1.1.C.12 Staff Use of State Computer Equipment and Technology

I Policy Index:

Date Signed:	*12/13/2019*
Distribution:	*Public*
Replaces Policy:	*N/A*
Supersedes Policy Dated:	*08/08/2019*
Affected Units:	*All Units*
Effective Date:	*12/13/2019*
Scheduled Revision Date:	*November 2020*
Revision Number:	*13*
Office of Primary Responsibility:	*DOC Administration*

II Policy:

Department of Corrections 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 of state computer equipment, software, services, information, data and technology.

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 Equipment:
For the purposes of this policy, electronic equipment is any mobile communication device, two-way radio, smartphone/Remote Access Device (RAD) (includes but is not limited to Blackberry, iPhones, and Androids) lap top, tablet, non-stationary audio and/or video recording equipment (which includes hand-held video cameras, still/digital cameras, camera phones, tape recorders, other images or voice capturing devices, etc.), music headphones and I-pods.

Email (Electronic Mail):
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.

Fundraising:
The act of seeking donations of money, products, goods and/or services for the benefit of an individual, group, organization or department.

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

Offender:
For the purpose of this policy, an offender is an inmate (in the custody of the DOC institutional system), a parolee (under parole or suspended sentence supervision by South Dakota Parole Services) or a juvenile (either in DOC placement, including private placement, or aftercare).

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

Social Media:
Web-based technology that allows interactive dialogue and includes but is not limited to, print, broadcast, digital and online services, such as blogs, collaborative projects, content communities and social networking sites. Social media sites include but are not limited to Face book, LinkedIn, MySpace, Plaxo, Twitter, Tumblr, Instagram, Google and blogs, as well as video and photo-sharing sites such as Flickr and YouTube.

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.

Staff Member:
For the purposes of this policy, a staff member is any person employed by the Department of Corrections (DOC), full or part time, including an individual under contract assigned to the DOC, an employee of another State agency assigned to the DOC, authorized volunteers and student interns.

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 generally limited to official state business.

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 is not permitted to install personal or non-state-owned hardware or software on state computers, servers or networks without approval from BIT or the DOC Data Systems Manager. Installation of software onto state computing platforms is typically performed by BIT or authorized DOC staff. Any software or files downloaded to the computer becomes the property of the department.

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 (See DOC policy 1.1.C.10 *Harassment*).

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 a 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 state computer equipment except that equipment designated for inmate access and use (See DOC policy 1.5.A.7 *Inmate Use of Computers*).

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 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, institutional OMs or 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 (See DOC policy 1.1.C.1 *Code of Ethics*).

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 BHR policy regarding state employees and political activities.

3. Maintenance of State Technology:

A. Maintenance of state technology supporting state computers is primarily provided by the Bureau of Information and Telecommunications (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.

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 is 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 is 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 is 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. Staff Member Use of Personal Electronic Equipment at Work:

A. The Secretary, Warden, Director or designee may limit a staff member's use and access of personal electronic equipment during scheduled work hours.

B. Staff members may use and access personal electronic equipment during work hours under the following conditions:

1. Use and access does not negatively interfere with the performance of the staff member's job duties.

2. It is understood by the user that the DOC is not responsible for personal electronic equipment that becomes damaged, lost or misplaced, even if used for work purposes.

3. Staff members will not use or access personal electronic equipment in a manner that is considered by their supervisor to be disruptive to others in the workplace.

4. Use or access may be restricted if the personal electronic equipment poses a safety or security issue.

C. Staff members bringing any electronic equipment inside the secure perimeter of a DOC institution housing inmates must have prior approval from the Warden, Senior Security officer or designee.

1. Electronic equipment not authorized by the Warden, Senior Security officer or designee must be left in outside lockers or stored outside the secure perimeter.

2. Staff is not permitted to photograph or visually record offenders with personal electronic equipment, unless such recording is for official purposes. Prior approval may be required.

   a. Use of micro-cameras or recorders concealed within clothing or other objects which is used for the purpose of capturing a visual recording of unauthorized images or photos of offenders, data, information or unauthorized purposes, without the knowledge or approval of the supervisor, is prohibited.

3. Staff authorized to possess a Remote Access Device within the security perimeter will ensure the RAD is password protected, has a lockout feature enabled after 10 failed password attempts, and an inactivity timer set for a maximum of 15 minutes.

5. 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 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 inmates may access.

C. If the initial report is made verbally, the staff member will follow up with an Informational Report to their supervisor.

6. Social Media:

A. The Warden, Director, Secretary of Corrections 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 may limit authorized staff's connection and exchange of DOC related information to specified social media websites. Questions regarding the appropriateness of a social media site will be directed to the staff member's supervisor. Approval may be based on whether the content of the site is consistent with the mission, vision and values of the DOC.

C. Staff member use of state technology and equipment while representing the DOC within social media or participation in social media on behalf of the DOC, will be consistent with related policies and directives, as set forth by the DOC, BHR and BIT.

D. An appropriate level of professionalism will be maintained by staff members accessing, creating, 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 1.1.C.1 *Code of Ethics.*

1. Staff will not post/contribute copy, save, transfer, divulge or otherwise release information or content generally considered proprietary, restricted or confidential by the DOC, or violate the state's privacy or confidentiality laws. Information contained on social media sites is widely accessible and difficult to retract. Such information is typically considered public record. The same standards of conduct apply to social media platforms as apply to traditional forms of communication such as e-mails. Questions regarding information that may be considered confidential should be directed to the staff member's supervisor.

2. Staff will not release personally identifiable information not in the public domain, and if improperly disclosed, could be used to steal a person's identity, violate the individual's right to privacy or otherwise bring harm to the person.

   a. The provisions contained within SDCL §§ 24-2-20 and 26-11A-30 apply toward the release of information pertaining to an offender.

   b. Staff will not post photographs or video material of DOC staff, offenders, property or other material that identifies the DOC without proper permission (See DOC policy 1.1.A.4 *Relationship with News Media, Public and Other Agencies*).

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 (See DOC policy 1.1.C.1 *Code of Ethics*).

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.

7. Staff may be approved to monitor offender social media accounts and communicate with offenders using social media. This must be approved in advance by the staff member's supervisor and will only be for official purposes and must be consistent with the legitimate penological interests of the DOC.

E. Discussions (posted content) on DOC managed technology infrastructures may be reviewed by the DOC Communications and Information Manager, or staff authorized to manage and monitor the content of the social media site. The Communications and Information Manager or authorized staff, has authority to remove posted content from DOC managed infrastructures.

F. 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 a 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.

7. 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 shall be responsible for their own appropriate use of the Internet and state networks.

B. Use of the Internet on state networks is primarily for legitimate business purposes. Incidental personal use is not prohibited, but such use must not unreasonably 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.

8. Email:

A. The DOC recognizes that email is a critical mechanism 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 primarily for legitimate DOC business purposes. Incidental personal use is not prohibited, but such use must not unreasonably 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.

9. Use of State Email for Fundraising:

A. Fundraising and/or solicitation, defined as seeking or requesting donations from a group or individual(s) by a staff member with the aid of state e-mail, that is not specifically related to DOC activities or the operations of the DOC, must be pre-approved by the staff member's supervisor.

B. Fundraising and/or solicitation requiring approval which use the state email system will be scheduled and conducted in a manner that does not interfere with or disrupt state business.

C. The Warden, Director, Secretary of Corrections or respective designees must approve the inclusion of email recipients outside of the state email system for any fundraising or solicitation.

The requestor must include information that describes the intended recipients of the fundraising email.

1. Staff may be required to submit a draft of the fundraising email to the Warden, Director, Secretary or respective designees in advance of the email being sent.

2. The total number of non-state email recipients will be pre-determined and may be required by the Warden, Director, Secretary or respective designees prior to the fundraising email being sent.

D. Approved fundraising for local charities will generally be confined to email users located within the local area/unit. Exceptions, such as sending an email to "ALL DOC STAFF" may be granted on an individual basis.

E. Fundraising 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, Secretary or designee and is not considered part of the operations of the DOC.

F. All fundraising and solicitation conducted by staff using the state email system that directly or indirectly benefit the DOC or groups or organizations affiliated with the DOC, must be consistent with the mission, vision and values of the DOC, applicable laws, and DOC policy.

10. 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.

11. 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 and 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.

12. 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 Related Directives:

SDCL § 43-43B-1.

DOC policy 1.1.A.4 − *Relationship with News Media, Public and Other Agencies*
DOC policy 1.1.C.1 − *Code of Ethics*
DOC policy 1.1.C.10 – *Harassment*
DOC policy 1.5.A.7 – *Inmate Use of Computers*
BHR – *Technology Use Policy*

VI Revision Log:

New policy March 2007.
Removed revisions from 2007-2009 in Revision Log.
January 2012: **Deleted** "Non-Public" and **Replaced** with "Public" **Added** F. to Section 1. **Added** "stalking, threatening" to Section 2 B. **Added** "lewd, obscene or pornographic" to Section 2 C. **Added** "or engage in wagering or betting" to Section 2 D. **Added** "including photos or images of an offender" and "or unauthorized" and "or distribution" to Section 2 H. **Added** "or for uses that are disruptive or harmful to the reputation or business of the state or reflects unfavorably on the State, destroys confidence in the operation of State services or adversely affects the public's trust in the State" to Section 2 J. **Added** K. "Staff cannot use state computers to promote political or religious activities or fund raising (unless agency sanctioned)" to Section 2. **Added** L. "Staff cannot use state computers to access/participate in internet chat rooms or unauthorized social media sites" to Section 2. **Deleted** "while on duty" and **Replaced** with "during working hours" and **Added** "Working hours include breaks and lunch periods if the staff member is on DOC grounds." to Section 3 A. **Added** "Director of Juvenile Community Corrections to Section 3 C, D. and D. 1. **Added** "inappropriate, offensive or" to Section 4 A. 1. **Added** 1. "Staff members should not expect privacy or confidentiality when using the state's network, state computer (hardware) e-mail system or accessing the internet." to Section 4 B.
December 2012: **Added** definition of "On-Line System". **Added** "Employees shall comply with software copyright laws" to Section 1 B. 3. **Added** "publish, add, transmit" to Section 1 D. **Added** G. and G. 1. and H. to Section 1. **Added** "or use a state computer to improperly divulge or release protected and/or confidential information pertaining to offenders, employees or the DOC which they may have access to during the course of their official duties" in Section 2 H. **Added** "or conduct" and **Deleted** "interests" and **Replaced** with "or services" in Section 2 I. **Added** "without prior authorization by their supervisor" to Section 2 L. **Deleted** "local" in Section 3 C. **Added** "generally" to Section 3 C. 3.
May 2013: **Deleted** F. "Staff members may use state computers for reasonable and appropriate personal communications" from Section 1. (this is contained in Section 1 A. 1.) **Added** "internet" and "from a staff member's workstation" to Section 2 G.
November 2013: **Added** definition of "Microblogging" and "Data Storage Device" **Added** 1. To Section 2 B. **Added** new Section 4 and renumbered sections that follow. **Added** "social media or micro blogging sites" to Section 5 B. 1. **Added** D. E. and F. to Section 5.
November 2014: **Deleted** definition of "Micro blogging" **Added** "and adhere to all policies governing the use of state computers and technology" to the policy statement. **Deleted** language in Section 1 C. and **Replaced** with new language. **Added** 1. to Section 2 G.
November 2015: **Added** definition of "Computer" and "Fundraising". **Deleted** "Emergency communications" from Section 1 A. **Deleted** "must arrange to have" and **Added** "or DOC Data Systems Manager will ensure" in Section 1 B. 2. **Added** "without approval from BIT" **Deleted** D. 1-3. Regarding state licensed software" **Added** "and Intranet and search" in Section 1 D. **Added**

"immediately" in Section 1 E. 1. **Added** "except for investigative purposes or part of a staff member's official duties" to Section 2 C. and D. **Deleted** M. in Section 2. **Added** "and/or solicitation (a request sent to a group or individual seeking a donation) conducted with the use of " and **Deleted** "member during working hours and **Added** "and approved by the staff member's supervisor and **Deleted** "Working hours for the purpose of this policy shall include breaks and meal periods if the staff member is on DOC grounds" and **Deleted** "consistent with the state policy on Solicitations on State Premises and be" in Section 3 A. **Deleted** B. "Staff members will not use an "all DOC staff" e-mail for fundraising unless it is part of the state's United Way campaign or other special project sponsored or sanctioned by the Secretary of Corrections" in Section 3 and **Replaced** with new B. **Added** "or designee must approve any fundraising that will include email recipients outside of the state email system" and **Deleted** "staff use of the state e-mail system for limited fundraising" in Section 3 C. **Deleted** "Approval will be made on a case-by-case basis" and **Replaced** with "Staff may be required to submit a draft of the email to the Warden, Superintendent, Director, Secretary of designee in advance of the email being sent" in Section 3 C. 1. **Deleted** people/staff that will be solicited will be kept to a minimum" and **Replaced** with email recipients will be pre-determined and provided to the Warden, Superintendent, Director, Secretary of designee prior to the email being sent" in Section 3 C. 2. **Added** "email users located within the local area" and **Deleted** "of the state computer system within the local area and **Added** "Exceptions may be granted on an individual basis" in Section 3 D. **Deleted** "will be coordinated" and **Replaced** with "must be pre-approved" in Section 3 E. **Added** F. to Section 3. **Deleted** "inadvertently comes across such a " and **Replaced** with "purposefully or accidently" and **Deleted** "site while utilizing the internet" and **Replaced** with "attempts to access an Internet site determined to be inappropriate, an email will be generated by BIT advising the user they have attempted to access a restricted site" and **Deleted** "warning message will typically be received from BIT.A staff member who receives such a warning message should contact his/her supervisor as soon as practical and advise the supervisor of the incident" in Section 5 A. 2. **Deleted** F. in Section 5.
June 2019: **Revised** policy statement. **Combined** DOC Policy 1.3.A.10 Staff Use of State Technology into this policy.
December 2019:

Mike Leidholt (original signature on file)	*12/13/2019*
Mike Leidholt, Secretary of Corrections	Date