1.5.A.7 Inmate Use of Computers

Policy Index:

Date Signed:	***03/11/2020***
Distribution:	***Public***
Replaces Policy:	***N/A***
Supersedes Policy Dated:	***12/10/2019***
Affected Units:	***All Institutions***
Effective Date:	***03/11/2020***
Scheduled Revision Date:	***December 2020***
Revision Number:	***18***
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 internal online information technology infrastructure throughout state government and is available to employees of state government that provides information on department policies and procedures, development services, standards and tools, electronic government and other internal resources within a department.

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. Correctional Industries work supervisors, education staff, Private Sector Prison Industry (PSPI) supervisors, or other DOC staff supervising inmates within a DOC institution are responsible for monitoring, approving and supervising inmate access to and use of,

computers and related equipment, systems, programs and installed hardware/software approved for inmate use.

1. Unless otherwise approved, inmates are prohibited from accessing stand-alone computers with an island LAN. Inmates shall not have access to the state Intranet system or computers with access to the Internet.

2. Inmates may only access computer workstations, systems, programs and installed hardware/software specifically designated and approved for inmate use.

3. An inmate's access to computers and related equipment, systems and programs may be withdrawn at any time, without advance notice, reason or cause.

4. Staff authorized to use state computers within an area where inmates are present are responsible for the security of the computer.

5. Staff shall always maintain confidentiality of their logon identification (User ID and password(s)). Staff will not willfully, recklessly or negligently facilitate access by unauthorized persons to state computers and related equipment, systems and programs (See DOC policy 1.1.C.12 *Staff Use of State Computer Equipment and Technology*).

    a. Staff will immediately change their password if they suspect the confidentiality of their password has been compromised.

    b. Staff approved to access state computers will ensure the computer LOCK device is enabled (by pressing <Window button> & <L>simultaneously on the keyboard) when not using the computer, including anytime the computer is not under the direct observation of the staff person when inmates are present in the area.

B. Inmate access to computers is limited to approved and authorized purposes.

1. Inmates may be provided access to designated computers in designated areas of the institution for approved processes. Inmate computers have designated software (Open Office, Microsoft Word, or similar programs) loaded onto the computer to facilitate access to specific, approved information and functions within the computer, such as access to legal forms or approved course work.

2. Inmate computers will be configured to allow only those tasks and functions that have been previously approved by the Warden or designee, such as typing and printing of forms/documents.

3. Inmate use of computers shall be under the supervision of staff.

4. Assigned staff will regularly check the computer and associated files for inappropriate use, access, or content. This includes any thumb drives which are checked out by an inmate for work/approved purposes.

C. Computers located in areas of the institution accessible to inmates will be marked with red tape on the monitor which indicate 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 (intended only for staff use).

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) or Correctional Industries may be authorized to view approved Internet sites by PI supervisors assigned to the area for work purposes only. The inmate must be under the direct, visual supervision of the supervisor or designated staff member while using the computer.

F. Inmates may be issued a thumb drive by the work supervisor to perform approved tasks. The thumb drive must be signed out by the inmate. The supervisor shall account for the thumb drive(s) at the conclusion of each work period. Thumb drives are subject to search by staff at any time. No unauthorized content/file shall be saved to the thumb drive.

G. 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, prohibited/illegal activity. An inmate's use of a computer shall not violate institutional rules or DOC policy. Inmates have no expectation of should privacy or confidentiality when accessing any computer.

H. Inmates may not 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 outside of authorized and approved uses (See DOC policy 1.3.C.4 *Inmate Personal Property*).

I. Inmates with a communication disability may be provided access to computers, systems, programs and installed hardware or software to facilitate communication of written materials or information, or otherwise meet an identified need for accommodation. Inmates requesting accommodation must 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 permitted access and use of computers for authorized work purposes only. Access must be pre-approved by staff assigned to monitor/supervise the inmate, 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 the 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 must be monitored by staff assigned to the area.

B. State computers used by CSP inmates must 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. Access to computers by work release inmates is at the discretion of the employer. The DOC must be notified if a work release inmate requires regular access to a computer as part of their assigned job duties (See Attachment 4, DOC Policy 1.5.A.5 *Work Release*).

1. Employers are responsible for implementing computer security measures to monitor or restrict an inmate's access to computers and programs and/or to otherwise monitor the inmate's activities on the computer.

2. A work release inmates' access and use of computers is limited to work-related purposes.

3. Employers are responsible for conducting audits of computers used/accessed by work release inmates.

4. The DOC is not responsible for intentional or unintentional damage or other harm or risk caused by an inmate through use of a computer.

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 stations 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 or program or use a computer or programs to otherwise access such information without prior authorization by DOC staff (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 granted 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 to use passwords to protect saved documents, forms or files. Inmates may not share User Ids.

5. Audits of Computers:

A. All computers approved for access 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 which are accessed by inmates under staff supervision.

1. If DOC or contract staff is not familiar with the computer system or is unable to conduct an audit of the computer, staff must request assistance from the respective BIT staff person.

2. The purpose of the audit is to identify inmate abuse or unauthorized access to data or systems.

3. The results of the audit shall be turned into the Deputy Warden, senior security staff or designee.

4. Inmates found to have used the computer in a manner contrary to policy, staff directive or rules, are subject to disciplinary action(See DOC policy 1.3.C.2 *Inmate Discipline System*).

B. Inmates found to have violated SDCL § 43-43B-1 (unlawful use of a computer system, software, or data) or who have violated any state or federal law with regards to use of a computer system are subject to criminal prosecution.

V Related Directives:

SDCL § 43-43B-1.

DOC policy 1.1.C.12 − *Staff Use of State Computer Equipment and Technology*
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.
Removed revisions from May 2006 December 2009.
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 workstations, 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** "logon 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.

December 2019: Minor language changes.

March 2020: **Added** "Correctional Industries work supervisors" and **Added** "and related equipment" to Section 1 A. **Added** "This includes any thumb drives which are checked out by an inmate for work/approved purposes" in Section 1 B. 4. **Added** F. to Section 1. **Added** "outside of authorized and approved uses" to Section 1 H.

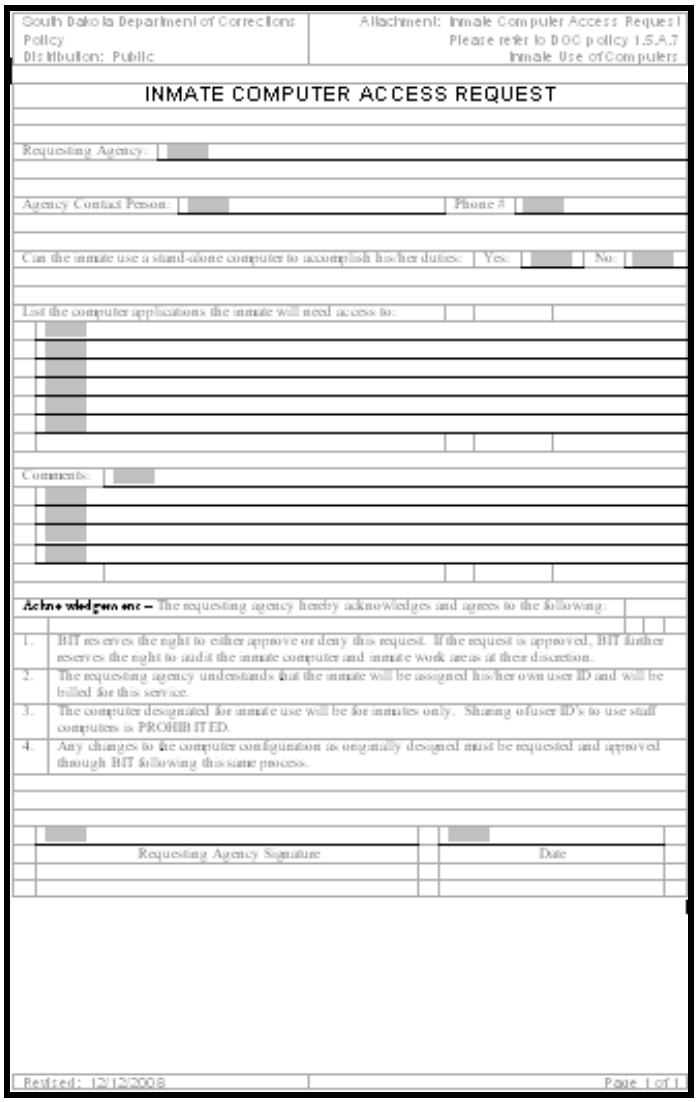
Mike Leidholt (original signature on file)	*03/11/2020*
Mike Leidholt, Secretary of Corrections	Date

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:

Agency Contact Person: Phone #

Can the inmate use a stand-alone computer to accomplish his/her duties: Yes: No:

List the computer applications the inmate will need access to:

Comments:

Acknowledgement – The requesting agency hereby acknowledges and agrees to the following:

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.

Requesting Agency Signature | Date

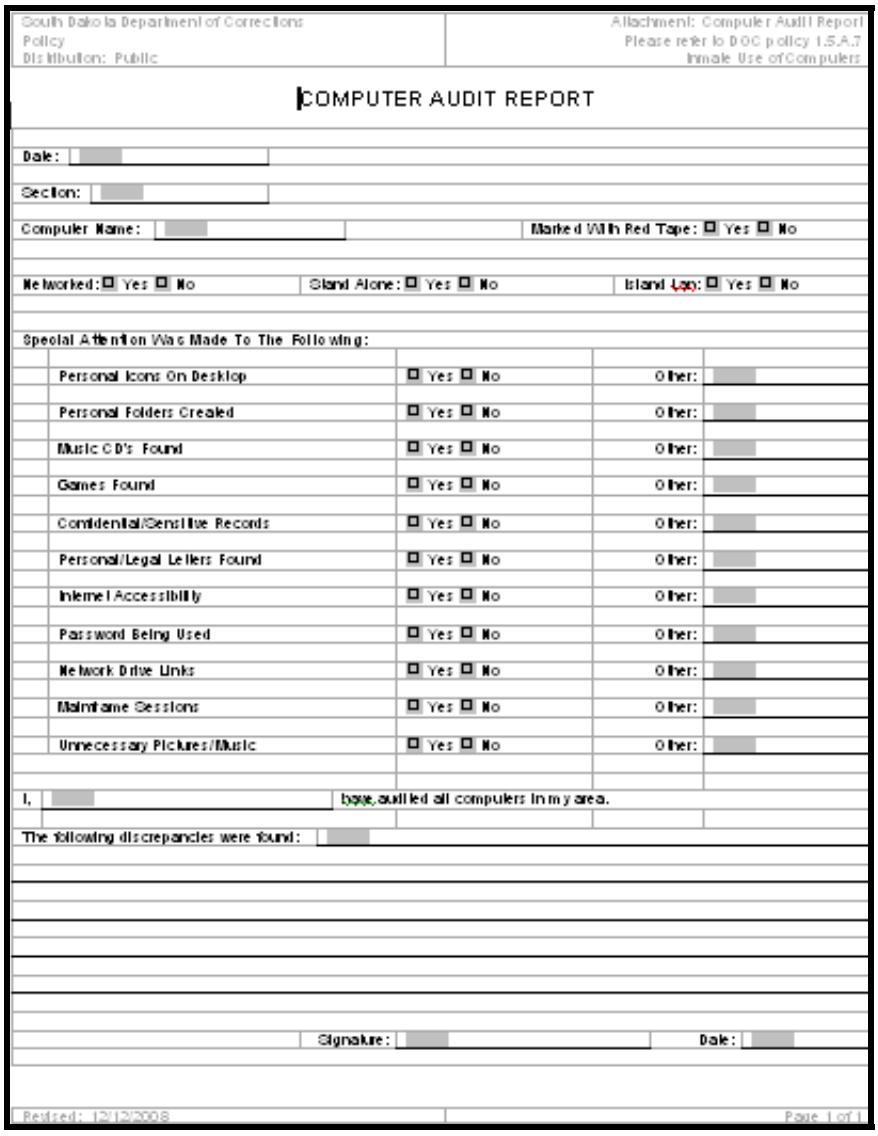
Revised: 12/12/2008 Page 1 of 1

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:

Section:

Computer Name: Marked With Red Tape: ☐ Yes ☐ No

Networked: ☐ Yes ☐ No Stand Alone: ☐ Yes ☐ No Island Lan: ☐ Yes ☐ No

Special Attention Was Made To The Following:

Personal Icons On Desktop	☐ Yes ☐ No	Other:
Personal Folders Created	☐ Yes ☐ No	Other:
Music CD's Found	☐ Yes ☐ No	Other:
Games Found	☐ Yes ☐ No	Other:
Confidential/Sensitive Records	☐ Yes ☐ No	Other:
Personal/Legal Letters Found	☐ Yes ☐ No	Other:
Internet Accessibility	☐ Yes ☐ No	Other:
Password Being Used	☐ Yes ☐ No	Other:
Network Drive Links	☐ Yes ☐ No	Other:
Mainframe Sessions	☐ Yes ☐ No	Other:
Unnecessary Pictures/Music	☐ Yes ☐ No	Other:

I, have audited all computers in my area.

The following discrepancies were found:

Signature: Date:

Revised: 12/12/2008 Page 1 of 1