SOUTH DAKOTA DEPARTMENT OF CORRECTIONS POLICY AND PROCEDURE		POLICY NUMBER 100-11	PAGE NUMBER 1 OF 8
		DISTRIBUTION:	Public
		SUBJECT:	Staff Use of State Computer Equipment and Technology
RELATED STANDARDS:	**ACA 5-ACI: 1F-02, 1F-07**	EFFECTIVE DATE:	September 01, 2024
		SUPERSESSION:	09/15/2023
DESCRIPTION: General Administration	REVIEW MONTH: August	**KELLIE WASKO** **SECRETARY OF CORRECTIONS**	

I. POLICY

It is the policy of the South Dakota Department of Corrections (DOC) to regulate staff's use and access of state computer equipment, software, and services, including computerized information and data processing resources and technology, shall be controlled by policy and directives to protect against errors, theft, loss, and misuse. Staff shall adhere to state policies, directives, and applicable law when using and accessing state computer equipment, software, services, information, data, and technology.

II. PURPOSE

The purpose of this policy is to establish ***written data security policy, procedure, and practice*** that ***govern the collection, storage, retrieval, access, use, and transmission of sensitive or confidential data contained in paper, physical, or media format*** **(ACA 5-ACI-1F-02)**.

III. DEFINITIONS

Computer:

A programmable electronic device designed to store, retrieve, and process data, perform prescribed mathematical and logical operations, and display the results of these operations. Includes mainframes, desktop and laptop models, tablets, and smart phones.

Computer Equipment:

The physical components of a computer or computer system, i.e., keyboard, monitor, printer, scanners, signature pads, etc.

Data Storage Device:

Any removable, rewritable CD, DVD, Universal Serial Bus (USB), flash drive, zip drive, thumb drive, or similarly constructed/intended device used to store data.

Electronic Communication Device:

An electronic communication device is any electronic device capable of transmitting signs, signals, writing, images, sounds, messages, data, or other information by wire, radio, light waves, electromagnetic means, or other similar means, including telephones, cellular phones, and computers.

Email (Electronic Mail) and Electronic Communication:

The electronic transmission of messages and documents. May be transmitted within an agency, between agencies of the state, or to a destination outside of the state email system. Attachments may be included, such as a word document

or file, which is not contained within the mail body of the email. Such communication is facilitated by a program designed to create, send, receive, and store messages and other data transmitted electronically between individual users or groups.

Internet:
Global system of interconnected computer networks providing users with access to information, resources, and services.

On-Line System:
Any mainframe or client/file server application which can be accessed using a computer or computer like device.

Personally Identifiable Information (PII):
Data that includes information that identifies a person by name or by government-issued identification numbers including Social Security, driver license, and passport numbers. It also includes data that can be used to distinguish an individual's identity, such as a name, social security number, date and place of birth, mother's maiden name, or biometric records. PII also includes financial account information, including account number, credit or debit card numbers, or protected health information (PHI), educational, or employment data relating to a person.

Software:
Machine/computer-readable instructions that direct the computer's processor to perform specific operations. Software includes programs, libraries, and their associated documentation. All software used by state computers is owned or leased by the state.

State Technology:
Telephone (including landline and wireless/mobile services) and computer services, including internet, intranet, and email.

IV. PROCEDURES

1. Approved Use:

A. Use and access to state computer equipment, software, services, computerized information, data, and technology is limited to official state business. Under no circumstances are employees allowed to use the state's technology to engage in outside business interests, inappropriate, offensive, or illegal activities. Abuse of the system is not acceptable. Employees should not expect privacy or confidentiality when using state resources. Use common sense. If in doubt, do not use state resources (see the Bureau of Human Resources and Administration's (BHRA) Technology Use policy at: https://intranetbit.sd.gov/docs/Information%20Technology%20Security%20Policy%20-%20BIT.pdf).

B. Staff may download software or applications not on the Bureau of Information and Telecommunications (BIT) standard inventory, only with prior approval from authorized BIT staff.
   1. The software requested must pertain to the staff member's official work duties.
   2. The staff member and/or the DOC data systems manager will ensure the software is properly licensed and registered.
   3. Downloaded software or applications will only be used or accessed in accordance with the provisions of the license/agreement or contract and is subject to all applicable copyright laws.

C. Staff are not permitted to install personal or non-state-owned hardware or software on state computers, servers, or networks.

D. Each staff member approved to use a state computer or access an on-line system of the DOC, data, or computerized information owned or kept by the DOC, is responsible for the maintenance and security of their user ID and password(s). Such information shall not be divulged to offenders or unauthorized individuals.

1. Staff will immediately change their computer log-on password if they suspect the confidentiality of their password(s) has been compromised.

2. Prohibited Use of State Computer Equipment and Technology:

A. Use of state computer equipment and technology for the purpose of harassing, stalking, or threatening another, or to further inappropriate or offensive behavior(s) toward others based on race, color, creed, religion, sex, ancestry, national origin, age, disability, or other legally protected status or characteristic is strictly prohibited.

B. Use of state computer equipment and technology to access sites that exhibit hate, bias, discrimination, libelous, or otherwise defamatory content (not an inclusive list), except for investigative or authorized purposes, is prohibited.

C. Use of state computer equipment and technology to access, display, archive, store, distribute, edit, or record sexually explicit, lewd, obscene, indecent, or pornographic material, except for investigative or authorized purposes, is prohibited.

D. Staff members will not use state computer equipment or technology to access entertainment software or games, play such games against an opponent(s), or engage in wagering/betting.

E. Staff members will not use state computer equipment or technology to knowingly download or distribute pirated software or data, including unlicensed software.

F. Staff members will not use state computer equipment or technology to knowingly distribute viruses/worms. Staff will not intentionally bypass any virus protection/detection system.

G. Staff members will not knowingly allow offenders access to state computer equipment except that equipment designated for offender access and use.

1. When unattended, staff computers containing sensitive information must be logged off the network. This is accomplished by pressing <Ctrl> <Alt> <Delete> on the keyboard and pressing <enter> to lock the computer.

H. Staff members will not improperly release computerized information or data originating from a DOC computer, network database, drive, or file that contains personally identifiable information (PII) not accessible in the public domain or open to public inspection or release, which if disclosed, could be used to steal a person's identity, violate the individual's right to privacy, or otherwise bring harm to the person unless such release is authorized, meets legal standards, and is for official DOC business.

I. Staff members will not use state computer equipment or technology to engage in or conduct personal or private business.

J. Staff members will not use state computer equipment or technology to engage in illegal or unlawful activities or purposes, including but not limited to, copyright infringement, libel, slander, fraud, defamation, harassment, intimidation, forgery, and impersonation.

K. Staff members will not use state computer equipment or technology in any way that violates DOC policy, directives, or for uses that are disruptive or harmful to the reputation or business of the DOC, reflect unfavorably on the DOC, destroy confidence in the operation of DOC, or adversely affect the public's trust.

L. Staff members will not use state computer equipment or technology to promote political or religious activities not directly related to the mission, function, or work/operations of the DOC, or which are inconsistent with state BHRA policy regarding state employees and political activities.

3. Maintenance of State Technology:

A. Maintenance of state technology supporting state computers is provided by BIT, which provides the DOC with database services and network data storage. The DOC may enter into contract with private technology providers/vendors for database services, data storage, and access to licensed software if approved by BIT

1. The provider/vendor will ensure the maintenance of their respective systems and software, and the availability, security, and reliability of computerized information and data stored on databases within the system.

B. Staff are responsible for immediately reporting any issues or problems occurring with state technology, including suspected breaches in the security of a DOC database or unauthorized access to DOC data, computerized information, or technology to their supervisor. Staff will contact their supervisor or BIT help desk regarding any damaged or broken computer hardware or infected software.

C. Staff are responsible for deleting any unnecessary or outdated files assigned to them and notifying their supervisor of any outdated files they may be aware of which they do not have permission to modify or delete. The DOC records retention schedule should be consulted before deleting files containing certain information.

D. Staff are responsible for the security of any removable, rewritable CD, DVD, Universal Serial Bus (USB) flash drive, zip drive, thumb drive, or other removable data storage device that contains confidential or sensitive DOC information or data.

E. All computers and computer equipment to be surplused, redistributed, or otherwise disposed of will be returned to the BIT parts center. BIT is responsible for ensuring any and all data has been wiped.

4. Lost/Damaged Electronic Equipment:

A. Staff will immediately report any lost, damaged, or stolen state owned or leased electronic equipment to a supervisor. In the case of a lost or stolen state issued remote access device (RAD), staff will:

1. Immediately notify BIT.
2. Change the Active Directory password, and
3. Notify the cellular company providing service to the RAD to have it deactivated.

B. Staff will immediately report to a supervisor, any electronic equipment (personal or state owned) that is lost or otherwise unaccounted for within the secure perimeter of a DOC facility or on the grounds of a DOC owned or leased facility which offenders may access.

1. If the initial report is made verbally, the staff member will follow up with an informational report to their supervisor.

5. Social Media:

A. The secretary of corrections (SOC) or designee may grant individual staff members approval to use state technology and computer equipment to create blogs, micro blogs, wikis, social networks, or videos containing DOC related information, or to officially participate (post/contribute or monitor) social media sites hosted on the technology infrastructure of the State of South Dakota/DOC or internet on behalf of the DOC during work hours. Such activity is limited to approved purposes and business.

B. The DOC will limit authorized connection and exchange of DOC related information to specified social media websites. Approval will be based on whether the content of the site is consistent with the mission, vision, and values of the DOC.

C. Professionalism will be maintained by staff members accessing, creating, and posting/contributing social media on behalf of the DOC. Staff conduct will be consistent with the mission, vision, and values of the DOC and will not violate standards of staff conduct, as described in DOC policy 100-05 – *Staff Code of Ethics*.

1. The provisions contained within SDCL apply toward the release of information pertaining to an offender.
2. Staff will not post photographs or video material of DOC staff, offenders, property, or other material that identifies the DOC without proper permission.
3. Staff will not engage in conduct or post/contribute information that reflects unfavorably on the DOC and/or the state, or that may destroy confidence in the operation of the DOC or state, or adversely affect the public trust in the DOC or state.
4. Social media will not be utilized by staff to communicate with other staff on official matters of the DOC or to relay confidential or business-related communications.
5. Staff posting/contributing content within social media will not claim to represent the DOC or its policies or comment on pending litigation or legal matters involving the DOC without prior authorization.
6. Staff engaged in social media activities on behalf of the DOC will not use vulgar, obscene, offensive language or terms, conduct personal attacks against fellow staff or offenders, be disrespectful to others, or negatively target a specific individual(s) or group(s). Posts will be appropriate and meaningful, and the staff member's conduct will be professional and respectful.

D. Discussions (posted content) on DOC managed technology infrastructures may be reviewed by the DOC public information officer (PIO), or staff authorized to manage and monitor the content of the social media site. The PIO or authorized staff, has authority to remove posted content from DOC managed infrastructures.

E. The DOC does not monitor staff personal use of social media. However, the DOC may investigate and take responsive action when it becomes aware of, or suspects staffs' conduct or communication on social media adversely impacts the DOC, staff, offenders, or violates applicable DOC policies, is inconsistent with the mission, vision, and values of the DOC, or compromises the staff member's ability to adequately perform their assigned duties.

6. Internet:

A. General information in the acceptable use of internet and state networks for DOC is available through BIT, including internet-based cyber security awareness training and information. Individual users who have been approved to have internet access shall be responsible for their own appropriate use of the internet and state networks.

B. Use of the internet on state networks is for legitimate business purposes. Incidental personal use is not prohibited, but such use must not affect staff's work performance, or the operations of the DOC. Internet use must not compromise system security. Use of the internet by staff must be consistent with the staff code of ethics, department policy, and legal standards, including applicable state and federal laws. The purpose of internet access from state resources is to conduct state business; examples include but are not limited to:

1. Communication with business associates.
2. Research.
3. Online training.
4. Obtaining relevant news/information.
5. Professional networking.
6. Listening to applicable legislative hearings or committee meetings for the purposes of fulfilling the user's agency or work group's mission.

7. Email and Electronic Communications:

A. The DOC recognizes that email and all electronic communications are critical mechanisms for communication, acquiring and sharing information, and participating in educational and professional activities. Use of the state email systems and services is a privilege, not a right, therefore state email must be used with respect and in accordance with the mission, vision, and values of the DOC.

B. Staff use of the state email system shall not disrupt the services or operations of the DOC and must comply with applicable policies, directives, and laws related to email and electronic communications.

C. Generation of an email creates a public record and may be considered to be open, unless privileged or made confidential by law. All email sent or received through the state email system is the property of the state/DOC. Staff have no expectation that email generated through the use of state computer equipment and state technology is privileged or confidential. The DOC may monitor, and with proper authorization, inspect any and all email traffic that passes through the state email system.

D. Staff shall use extreme caution when using email to communicate any confidential, personal, or sensitive information. Such email communication should be sent encrypted. All email messages sent outside of the DOC become the property of the receiver.

E. Important official communications may at times be sent by email. Staff with email accounts are expected to check their email in a consistent and timely manner. Non-exempt staff should only check email during work hours, in accordance with federal law.

F. Staff may use personal, or DOC issued cell phones or other electronic devices to check their state email account; however, the device must meet BIT standards for access and security software and all protection systems must be current.

G. Email users are expected to comply with the normal standards of professional and personal courtesy and conduct when using email. Users shall comply with the staff code of ethics and legal standards that apply to electronic communications.

H. The state email system is to be used for legitimate DOC business purposes. Incidental personal use is not prohibited, but such use must not affect the user's work performance or operations of the DOC or state and must not compromise system security or safety. Appropriate uses of state email typically further the goals and objectives of the DOC.

I. Staff shall use caution when opening email attachments from unknown or outside sources. Attachments are the primary source of computer viruses. Staff should contact BIT if they suspect their state computer or state technology has been affected by a virus or to report possible malicious email.

1. Staff are allowed to upload or change their photo in their Outlook and Teams accounts. Staff should use a photo of themselves that is a headshot, and a plain background is preferred. Staff should ensure that the photo portrays a professional image and is not discriminatory, political, obscene, or vulgar. Fund raising using the state email system for the individual and direct benefit of staff or family members of DOC staff must be pre-approved by the warden, director, SOC, or designees and is not considered part of the operations of the DOC.

8. DOC Website:

A. Anyone may view, copy, or distribute information found on the DOC's website for personal or informational use without obligation to the DOC. Staff may direct the public, media, outside groups, or other agencies to information contained on the DOC website without seeking prior authorization from the DOC and/or their supervisor.

B. The DOC makes no claim, promise, or guarantee about the absolute accuracy, completeness, or adequacy of the contents of its website and expressly disclaims liability for errors and omission in the contents and makes no warranty regarding the completeness or accuracy of the information or data contained within.

C. The DOC may make changes to information on its website at any time, including adding, removing, updating, or correcting any information.

9. Oversight:

A. The DOC reserves the right to monitor and restrict a staff member's use and access to state computer equipment and technology.

B. The DOC may authorize the inspection of any and all computerized information or data stored in public or personal/individualized systems of state computers or networks.
   1. Staff members have no expectation to privacy or confidentiality when using the state computer equipment.

10. Reporting Violations and Disciplinary Action:

A. It is the responsibility of every staff member to promptly report any violations of this policy to their immediate supervisor.

B. Violations of this policy by a staff member may result in disciplinary action, up to and including termination. If laws are violated, the staff member may be subject to criminal or civil action. Any evidence of criminal activity will be reported to law enforcement.

V. RESPONSIBILITY

It is the responsibility of the director of Finance and Administration to annually review and revise this policy as needed. It is the responsibility of supervisors to ensure ***all staff who have direct access to information in the information system have authorized access associated with their job duties and are trained in and responsive to the system's security requirements*** **(ACA 5-ACI-1F-07**).

VI. AUTHORITY

A. SDCL § **24-2-20 Records and information furnished court, secretary, board, or Governor--Information that may be released for certain other purposes.**
B. SDCL § **26-11A-30 Disclosure of identities of juveniles or others requesting assistance not required--Identity of person reporting to monitor to remain confidential.**
C. SDCL § **49-31-31.1 Electronic communication device defined.**

VII. HISTORY

September 2024
August 2023
February 2021
December 2019
June 2019
November 2015
November 2014

November 2013
May 2013
December 2012
January 2012

ATTACHMENTS

1. DOC Policy Implementation / Adjustments.