

1.5.A.7 Inmate Use of Computers

Policy Index:



Date Signed: 08/07/2019
Distribution: Public
Replaces Policy: N/A
Supersedes Policy Dated: 03/18/2019
Affected Units: All Institutions
Effective Date: 08/08/2019
Scheduled Revision Date: December 2019
Revision Number: 16
Office of Primary Responsibility: DOC Administration

II Policy:

Inmate access and use of computers will be monitored and regulated to prevent unauthorized activity.

III Definitions:

Intranet:

The BIT Intranet is an online network providing information on department policies and procedures, development services, standards and tools, electronic government and other internal resources within a department. The Intranet is an internal online information technology infrastructure throughout state government and is available to employees of state government.

Stand-Alone Computer:

A computer not tied into a state Local Area Network (LAN) system or the state's Wide Area Network (WAN). These machines cannot connect to the Intranet or a computer not tied into another island LAN.

Stand-Alone Local Area Network:

Computer workstations connected to each other but not connected to the State's Wide Area Network (WAN). Such configurations are sometimes referred to as an "island LAN".

Social Media:

Includes but is not limited to, print, broadcast, digital, and online services such as Facebook, LinkedIn, Myspace, YouTube, Plaxo and Twitter.

IV Procedures:

1. Inmate Use and Access to Computers Within the Institution:

- A. Institutional work supervisors, education staff, Private Sector Prison Industry (PSPI) supervisor(s) or other staff as assigned, shall be responsible for monitoring, approving and supervising inmate access and use of computers, systems, programs and installed hardware/software.

1. Unless otherwise approved, inmates are prohibited from accessing or using stand-alone computers with an island LAN. Inmates shall not have access to the state Intranet system or Internet. Inmates may not access computers without prior authorization.
 2. All computer hardware and software components used by inmates (including any type of removable data storage device), must remain at the inmate's assigned work station or assigned area and must be regularly and consistently accounted for and inspected by the work supervisor, PSPI supervisor, education staff or other authorized staff.
 3. Inmates may only access computer work stations, systems and programs designated for inmate use.
 4. An inmate's access to computers, systems or programs may be withdrawn at any time without notice or reason.
 5. Each DOC staff member authorized to use state owned computers capable of accessing the state Intranet or Internet that are located in an area where inmates may gain access to the computer, is responsible for the security of the computer and data. Staff shall maintain confidentiality of their logon identification (User ID and password(s)) at all times. Staff will not willfully, recklessly or negligently divulge such information to inmates, or in any way facilitate unauthorized access by an inmate to state computers, data or access to the Internet or Intranet (See DOC policy 1.1.C.12 [Staff Use of State Computers](#)).
 - a. Staff will immediately change their computer log in ID and password if they suspect the confidentiality of their ID or password has been compromised.
 - b. Staff assigned to state computers will ensure the computers LOCK device is enabled (by pressing <Window button> & <L>simultaneously on the keyboard) when the computer is not in use by the staff member or the staff member's workstation will be unattended, particularly when inmates are present in the area.
- B. Inmate access to computers is limited to approved and authorized purposes.
1. Designated areas within each institution shall permit inmates access to approved computers and software (Open Office, Microsoft Word, or similar programs) to access specific approved information on the computer, such as legal forms or approved course work. These computers will be configured to allow only approved tasks such as typing and printing of forms/documents and will prevent saving or storing any document or accessing unauthorized programs or systems, unless otherwise permitted. Inmate use of such computers shall be under the supervision of staff.
 2. Assigned staff will regularly check the computer and associated files for any saved data.
- C. Computers located in areas of the institution accessible to inmates will be marked with red tape on the monitor indicating the computer is a "Stand Alone" machine (not connected to the Intranet or Internet). Computers not marked with red tape are presumed to be connected to the Intranet or Internet.
- D. Inmates are not allowed to repair or modify any state owned or leased computer equipment, hardware, software, system(s) or program(s), except in an authorized training program or when an exemption has been granted by the Bureau of Information and Technology (BIT), Warden or designee.

1. When BIT staff is working on a computer, inmates will be required to distance themselves from the area where BIT staff is working.
 2. In the event an inmate needs to show BIT staff the issue, BIT staff will have the inmate log in and demonstrate the issue. The inmate will then be required to vacate the area.
 3. In the event inmates cannot be readily evacuated from the room, staff will schedule the repair at a time when inmates are not present.
- E. Inmates employed by Pheasantland Prison Industry (PI) may be authorized to view approved Internet sites by PI supervisors assigned to the area. Access to these sites will be for PI work related purposes only and the inmate(s) will be under the direct supervision of the supervisor or designated staff member.
- F. Inmate supervisors will ensure inmates accessing computers are made aware of all restrictions and limitations that apply to the use and access of computers, programs or systems.
1. Inmates permitted to use computers may not engage in inappropriate, offensive or illegal activities. An inmate's use of a computer shall not violate institutional rules or this policy. Inmates should not expect privacy or confidentiality when accessing or using any computer.
- G. Inmates cannot possess a personal computer, word processor, removable data storage device (such as floppy disks, hard drive disks, USB flash drives/thumb drives, rewritable CD's, DVD's or memory sticks) or a typewriter with memory (See DOC policy 1.3.C.4 [Inmate Personal Property](#)).
- H. Inmates with a communication disability may be provided access to computers, systems, programs and installed hardware or software to facilitate communication or receipt of written materials or information or otherwise meet an identified need for accommodation. Inmates requesting such accommodation shall contact the Facility ADA Coordinator (See DOC policy 1.1.E.7 [Americans with Disabilities Act \(ADA\)](#)).

2. Community Service Inmate Access to Computers:

- A. Community Service Program (CSP) inmates working for a state host agency may be allowed to access and use computers for authorized work purposes only. Access must be pre-approved by staff assigned to monitor/supervise the CSP inmate and consistent with DOC policy 1.5.A.6 [Community Service Program](#).
1. CSP inmates will not have direct or indirect access, viewing or interaction with networked computers, secure systems or Internet or Intranet, unless arrangements are made with and authorized by BIT staff and the DOC (See [Attachment 1](#)).
 2. Inmates using state host agency owned computers to access, view or interact with the LAN, WAN, secure systems or the internet or Intranet for authorized work purposes will be monitored by staff assigned to the area.
- B. State computers used by CSP inmates should be audited at least quarterly by agency staff or BIT staff. Audits are the responsibility of the host agency.

3. Work Release Inmate Access to Computers:

- A. Computer access by work release inmates is at the discretion of the employer. The DOC must be notified if a work release inmate will access computers as part of their assigned job duties (See [Attachment 4](#), DOC Policy 1.5.A.5 *Work Release*).
 - 1. Employers are responsible for deciding whether to implement additional computer security measures for work release inmates who have access to computers or use computers to perform their job duties.
 - 2. A work release inmates' access to computers is limited to work-related purposes.
 - 3. Employers are responsible for conducting audits of computers used/accessed by work release inmates.
- B. Inmates on work release job search status may be granted access to computers equipped with Internet at Department of Labor (DOL) offices and designated worksites within DOC institutions to view employment opportunities, complete job applications and job skill assessments. DOL staff are responsible for monitoring and supervising inmate access to the Internet.

4. Inmate Access to Sensitive Information:

- A. Inmates will not have access to personal/confidential information or any sensitive data stored on a computer, system, program that is accessible through the computer, system or programs (See DOC policy 1.1.E.3 *Offender Access to DOC Records*). Sensitive data is defined as any information not available to the public or subject to open records disclosure.
- B. Inmates will not be given direct or indirect access to staff passwords, administrative passwords, authorized codes (Log In ID) or system manuals intended for staff use only.
- C. Inmates are not permitted to have password protected screen savers or use a password to protect saved documents, forms or files. Inmates may not share User Ids.

5. Audits of Computers Used by Inmates within an Institution:

- A. All computers used by inmates will be audited at least quarterly by DOC staff, BIT staff or contract staff supervising the area (See [Attachment 2](#)). This includes computers at staff workstations from which inmates are permitted access to the computer.
 - 1. If DOC staff or contract staff is not familiar with the computer system or unable to conduct audits of the system/computer, staff will request assistance from BIT.
 - 2. The purpose of the audit is to identify abuse or unauthorized access to data or systems.
- B. Inmates are subject to disciplinary action for any unauthorized access or prohibited use of a computer (See DOC policy 1.3.C.2 *Inmate Discipline System*).
- C. Computer audits will be logged, and the log turned into the respective Major or designated security staff at the end of each quarter.
- D. Inmates found to have violated SDCL § [43-43B-1](#) (unlawful use of a computer system, software, or data) may be subject to disciplinary action and criminal prosecution.

V Related Directives:

SDCL § [43-43B-1](#).

DOC policy 1.1.C.12 – [Staff Use of State Computers](#)
DOC policy 1.1.E.3 – [Offender Access to DOC Records](#)
DOC policy 1.1.E.7 – [Americans with Disabilities Act \(ADA\)](#)
DOC policy 1.3.C.2 – [Inmate Discipline System](#)
DOC policy 1.3.C.4 – [Inmate Personal Property](#)
DOC policy 1.5.A.5 – [Work Release](#)
DOC policy 1.5.A.6 – [Community Service Program](#)

VI Revision Log:

December 2004: New policy.

May 2006: **Added** restrictions on inmate use of computers. **Noted** that the inmate's work supervisor is responsible for approving inmate use of computers. **Added** attachments 1 and 2.

January 2007: Minor style and format changes throughout the policy.

December 2008: **Revised** formatting of policy and attachments in accordance with DOC policy 1.1. A.2. **Replaced** Adult Units to Adult Institutions within Affected Units of Section I. **Added** ss (G of Authorized Inmate Use of Computers). **Revised** title of Attachment 1 to be consistent with policy, attachment and WAN.

December 2009: **Added** hyperlinks.

January 2011: **Added** Social Media definition. **Added** "monitoring" to Section 1 A. 1. **Added** "or other DOC policies or institutional OM's pertaining to inmate use of computers" to Section 1 A. 6. **Added** State host agency to Section 1 D. **Added** "state owned or leased" to Section 1 E. **Deleted** all of A. 2. in section 1 of Procedures. **Added** "social network e.g. Face book to A. 5. section 1 of Procedures **Added** A. 6 to section 1. **Deleted** "are not allowed internet access unless they are" from C. in same section. **Added** "may be allowed internet access for authorized work purposes" in Section 1 C. **Added** "employed" and "or supervisor" to Section 1 G. **Added** ss 1. and 2. to G. **Added** H. **Added** ss 1. - 3. to H. **Added** "state host agency" to A. in section 2.

March 2012: **Deleted** "An exception may be made for computers in a classroom setting used to teach LAN based applications" in definition of Stand-Alone Computer. **Deleted** "and documenting the approval" from Section 1 A. **Added** "approved by and" to Section 1 A. 1. **Added** "restrictions" and **Deleted** "and understand this policy before being given" and **Replaced** with "that apply to accessing a computer before granting the inmate" in Section 1 F. **Deleted** 1.-3. in Section 1 H.

January 2013: **Added** "codes or manuals intended for staff use only" to Section 2 B.

May 2013: **Added** "Within the Institution" to title of Section 1. **Added** "supervisor, education staff, PPSI supervisor or other authorized staff" and **Added** "access, viewing" and **Added** "and systems, programs and installed hardware/software" to Section 1 A. **Deleted** "noted in DOC policy" and **Replaced** with "viewed" and **Deleted** "contractual staff" in Section 1 A. 1. **Deleted** "site" and **Replaced** with "station" and **Added** "(including any type of removable data storage device" and **Added** "station shall be maintained and accounted for by the work supervisor, education staff or other authorized staff" in Section 1 A. 2. **Deleted** "who have been approved to access a computer" and **Replaced** with "may only access work stations, systems, programs designated for inmate use by work supervisors, education staff or other authorized staff" in Section 1 A. 4 **Deleted** 5. "Inmates must have the approval of their work supervisor, Warden or his/her designee to view or change any information in a database" in Section 1 A. **Renumbered** subsections that followed. **Added** "access, view or interact (directly or indirectly) with computers, systems the internet and or electronic media" and **Added** "pleasure" and **Added** "or access, view or interact with email, instant messaging, social media or viewing unapproved internet sites" in Section 1 B. **Added** "located in areas of the institution where inmates have access to computers" in Section 1 C. **Added** "Systems and/or hardware/software to Section 1 D. **Added** New E. and E. 1. and **Renumbered** F & G. that followed in Section 1. **Added** "any type of removable storage device (such as floppy disks, hard drive disks, USB flash drives/thumb drives, rewritable CD's or

DVD's or memory sticks)" in Section 1 G. **Added** new section 2 and Section 3. **Renumbered** sections that followed. **Added** "CSP" and **Deleted** "working for state host agencies" and **Deleted** "as part of the CSP" and **Added** "to access, use, view approved internet sites" in Section 2 A. **Added** "employee workstations" and **Added** "the DOC" to Section 2 A. 1 **Added** 2. to Section 2 A. **Added** B. to Section 2 **Added** 3 & 4 to Section 3 A. **Added** "Department of Labor and Regulation staff" and **Added** "DLR staff may monitor the inmate's access to the internet as they deem appropriate/necessary" to Section 3 B. **Added** 1. to Section 3 B. **Added** "Within an Institution" to Section 5 title. **Added** "This includes computers at staff workstations where an inmate may be allowed access to the internet for approved work-related purposes" in Section 5 A **Added** "within an institution" to Section 5 A. 1.

December 2013: **Added** definition of "Intranet". **Added** "in an area where inmates may gain access to the computer" and **Added** "for security of information on their assigned workstation" and **Added** "login identification, User Id" in Section 1 A. 5. **Deleted** "are password protected and locked" and **Replaced** with "LOCK device is enabled" and **Added** "or the workstation is unattended" in Section 1 A. 5. b. **Added** 1. to Section 1 F. **Added** "Sensitive data is defined as any information not available to the public via the Freedom of Information Act" in Section 4 A. **Added** "If a User Id is assigned to an inmate(s), staff shall maintain a comprehensive list of all inmate User Ids. Inmates will not share User Ids" in Section 4 D. **Added** D. to Section 4.

December 2014: **Reviewed** with no changes.

December 2015: **Reviewed** with no changes.

December 2016: **Deleted** "legal work" from Section 1 B. **Added** 1. to Section 1 B. **Added** H. and H. 1. to Section 1.

December 2017: Minor structure and sentence revisions.

December 2018: **Reviewed** with no changes.

February 2019: **Added** DOL offices and designated worksites in DOC institutions to Section 3 B.

August 2019: **Deleted** "Inmates may not access state computers, systems or programs (includes Internet and/or electronic media) for personal business or pleasure, e.g. writing personal letters, playing computer games, listening to music, accessing, viewing or interacting with email, instant messaging, social media or viewing unapproved sites" and **Replaced** with "Inmate access to computers is limited to approved and authorized purposes" in Section 1 B. **Added** "and software (Open Office, Microsoft Word, or similar programs) and **Added** "unless otherwise permitted" in Section 1 B. 3.

Mike Leidholt (original signature on file)

Mike Leidholt, Secretary of Corrections

08/07/2019

Date

Attachment 1: Inmate Computer Access Request

The *Inmate Computer Access Request* form is located at:

<M:\DOC\DOC Policies\Agency\DOC Policies\Attachment Templates\INMATE COMPUTER ACCESS REQUEST.doc>

The gray areas indicate the information that is to be entered.

South Dakota Department of Corrections Policy Distribution: Public	Attachment: Inmate Computer Access Request Please refer to DOC policy 1.5.A.7 Inmate Use of Computers
INMATE COMPUTER ACCESS REQUEST	
Requesting Agency: <input type="text"/>	
Agency Contact Person: <input type="text"/>	Phone #: <input type="text"/>
Can the inmate use a stand-alone computer to accomplish his/her duties: Yes: <input type="checkbox"/> No: <input type="checkbox"/>	
List the computer applications the inmate will need access to:	
<input type="text"/>	
<input type="text"/>	
<input type="text"/>	
Comments: <input type="text"/>	
<input type="text"/>	
<input type="text"/>	
<input type="text"/>	
Acknowledgment - The requesting agency hereby acknowledges and agrees to the following:	
<input type="checkbox"/>	
1. BIT reserves the right to either approve or deny this request. If the request is approved, BIT further reserves the right to audit the inmate computer and inmate work areas at their discretion.	
2. The requesting agency understands that the inmate will be assigned his/her own user ID and will be billed for this service.	
3. The computer designated for inmate use will be for inmates only. Sharing of user ID's to use staff computers is PROHIBITED.	
4. Any changes to the computer configuration as originally designed must be requested and approved through BIT following this same process.	
<input type="text"/>	
<input type="text"/>	<input type="text"/>
Requesting Agency Signature	Date
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
Revised: 12/12/2008	Page 1 of 1

Attachment 2: Computer Audit Report

The **Computer Audit Report** form is located at:

<M:\DOC\DOC Policies\Agency\DOC Policies\Attachment Templates\COMPUTER AUDIT REPORT.doc>

The gray areas indicate the information that is to be entered.

South Dakota Department of Corrections Policy Distribution: Public		Attachment: Computer Audit Report Please refer to DOC policy 1.5.A.7 Inmate Use of Computers	
COMPUTER AUDIT REPORT			
Date: <input type="text"/>			
Section: <input type="text"/>			
Computer Name: <input type="text"/>	Marked With Red Tape: <input type="checkbox"/> Yes <input type="checkbox"/> No		
Networked: <input type="checkbox"/> Yes <input type="checkbox"/> No	Stand Alone: <input type="checkbox"/> Yes <input type="checkbox"/> No	Island Lap: <input type="checkbox"/> Yes <input type="checkbox"/> No	
Special Attention Was Made To The Following:			
Personal Icons On Desktop	<input type="checkbox"/> Yes <input type="checkbox"/> No	Other:	<input type="text"/>
Personal Folders Created	<input type="checkbox"/> Yes <input type="checkbox"/> No	Other:	<input type="text"/>
Music CD's Found	<input type="checkbox"/> Yes <input type="checkbox"/> No	Other:	<input type="text"/>
Games Found	<input type="checkbox"/> Yes <input type="checkbox"/> No	Other:	<input type="text"/>
Confidential/Sensitive Records	<input type="checkbox"/> Yes <input type="checkbox"/> No	Other:	<input type="text"/>
Personal/Legal Letters Found	<input type="checkbox"/> Yes <input type="checkbox"/> No	Other:	<input type="text"/>
Internet Accessibility	<input type="checkbox"/> Yes <input type="checkbox"/> No	Other:	<input type="text"/>
Password Being Used	<input type="checkbox"/> Yes <input type="checkbox"/> No	Other:	<input type="text"/>
Network Drive Links	<input type="checkbox"/> Yes <input type="checkbox"/> No	Other:	<input type="text"/>
Mainframe Sessions	<input type="checkbox"/> Yes <input type="checkbox"/> No	Other:	<input type="text"/>
Unnecessary Pictures/Music	<input type="checkbox"/> Yes <input type="checkbox"/> No	Other:	<input type="text"/>
I, <input type="text"/> have audited all computers in my area.			
The following discrepancies were found: <input type="text"/>			
<input type="text"/>			
<input type="text"/>			
<input type="text"/>			
<input type="text"/>			
<input type="text"/>			
Signature: <input type="text"/>		Date: <input type="text"/>	
Revised: 12/12/2008		Page 1 of 1	