installations or configurations needed to access the Branch's network must be authorized and performed by authorized Branch IT personnel. All wireless devices shall be approved by authorized IT personnel before being connected to the network.

S. Computing devices, regardless of technology or ownership, shall meet Branch security policies, procedures, and configuration standards.

T. Branch users are strictly prohibited from downloading and using any hacking type tools, network scanning software, or password crackers unless specifically approved and authorized by the Branch CIO in writing.

U. All account access will follow the principle of least privilege. The principle of least privilege means granting the minimum access to applications and services which are required to perform a business function.

VI. Security Incidents.

A. A security incident is an activity that results (or may result) in misuse, damage, denial of service, compromise of integrity, or loss of confidentiality of a network, computer, application, or data. Security incidents may also include threats, misrepresentations of identity, or harassment of or by individuals using these resources.

B. All incidents related to information security shall be reported immediately to the Branch user's supervisor, if applicable, and the Branch ISO. Reportable incidents include theft, loss, or compromise of Branch sensitive information or information systems.

1. If a compromise of personal identifiable information (PII) has occurred, an appointed

incident response team will examine the details surrounding the incident ensuring information and systems are not compromised. If the incident is believed to involve criminal activity, the CIO or his/her delegate will contact local law enforcement.

2. The Branch ISO will track and document information system security incidents on an ongoing basis.

C. Personnel will be provided training by authorized Branch IT personnel in their incident response roles.

D. Branch users should be alert to their surroundings and immediately report any suspicious activity or suspected incidents to their immediate supervisor, if applicable, and the ISO.

VII. Unauthorized Access.

Unauthorized access is defined as not having formal written permission or approval for access to Branch systems or data. Unauthorized access to Branch information may also include access by someone who has met all requirements to access the systems and/or data but accesses the systems and/or data for an unauthorized purpose. Users shall not allow unauthorized access to Branch systems or data and shall not use systems or data for unauthorized purposes.

VIII. Electronic Mail.

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 non-branch 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 VIII(d)(5)(A) through (H).

E. Care should be taken in opening any email message if the Branch user is not familiar with the message sender. If the email message looks suspicious, the Branch user should permanently delete the message by pressing "Shift+Delete" and report the message to the Branch ISO. 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.

IX. 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 (Appendix 2).

X. Data Protection & Destruction.

A. Network drive storage is provided for court and probation employees with backup protection and disaster recovery for business purposes. Branch users shall use Branch provided network/cloud storage for all business-related products.

B. All data created and or stored on the Branch's networks, computers, peripherals or otherwise is the property of the Branch.

C. Restricted and confidential data should not be transferred unless encrypted.

D. Data that has exceeded its retention period or that is no longer used or needed should be deleted in a timely manner. Hiring managers must inform Branch IT upon an employee's separation from the Branch on whether local data, emails, and network data can be purged, or must be saved to another location.

XI. Implementing the Policy.

The Supreme Court directs the Chief Information Officer and the Judicial Branch IT Division to implement the provisions of this policy using various security controls including but not limited to malware detection/prevention programs, intrusion detection software, internet blocking programs, encryption practices, firewalls, and methodologies for centrally distributing critical security updates from approved Branch software or hardware providers.

XII. Education.

The Supreme Court directs all branch users to participate in the Branch's information security awareness education which shall consist of one hour of education annually. Judicial Branch Education shall provide this training. For Branch Users who must comply with Neb. Ct. R. § 1-501 et seq. for Mandatory Continuing Judicial Education, security awareness education participation will be reflected in the Branch's learning management system.

Appendix 2

Nebraska Judicial Branch
Acknowledgment of the Information Systems and Security Rule and Policy

Pursuant to Neb. Ct. R. § 1-1201(C) and as directed by the Nebraska Supreme Court, I acknowledge that I have received a copy of and read the Information Systems and Security Rule and the Information Systems and Security Policy. I acknowledge the following:

1. I understand that when I use any Branch information system, I have NO expectation of privacy in any Branch records that I create or in my activities while accessing or using the Branch's information systems.

2. I understand that the Nebraska Supreme Court may direct the State Court Administrator, Probation Administrator, or the Chief Information Officer to review my conduct or actions without notice, concerning Branch information and information systems, and take appropriate action to protect the Branch's information systems from threats, vulnerabilities, and data loss, if warranted.

3. I understand that refusal to sign the Acknowledgment of the Information Systems and Security Rule and Policy may have an adverse impact on my access to Judicial Branch Information Systems as directed by the Nebraska Supreme Court.

Acknowledgment and Acceptance

I acknowledge that willful violation of Neb. Ct. R. § 1-1201 et seq. and/or the Judicial Brach Information Systems and Security Policy may cause the Nebraska Supreme Court to direct any or all of the following:

1. Loss of access to information technology systems, networks, hardware and /or software;

2. Reporting of such violation to any disciplinary authority as directed by the Nebraska Supreme Court;

3. Disciplinary action if I am an employee covered by the Nebraska Supreme Court Personnel Policies and Procedures;

4. Termination or breach of contract;

5. Reporting of such violation to law enforcement, if a criminal act; and/or

6. Any other action the Nebraska Supreme Court deems advisable to protect the Judicial Branch's Information Systems.

_____	_____
Print or type your full name	Signature
_____	_____
Title or job description	Location of employment
_____	
Date	