		POLICY NUMBER 1.5.A.7	PAGE NUMBER 1 OF 4
SOUTH DAKOTA DEPARTMENT OF CORRECTIONS POLICIES AND PROCEDURES		DISTRIBUTION: Public	
		SUBJECT: Offender Use of Computers	
RELATED STANDARDS:	None	EFFECTIVE DATE: June 01, 2023	
		SUPERSESSION: 06/18/2021	
DESCRIPTION: Work and Correctional Industry	REVIEW MONTH: May	**KELLIE WASKO SECRETARY OF CORRECTIONS**	

I. POLICY

It is the policy of the South Dakota Department of Corrections (DOC) to allow offenders limited use of computers and to monitor and regulate their use to prevent unauthorized activity.

II. PURPOSE

The purpose of this policy is to outline the guidelines which allow offenders to have controlled access to state-owned computers.

III. DEFINITIONS

Intranet:

The Bureau of Information and Technology (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.

IV. PROCEDURES

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

A. Pheasantland Industries (PI) work supervisors, education staff, private sector prison industry (PSPI) supervisors, or other DOC staff supervising offenders within a DOC institution are responsible for monitoring, approving, and supervising offender access to, and use of, computers and related equipment, systems, programs, and installed hardware/software approved for offender use.

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

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

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 An offender's access to computers and related equipment, systems, and programs may be withdrawn at any time, without advance notice, reason, or cause.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

   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 offenders are present in the area.

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

   1. Offenders may be provided access to designated computers in designated areas of the institution for approved processes. Offender 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 forms or approved course work.

   2. Offender 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. Offender 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.

C. Computers located in areas of the institution accessible to offenders 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 authorized staff use).

D. Offenders 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 BIT, warden, or designee.

   1. When the BIT staff are working on a computer, offenders will be required to distance themselves from the area where the BIT staff are working.

   2. In the event an offender needs to show BIT staff the issue, the BIT staff will have the offender log in and demonstrate the issue. The offender will then be required to vacate the area.

   3. In the event offenders cannot be readily evacuated from the room, staff will schedule the repair at a time when offenders are not present.

E. Offenders employed by PI may be authorized to view approved Internet sites by PI supervisors assigned to the area for work purposes only.

F. Supervisors will ensure offenders accessing computers are made aware of all restrictions and limitations that apply to the use and access of computers, programs, or systems.

   1. Offenders permitted to use computers may not engage in inappropriate, offensive, or prohibited/illegal activity. An offender's use of a computer shall not violate institutional rules or DOC policy. Offenders should have no expectation of privacy or confidentiality when accessing any computer.

G. Offenders 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 CDs, DVDs, or memory sticks), or a typewriter with memory.

H. Offenders 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. Offenders requesting accommodation must contact the facility Americans' with Disabilities Act (ADA) coordinator.

2. Offender Access to Sensitive Information:

A. Offenders 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. Sensitive data are defined as any information not available to the public or subject to open records disclosure.

B. Offenders 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. Offenders are not permitted to have password protected screen savers, or to use passwords to protect saved documents, forms, or files. Offenders may not share user IDs.

3. Audits of Computers:

A. All computers approved for access by offenders will be audited at least quarterly by DOC supervisory staff or designee, BIT staff, or contract staff supervising the area (See Attachment 2 – *Computer Audit Report*). This includes computers at staff workstations which are accessed by offenders 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 offender abuse or unauthorized access to data or systems.
   3. The results of the audit shall be turned in to the associate warden, senior security staff, or designee.
   4. Offenders found to have used the computer in a manner contrary to policy, staff directive, or rules, are subject to disciplinary action and loss of computer privileges.

B. Offenders 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. RESPONSIBILITY
The director of Prisons is responsible for the annual review and revision of this policy.

VI. AUTHORITY
   A. SDCL §§ 43-43B-1

VII. HISTORY
May 2023
June 2021
March 2020
December 2019
August 2019
February 2019
December 2018

December 2017
December 2016
December 2015

ATTACHMENTS (*Indicates document opens externally)

1. Offender Computer Access Request*
2. Computer Audit Report*
3. DOC Policy Implementation / Adjustments

OFFENDER COMPUTER ACCESS REQUEST

Requesting Agency: _____

Agency Contact Person: _____   Phone # _____

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

List the computer applications the offender will need access to:

_____
_____
_____
_____
_____
_____

Comments: _____

_____
_____
_____
_____

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

1. The BIT reserves the right to either approve or deny this request. If the request is approved, BIT further reserves the right to audit the offender computer and offender work areas at their discretion.
2. The requesting agency understands that the offender will be assigned his/her own user ID and will be billed for this service.
3. The computer designated for offender use will be for offenders only. Sharing of user IDs to use staff computers is PROHIBITED.
4. Any changes to the computer configuration as originally designed must be requested and approved through the BIT following this same process.

_____   _____
Requesting Agency Signature   Date

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 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: _____
Unnecessary Pictures/Music	☐ Yes ☐ No	Other: _____

I, _____ have audited all computers in my area.

The following discrepancies were found: _____

_____

_____

_____

_____

Signature: _____ Date: _____