On November 22, 2017, the Nebraska Supreme Court approved the deletion of two miscellaneous rules policies--the Acceptable Use Policy for Computer and Internet Use and the Electronic Communications Equipment Policy--and approved a new miscellaneous rules policy--the Information Systems and Security Policy:

~~Acceptable Use Policy for Computer and Internet Use~~

~~(*Effective March 29, 2006; Revised June 7, 2006; Revised September 15, 2010; Revised March 9, 2011; Revised May 23, 2012)*~~

~~1.0 Standard~~

~~1.1 Application and Intent~~

~~This policy shall apply to all judicial officers and employees using the State Data Communications Network (SDCN), the Nebraska Supreme Court Network (NSCN), Removable Media, and Social Media. It is intended to provide minimum standards for acceptable use, including clarification of uses which are consistent or inconsistent with this policy.~~

~~All use of the State Data Communications Network and/or the Nebraska Supreme Court Network (such as Internet logs and e-mail) by judicial officers and employees is the property of the State of Nebraska and is subject to applicable Nebraska Supreme Court rules and policies, and State and Federal laws, such as public record laws of the State of Nebraska as applicable. End users should not have any expectations of privacy regarding personal business conducted on the State Data Communications Network and/or the Nebraska Supreme Court Network unless protected by State or Federal law.~~

~~Use of the SDCN and/or the NSCN shall be consistent with the goals of:~~

~~· Simplifying and disseminating information;~~

~~· Encouraging collaborative projects and sharing of resources;~~

~~· Aiding technology transfer within and outside the State of Nebraska;~~

~~· Fostering innovation and competitiveness within Nebraska;~~

~~· Building broader infrastructure in support of the performance of professional work-related activities.~~

~~1.2 Acceptable Uses of the SDCN and/or the NSCN~~

~~1. To provide and simplify communications with other state agencies, units of government, and citizens.~~

~~2. To communicate and exchange professional development information, including online discussion or debate of issues in a field of knowledge.~~

3. To exchange communications in conjunction with professional associations, advisory committees, standards activities, or other purposes related to the user's professional capacity.

4. To apply for or administer grants or contracts for work-related applications.

5. To carry out regular administrative communications in direct support of work-related functions.

6. To announce new products or services within the scope of work-related applications.

7. To access databases or files for purposes of work-related reference or research material.

8. To post work-related questions or to share work-related information.

9. To communicate to children, teachers, doctors, day care centers, babysitters, or other family members to inform them of unexpected schedule changes, and for other minimal personal business. The use of the State's telecommunications systems for personal business shall be kept to a minimum and shall not interfere with the conduct of state business.

1.3 Unacceptable Uses of the SDCN and/or the NSCN

Unacceptable uses of the SDCN and/or the NSCN subject to remedial action (see Section 1.6), include, but are not limited to the following:

1. Violation of the privacy of other users and their data. For example, users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or represent themselves as another user unless explicitly authorized to do so by that user.

2. Violation of the legal protection provided by copyright and licensing laws applied to programs and data. It is assumed that information and resources available via the SDCN and/or the NSCN are private to those individuals and organizations owning or holding rights to such information and resources, unless specifically stated otherwise by the owners or holders, or unless such information and resources clearly fall within the statutory definition of a public record. It is unacceptable for an individual to use the SDCN and/or the NSCN to gain access to information or resources not considered a public record without the granting of permission to do so by the owners or holders of rights to such information or resources.

3. Downloading or installation of unauthorized software or hardware in violation of license agreements.

4. Violation of the integrity of computing systems. For example, users shall not intentionally develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system.

5. Use of the SDCN and/or the NSCN for fund-raising or public relations activities unrelated to an individual's employment with the Nebraska Supreme Court.

6. Use inconsistent with laws, Nebraska Supreme Court rules and policies, regulations, or accepted community standards. Transmission of material in violation of any local, state, or federal law or regulation is prohibited. It is not acceptable to transmit or knowingly receive threatening, obscene, or harassing material.

7. Malicious or disruptive use, including use of the SDCN and/or the NSCN or any attached network in a manner that precludes or significantly hampers its use by others. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer worms or viruses, and use of the SDCN and/or the NSCN to make unauthorized entry to any other machine accessible via the network.

8. Unsolicited advertising, except for announcement of new products or services as described in item No. 6 under "Acceptable Uses."

9. Use of the SDCN and/or the NSCN for recreational games.

10. Use in conjunction with for-profit activities, unless such activities are stated as a specific acceptable use.

11. Use for private or personal business ventures such as second sources of income, other family member personal business interests, et cetera.

12. Misrepresentation of one's self, the Nebraska Supreme Court, or the State of Nebraska when using the SDCN and/or the NSCN.

13. Contacting senators, lobbyists, and coworkers regarding legislative matters, unless requested as part of a unified strategy to do so. Communication via SDCN and/or NSCN to contact senators or lobbyists regarding personal issues or the advancement of legislation for the sole benefit of a specific employee group (e.g., salary bills, retirement benefits) and not the court as a whole.

1.4 Acceptable Uses of Removable Media (applicable only to users of the NSCN)

In order to prevent damage, compromise, or loss of data, the following mandatory restrictions will apply to the use of all removable media:

1. Only Nebraska Supreme Court owned or leased and managed removable media shall be used within the NSCN. No personal, non-Nebraska Supreme Court, or other unauthorized removable media may be used within the NSCN system.

2. It is not permissible to use Nebraska Supreme Court owned or leased media on personal computers or other devices that do not have an official connection to the NSCN unless authorized by the Nebraska Supreme Court's Information Technology Services.

3. Removable media should only be used to transport or store data when other more secure means, for example, NSCN e-mail system or network shared folders, are not available.

4. Removable media will only be used to store or transport data for such purposes of direct support of work-related functions, work-related reference, and/or research material.

5. All removable media is to be afforded the same level of physical protection as the most sensitive material stored thereon. All removable media should be stored in a safe, secure environment at all times. Users will ensure that all removable media checked out to them will be secured discretely, carried in a closed container, and not in public view where it can attract attention.

6. “On-Access” anti-virus and authorization scanner controls will be configured on all servers and workstations attached to the NSCN to check for removable media devices. Rather than scanning whole systems, on-access scanners will scan files and other removable media and their associated drives when they are accessed. Access is not allowed to such objects until the scanner has verified the device is authorized and virus free.

7. When transferring data from outside of the NSCN, extreme caution must be taken, as the potential impact of malicious software attacks on the NSCN system could be severe. All data is to be scanned by the on-access scanner prior to transfer.

8. Any loss or theft of any item of removable media must be reported immediately to the Nebraska Supreme Court's Information Technology Services so that the level of compromise can be assessed and necessary efforts can be made for recovery.

9. If any item of removable media is no longer required, it must be destroyed by approved secure means. This is only to be carried out by the Nebraska Supreme Court's Information Technology Services.

1.5 Unacceptable Uses of Removable Media (applicable only to users of the NSCN)

Unacceptable uses of Nebraska Supreme Court owned or leased removable media to store and/or move data, subject to remedial action (see section 1.6), include, but are not limited to the following:

1. Violation of the privacy of others and their data. For example, users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or represent themselves as another user unless explicitly authorized to do so by that user.

2. Violation of the legal protection provided by copyright and licensing laws applied to programs and data. It is assumed that information and resources available via the NSCN are private to those individuals and organizations owning or holding rights to such information and resources, unless specifically stated otherwise by the owners or holders, or unless such information and resources clearly fall within the statutory definition of public record. It is unacceptable for an individual to use the NSCN to gain access to information or resources not considered a public record without the granting of permission to do so by the owners or holders of rights to such information or resources.

3. Downloading of software in violation of license agreements.

4. Violation of the integrity of computing systems. For example, users shall not intentionally develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software or hardware components of a computer or computing system.

5. Storing or moving of data for fund-raising or public relations activities unrelated to an individual’s employment with the Nebraska Supreme Court, unsolicited advertising, for-profit activities, or use in private or personal business ventures such as second sources of income or other family member business interests, etc.

6. Use inconsistent with laws, regulations, or accepted community standards. Transmission of material in violation of any local, state, or federal law or regulation is prohibited. It is not acceptable to transmit or knowingly receive threatening, obscene, or harassing material.

7. Malicious or disruptive use in a manner that precludes or significantly hampers its use by others. Disruptions include, but are not limited to, destruction of stored data or physical destruction of the removable media device, propagation of computer worms or viruses, and the use of any removable media device to make unauthorized entry to any other machine owned or leased by the Nebraska Supreme Court or the State of Nebraska.

8. Use of Nebraska Supreme Court owned or leased removable media devices for recreational games.

9. Misrepresentation of one's self, the Nebraska Supreme Court, or the State of Nebraska.

1.6 Remedial Action

Routine monitoring of usage will not occur. In the event of reported or suspected unacceptable use in violation of this policy, the Chief Justice of the Nebraska Supreme Court, the State Court Administrator, the State Probation Administrator, or their designee may authorize the Deputy State Court Administrator for Information Technology to request monitoring of usage by a person subject to this policy, including Internet access and e-mail transmission, to be conducted by State of Nebraska Office of the Chief Information Officer (OCIO) or an applicable service provider.

Remedial action may include disciplinary proceedings against the individual or individuals responsible for the violation of this policy, including termination of employment or reporting to the appropriate disciplinary authority. If, in the judgment of the Chief Justice, it is believed that criminal activity has taken place within the SDCN and/or the NSCN infrastructure, the Chief Justice will notify the proper authorities and will assist in any investigation of any offense.

The Nebraska Supreme Court accepts no responsibility for traffic which violates the acceptable use policy of any other networks connected, either directly or indirectly, to the SDCN and/or the NSCN. If the owner of any network connected to the SDCN and/or the NSCN notifies the Nebraska Supreme Court's Information Technology Services of a violation of its acceptable use policy, the Nebraska Supreme Court's Information Technology Services shall inform the agency, board, commission, or affiliate organization within which such violation occurred. It shall be the responsibility of the agency, board, commission, or affiliate organization to take appropriate remedial action and notify the owner of the connected network.

2.0 Definitions

2.1 Nebraska Supreme Court Network (NSCN)

NSCN shall mean any data communications facility or equipment contracted for or provided by the Nebraska Supreme Court, Nebraska Court of Appeals, or the Administrative Offices of the Courts/Probation, including State provided Internet access and network connections to Nebraska Supreme Court owned or leased equipment.

The purpose of the NSCN is to provide a vehicle that allows data communications to occur among officers and employees of the appellate courts and administrative employees. Use of the NSCN is subject to the policies and standards contained in this document.

2.2 State Data Communications Network (SDCN)

State Data Communications Network (SDCN) shall mean any data communications facility or equipment contracted for or provided by the State of Nebraska, including State provided Internet access and network connections to Nebraska Supreme Court owned or leased equipment.

The purpose of the SDCN is to provide a vehicle that allows data communications to occur between agencies and across interstate and intrastate boundaries. Use of the SDCN is subject to the policies and standards contained in this document.

2.3 Removable Media (applicable to users of the NSCN only)

Removable media is defined as but not limited to the following: floppy disks, compact disks (CD's), Digital Video Disks (DVD's), jump drives, flash drives, portable hard drives, Firewire connected devices, Personal Digital Assistants (PDA's), and Universal Serial Bus (USB) connected devices.

3.0 Applicability

This policy shall apply to all judicial officers and employees using the SDCN and/or the NSCN.

4.0 Responsibility

The Nebraska Supreme Court's Information Technology Services is responsible for administration of the courts' use of the SDCN and/or the NSCN and for ensuring compliance with applicable laws, regulations, and policies. Individual supervisors are responsible for the activity of their employees and for ensuring that each employee is familiar with this Nebraska Supreme Court Acceptable Use Policy for Computer and Internet Use and that failure to comply with this policy may constitute grounds for disciplinary actions (see Section 1.6).

This policy applies to all judicial officers and employees using the SDCN and/or the NSCN or any other networks accessed through an SDCN and/or an NSCN connection, including the Internet. Compliance with this policy and the acceptable use policies of any other networks accessed through the SDCN and/or the NSCN connection is also subject to enforcement by the owner of that network.

Should a violation of this policy occur, the individual who committed the violation shall be personally liable for his or her actions. Lack of knowledge of or familiarity with this policy shall not release an individual from such liability.

Electronic Communications Equipment Policy

I. Purpose

This Policy provides guidance as to the appropriate circumstances for the Administrative Office of the Courts/Probation (AOC/AOP) purchase/lease of and service support for cellular phones, iPhones/Smart Phones, iPads/Tablets, laptop personal computers, data/air cards and other electronic communication or storage devices for use by employees in the course of their work.

II. Administrative Office of the Courts and Probation Electronic Communications Equipment Policy

A. Authority

This Policy is issued by the State Court Administrator under authority authorized by the Nebraska Supreme Court.

B. Policy

The Electronic Communications Equipment Policy (ECEP) encourages employees to use electronic communications equipment services and facilities for efficiency, conducting official Administrative Office of the Courts/Probation (Judicial Branch) business. There may be many work-related situations that require an employee's offsite use of electronic resources, such as issues that require immediate attention, prolonged discussions, or working from home during non-business hours. Some AOC/AOP business needs require an employee to be accessible at all times by electronic means, including cellular phones, computers, and other electronic communication devices. Electronic resources provided by the AOC/AOP, however, shall be used primarily for business-related purposes and any personal use of such resources must satisfy the conditions set forth in section III.B of this Policy.

C. Approval of Transactions

The State Court Administrator, or his or her designee, has the authority to approve the purchase or lease of electronic communications devices, and the accompanying services under which the AOC/AOP is the official "customer" to be billed. All purchases/leases of this type of equipment/services will be made through the Nebraska State Office of the Chief Information Officer, (OCIO) Network Services Division and /or the AOC Information Technology division.

III. Procedures

A. Criteria for Purchasing

The AOC/AOP may provide employees with electronic communications resources for use in conducting official AOC/AOP business outside the workplace when there is a significant business-related reason for doing so. To this end, the State Court Administrator may authorize AOC/AOP purchase of electronic resources only when the primary use of the resources will be for AOC/AOP business.

The State Court Administrator or division head should consult the following criteria in evaluating the business-related reason for purchasing electronic resources for employee use:

1. Electronic Communication Devices

Electronic communication devices and services may be purchased for those employees whose jobs entail some or all of the following responsibilities:

a. **Travel** – Employees who frequently travel or are out of the office and need to be in contact with staff, clients, managers, or other AOC business associates.
b. **Work Location** – Employees who typically work in the field or at job sites where access to electronic communications devices is not readily available.
c. **Emergency Response** – Employees who need to be contacted and/or to respond in the event of an emergency or are required to be available during non-business hours.
d. **Other** – Employees who are required by their division to be accessible at all times by electronic means.

The following list of devices and justifications will assist division heads in determining equipment and service needs for an employee.

iPad Wi-Fi Only (If they are capable of doing the following near a wireless access point.)

- Employee requires the ability to run a particular application to streamline their daily work,
- Employee requires the ability to consume reading materials,
- Employee requires the ability read/compose email frequently.

iPad 3G (Cellular Connectivity and Wi-Fi connectivity, additional data fees will apply)

- Employee requires the ability to run a particular application to streamline their daily work,
- Employee requires the ability to consume reading materials,
- Employee requires the ability read/compose email frequently.

iPhone/Smartphone

- Employee requires the ability to be contacted 24 hours per day 7 days per week,
- Employee requires the ability read/compose email frequently,
- Employee requires the ability to make telephone calls/texting away from their office.

Laptop Personal Computer

- Employee requires the ability do work away from their office.

Data Card (Cellular Data Connectivity)

- Employee requires the ability to connect to the Internet or State Data Communications Network frequently while away from their office.

Flash Drive (Thumb Drive)

- Employee requires the ability to transfer data between non-networked devices,
- Employee requires the ability to store data for backup purposes.

Web Camera

- Employee requires the ability connect with video conferencing software.

2. Office Equipment Located at Home and Internet Connection and Access

The AOC/AOP may purchase or lease personal computers and related software, printers, telephone lines, facsimile machines, and Internet and e-mail service for employees who telecommute or frequently work from home. The designated employee will approve such purchases in accordance with AOC/AOP guidelines for employees who work from home. The employee is responsible for ensuring that AOC equipment in the employee's off-site workspace is maintained in a safe and secure condition and is used primarily for AOC/AOP business. In addition, the division head should ensure that the employee is informed regarding the AOC/AOP's information security requirements for electronic communications equipment.

B. Incidental Personal Use

Personal use of electronic communications resources shall be kept to a minimum and shall not adversely affect the performance of an employee's official duties or the functions of an employee's division. The ECEP allows incidental personal use of an AOC/AOP electronic communications facility or service provided that such use does not violate the circumstances identified in the policy. Such personal use shall not (i) directly or indirectly interfere with the AOC/AOP's operation of electronic communications resources; (ii) interfere with the user's employment or other obligations to the AOC/AOP; or (iii) burden the AOC/AOP with additional costs.

C. Documentation

An employee who is to be provided electronic communications equipment or services must prior to receipt of such resources sign a usage agreement acknowledging that primary use of the resources will be for official AOC/AOP business and that any personal use of the resources will be incidental in nature. The Employee Agreement Concerning the Use of Electronic Communications Equipment Resources (the "Agreement") in Appendix A is to be used for this purpose.

D. Reimbursement of Non-Incidental Personal Use

As provided under the ECEP, any additional costs for personal use of an AOC/AOP-provided electronic communications resource must be reimbursed by the employee furnished with the resource.

With respect to cellular devices, it is the responsibility of the employee to reimburse the AOC/AOP for non-incidental, personal calls reported on statements billed to the AOC/AOP. If the employee should exceed the package minutes under a cellular phone contract, the AOC/AOP shall be reimbursed for any personal calls associated with the excess minutes at the excess-minute rate. If the employee does not exceed the package minutes, reimbursement is not required for any personal calls. However, both the employee and his or her division should annually review the contract with the OCIO Network Services staff to ensure that the employee is utilizing the most cost-effective plan.

AOC guidelines and procedures must utilize similar mechanisms to recover costs associated with the non-incidental personal use of other electronic communications resources where there are statements billed to the AOC that provide sufficient detail to identify such personal use.

E. Data Security and Confidentiality

Employees should be aware that all records related to the purchase, use, and disposition of AOC/AOP-owned electronic communications equipment, including cell phone statements, are the property of the AOC/AOP and are potentially subject to disclosure under the Nebraska Public Records Act.

Responsibilities

State Court Administrator

The State Court Administrator is responsible for establishing and updating the procedures set forth in this Policy.

Division Heads

The division is responsible for ensuring that any purchase of electronic communications resources for use by an employee conforms to the requirements of this Policy, and that claims submitted for payment or reimbursement include the appropriate supporting documentation. The division head is also responsible for monitoring the personal and business-related use of cellular phones to ensure that its employees are utilizing the most appropriate plan and for obtaining reimbursement for any personal use that burdens the AOC/AOP with additional costs, in accordance with this Policy.

Employees

An employee assigned AOC/AOP electronic communications equipment is responsible for safeguarding the equipment and controlling its use. The employee is required to reimburse the AOC/AOP for any Personal Use of a cellular phone should that result in additional costs to the AOC/AOP and should annually review the contract to ensure that the calling plan is appropriate for his or her business use.

The employee is expected to avoid using a cellular phone or any other type of electronic communications equipment under any circumstances where such use might create or appear to create a hazard, including use while operating a motor vehicle. In addition, the requirement does not apply to any AOC/AOP employee who uses a cellular telephone for emergency purposes, including, but not limited to, an emergency call to a law enforcement agency, health care provider, fire division, or other emergency services agency or entity.

Any employee whose electronic communications equipment is mislaid or stolen should immediately report the loss or theft of such equipment to his or her division and to the AOC Information Technology division, to the service carrier, and to the Office of the CIO if applicable. If it is determined the loss or damage to the equipment was caused by negligence by the employee, the cost to replace or repair the item may be passed on to the employee. Upon separation from AOC/AOP employment, the employee is required to promptly return such equipment to the AOC/AOP.

Appendix A

To: Division Head

Re: Employee Agreement Concerning the Use of Electronic Communications Equipment Resources

I hereby certify that I am the recipient of the following AOC/AOP-provided electronic communications equipment and/or services (check appropriate box):

____ **Equipment** - I agree that this equipment is to be used primarily for official AOC/AOP business, and that any personal use of the equipment will be kept to a minimum. I agree to reimburse my division for any personal use of this equipment that results in additional costs to the AOC/AOP and will exercise appropriate care and caution when using the equipment, in accordance with the policy and procedures set forth in AOC/AOP Electronic Communication Equipment Policy, In addition, I understand that all records related to the purchase, use, and disposition of this AOC/AOP-owned equipment, including cell phone statements, are the property of the AOC/AOP and potentially subject to disclosure under the Nebraska Public Records Act.

I further understand that I am responsible for safeguarding the equipment, including any data on the equipment, and controlling its use in accordance with the AOC/AOP Electronic Communication Equipment Policy. If the AOC/AOP determines that there is no longer a business need for me to possess such equipment, I will return the equipment. Likewise, if I separate from AOC/AOP employment, I will promptly return the equipment to my division.

Any employee whose electronic communications equipment is mislaid or stolen should immediately report the loss or theft of such equipment to his or her division, to the AOC Information Technology division, to the service carrier if applicable, and to the Office of the CIO. If it is determined the loss or damage to the equipment was caused by negligence by the employee, the cost to replace or repair the item may be passed on to the employee.

Device 1_____Device 2_____

Device 3_____Device 4_____

Device 5_____Device 6_____

_____ **Services** - I agree that this service is to be used primarily for official AOC/AOP business, and that any personal use of the service will be incidental in nature. I agree to reimburse my division for any personal use of this service that results in additional costs to the AOC/AOP, in accordance with the policy and procedures set forth in AOC /AOP Electronic Communication Equipment Policy. In addition, I understand that all records related to the purchase and use of this AOC/AOP-provided service, are the property of the AOC/AOP and potentially subject to disclosure under the Nebraska Public Records Act.

I further understand that if the AOC/AOP determines there is no longer a significant business need for me to utilize this service, the AOC/AOP will discontinue its funding of the service. Likewise, if I separate from AOC/AOP employment, the service will no longer be paid for or reimbursed by the AOC/AOP.

Name: _____ Title: _____

Signature: _____ Date: _____

Nebraska Supreme Court:

Information Systems and Security Policy

I. Intent:

The purpose of the Information Systems and Security Policy is to protect the judicial branch's information technology (IT) resources and to allow for current and future oversight of IT resources, restricting access as needed for security while still promoting the daily ability to conduct business and provide services.

II. Applicability:

This Information Systems and Security Policy shall apply to all judicial officers and employees of the Nebraska Supreme Court (NSC). Where indicated, this policy shall also apply to contract workers and internship positions. Any judicial officer, employee, intern or contractor (end user) of the judicial branch is also governed by NITC (Nebraska Information Technology Commission) standards, when not in conflict with internal judicial branch policies.

III. Acceptable Use:

Use of judicial branch equipment and networks shall be prioritized for professional communications and handling of work-related business. Employees can use the equipment for personal use "within reasonable limits," which means it cannot result in loss of work

productivity, interfere with official duties or result in additional expense. End users should not have any expectations of privacy regarding personal business conducted on equipment or networks provided through the judicial branch unless protected by state or federal law. All use is subject to applicable state and federal laws and regulations, such as public record laws of the State of Nebraska as well as Supreme Court rules. Routine monitoring of individual end users will not occur however NSC-IT will perform some routine monitoring of overall use of equipment or networks. In the event of reported or suspected violation of this policy, the State Court Administrator, the State Probation Administrator, or their designee may authorize monitoring of usage by a person subject to this policy, including Internet access and e-mail transmission, to be conducted by State of Nebraska Office of the Chief Information Officer (OCIO) or an applicable service provider. Unacceptable uses of judicial branch equipment and networks include, but are not limited to, violation of the privacy of other users and their data; malicious or disruptive use; unsolicited advertising, fund-raising or other for-profit activities; misrepresentation of the judicial branch; and use of unauthorized software or hardware in violation of license agreements. See also: NITC 7-101: Acceptable Use Policy State Data Communication Network.

IV. Access Control:

a. Physical Access

i. The data center shall only be accessible by the Network Administrator. If a contract worker or anyone else needs to access NSC's servers in the data center the Network Administrator must accompany them. Physical access to the data center shall be granted by smart card

credentials and fingerprint scanning of the Network Administrator by the OCIO and building security.

ii. Access to the storage vault(s) used for equipment storage by the NSC-IT (Nebraska Supreme Court Information Technology) Department in the basement of the state Capitol shall be controlled by the Court Administrator's office. The employee (employee, intern or contractor) must have smart card access to the basement of the Capitol and a vault key, or be accompanied by an authorized employee.

iii. Access to the NSC-IT work areas will be secured to ensure the protection of stored computer assets, as well as preventing unauthorized access to any IT workstations and equipment.

iv. NSC-IT will have a smart card and / or key access to all employee work areas before, during and after work hours for emergency IT purposes. NSC-IT will schedule visits ahead of time wherever possible.

v. Devices are available for checkout that allow end users to utilize hardware or software needed to do their job while away from their office. NSC-IT will manage access to and security for these devices. End users are responsible for safekeeping during the period in which they are checked out.

vi. Use of removable media shall be limited to purposes of direct support of work-related functions where other means of secure data transfer are not available. Only removable media issued by

NSC-IT shall be used on judicial branch owned or leased equipment. NSC-IT will be responsible for scanning and securing removable media when not in use.

b. User Access

i. The Network Administrator and or NSC-IT is responsible for creating user accounts and accompanying passwords, active directory (AD) structures for different departments and the needed group policies (GPO) to accompany them within the NSCAP (Nebraska Supreme Court Administration and Probation) domain. The state OCIO is responsible for exchange services and all other services and applications it provides and administers support for.

ii. When an employee position is open for hire, the hiring manager must notify the Network Administrator as soon as possible by submitting the approved NSC-IT checklist. This is necessary in order to facilitate procuring the hardware by the employee's start date.

iii. Once an employee has passed a background check and has been formally hired, the manager must then notify NSC-IT by submitting the approved form. Depending upon the needs of the position and requirements of the hiring manager, the new employee will be given access to the NSCAP domain. This will facilitate the creation of AD accounts, creation of a state email account and forwarding of the new employee's information on to other departments for additional

program accounts to be created. Employees may be issued state equipment for accessing state systems. Employees will also be given access needed for web applications and necessary software relating to the position.

iv. State issued cellular devices are available upon the approval of the hiring manager assuming the position is eligible for a cellular device. The phone must be requested through the Network Administrator or other designated Communications Coordinators authorized to procure through the OCIO.

v. Personal phones may have state email accounts installed on them but only after the required form is filled out and returned to the Network Administrator, signed by the Court Administrator and Chief Information Officer for the state. See: NITC 5-204: Linking a Personal Portable Computing Device to the State Email System

vi. Hiring managers must notify the NSC-IT department of any upcoming employee termination/separation. For security reasons, all accounts must be immediately disabled upon any employee leaving his or her position. Any data that is still needed, whether email or network-related, must be transferred or saved by 5 p.m. on the employee's last day. For unplanned separations, the hiring manager must contact NSC-IT immediately.

vii. Contractors / Interns

Access for contractors or interns must be requested by the

administrator or director of the department under which the systems reside. An AD account and a state email account can be created by NSC-IT at the request of the administrator or director.

c. Network Access

i. The Network Administrator is responsible for the NSCAP domain and all servers running within that domain. The Administrator is responsible for the daily upkeep, setup, disaster recovery and usage of these servers. The Administrator must be a part of any planned changes to the NSCAP domain, or usage of the domain by employees or third parties.

ii. The Network Administrator shall be the only one who is allowed to make programmatic changes to the NSCAP servers unless designated otherwise by the Administrator. The NSC-IT department is allowed to access AD for user setup and disabling user accounts along with creating file server shares. The NSC-IT department is also allowed to push software installs and updates over the NSCAP domain to its employees as needed.

iii. The Network Administrator shall utilize AD security event logs to log login and logout times for NSCAP domain access. The Network Administrator will also be responsible for administering the judicial branch's Mobile Device Management (MDM) solution for all state purchased mobile devices.

iv. The state OCIO department is responsible for VPN creation, upkeep and usage monitoring for all judicial branch employees, contractors and interns.

d. Computer Access

i. Only NSC devices with NSCAP user accounts shall be allowed to log onto the NSCAP domain. No other devices will have access to shared drives or applications residing on the NSCAP domain or VPN access to the NSCAP domain.

ii. User accounts will use ID's of employees' first initial of their first name and their whole last name. If this user ID is already taken, a middle initial will be used after the first initial of the first name. The password will conform to minimum password requirements. See NITC 8-302 Minimum Password Configuration. NSC-IT will not override these requirements for any employee.

iii. All judicial branch employees with system administrative credentials and contractors must use the state's VPN solution with dual authentication.

e. Application Access

i. All computers assigned from the NSC-IT department will have an operating system and basic software package that will allow employees to perform all necessary job responsibilities. Each office shall have software to fit their specific needs.

ii. If the application is controlled by the NSC-IT department, they will

furnish the username and password and be in charge of resetting passwords. If the application is controlled by the individual departments, that department must appoint a person to handle usernames and passwords.

iii. Terminated end users must have their application access removed within 3 calendar days by the responsible department.

V. Procurement

a. The State Court Administrator, the State Probation Administrator or his or her designee, has the authority to approve contracts for the purchase or lease of electronic communications devices, and the accompanying services under which the Administrative Office of the Courts and Probation is the official "customer" to be billed. All purchases/leases of this type of equipment/services will be made through NSC-IT or the OCIO.

b. The judicial branch may provide employees with computer equipment and appropriate licensed software for business use. The hiring manager is responsible for ensuring that purchase of any software and/or hardware for use by an employee conforms to the needs of the position. Hiring managers must follow procedures for requesting hardware/software through NSC-IT. Technology provided by the judicial branch for use in county courthouses will follow a set of published standards.

c. The judicial branch may provide employees with mobile devices with a data plan for use in conducting official business outside the workplace when there is a significant business-related reason for doing so. Hiring managers must

follow procedures for requesting mobile devices through NSC-IT.

d. The judicial branch will only procure electronic payment services, either online or point-of-sale, that have been approved through the State of Nebraska's contract process. These contracts shall ensure that the provider is fully PCI-DSS compliant and is subject to annual reviews of compliance status.

e. It is best practice when dealing with IT services to negotiate a Service Level Agreement (SLA). Be sure to keep the following points in mind when negotiating the SLA. Have the SLA reviewed by our legal counsel.

   i. Full description of all services provided

   ii. Responsibilities of all parties involved

   iii. Ownership of data / programing code

   iv. Uptime requirements

VI. Data Protection and Destruction

a. Network drive storage is provided for court employees with backup protection and disaster recovery for work-related data storage.

b. All data created and or stored on state networks, computers, peripherals or otherwise is property of the Supreme Court.

c. Any confidential or restricted data saved to the file server needs to be made a part of a data inventory maintained by NSC-IT. Examples include Social Security numbers, individual health information, financial information, et cetera. See NITC 8-902 Data Classification Categories.

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

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

f. As physical data storage media such as hard drives, thumb drives, DVD's / CD's, et cetera, wear out, they must be physically destroyed by NSC-IT.

VII. Employee Responsibilities

a. It is the responsibility of all employees to follow the Information Systems and Security Policy. All judicial branch employees must also review IT security training materials each year to maintain compliance.

b. All employees are responsible for being security minded when dealing with passwords, hardware and state data. Passwords shall not be written down. Encrypted password keepers and training on how to use them can be provided by NSC-IT.

c. Employees should only login with their own credentials to any network or application. Sharing of login credentials is not allowed.

d. When an employee leaves his or her desk or computer, the employee will lock the device (Win+L).

e. An employee who is assigned technology equipment is responsible for safeguarding the equipment and controlling its use. Any employee whose equipment is mislaid or stolen should immediately report the loss or theft of such equipment to his or her supervisor and to the NSC-IT for proper incident reporting. If loss or damage of judicial branch owned equipment was caused

by negligence on the part of the employee, the cost to replace or repair the item may be passed on to the employee. Upon separation from judicial branch employment, the employee is required to release any assigned equipment back to hiring manager or supervisor.

f. An employee who detects malware or any other compromise of the employee's device should immediately make a report to NSC-IT for proper incident reporting.

g. Employees will ensure that all removable media checked out to them will be secured at all times. Once an item of removable media has been used on a device not owned or leased by the judicial branch, it must be returned to NSC-IT for security scanning. Loss or theft of any item of removable media must be reported immediately to an employee's supervisor and NSC-IT.

h. Employees/contractors must utilize VPN whenever they are not directly connected to the state network. VPN must be used on any unsecured or public connection.

i. All judicial branch employees using state issued mobile devices must password protect the devices with a minimum of a 4-digit pin number. Stronger types of access control such as a longer password, thumbprint recognition are also acceptable. Personal mobile devices used to access state email must also adhere to the above guidelines.

VIII. Remedial Action

Remedial action for a violation of this policy may include disciplinary proceedings against the

individual or individuals responsible, including termination of employment or reporting to the appropriate disciplinary authority. Criminal activity performed using any judicial branch device or system can result in criminal investigation and/or prosecution.