Virginia Department of Corrections

Technology

Operating Procedure 310.3

Inmate/Probationer/Parolee Access to Information Technology

Authority:
Directive 310, *Technology Management*

Effective Date: July 1, 2021

Amended: 8/1/23

Supersedes:
Operating Procedure 310.3, June 1, 2018

Access: ☐ Restricted ☒ Public ☒ Inmate

ACA/PREA Standards: 5-ACI-1F-05; 2-CI-2C-1, 2-CI-2C-2

Content Owner:	Kartik Yadav Director of Field Technology Services	*Signature Copy on File*	5/14/2021
		Signature	Date
Reviewer:	Zacc Allen Chief Information Officer	*Signature Copy on File*	5/14/2021
		Signature	Date
Signatory:	Joseph W. Walters Deputy Director for Administration	*Signature Copy on File*	5/14/2021
		Signature	Date

REVIEW

The Content Owner will review this operating procedure annually and re-write it no later than three years after the effective date.

The content owner reviewed this operating procedure in July 2022 and necessary changes are being drafted.
The content owner reviewed this operating procedure in July 2023 and necessary changes are being drafted.

COMPLIANCE

This operating procedure applies to all units operated by the Virginia Department of Corrections (DOC). Practices and procedures must comply with applicable State and Federal laws and regulations, ACA standards, PREA standards, and DOC directives and operating procedures.

Table of Contents

DEFINITIONS

Constant Sight Supervision - Each inmate or CCAP probationer/parolee is continually under the observation of a trained staff member, i.e., Corrections Officer, DOC Foreman, Supervisor, Teacher, or Virginia Department of Transportation (VDOT) Foreman.

Information Technology (IT) - Equipment, interconnected system, or subsystem used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This term includes computers, peripherals, software, firmware, similar procedures, services, and related resources.

Information Technology Initiative - Any software development or purchase, network deployment including utilizing solutions such as Internet access or wireless technology, and hardware deployment.

Inmate - A person who is incarcerated in a Virginia Department of Corrections facility or who is Virginia Department of Corrections responsible to serve a state sentence.

Password - An alphanumeric combination of characters unique to individual users that allows access to a specific computer, network, or computer system.

Personal Information - All information that describes, locates, or indexes anything about an individual including their real or personal property holdings derived from tax returns, and their education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment records, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such an individual; and the record of their presence, registration, or membership in an organization or activity, or admission to an institution; the term does not include routine information maintained for the purpose of internal office administration; nor does the term include real estate assessment information.

Proctor - An assigned school employee who is responsible for administering educational tests and examinations.

Purchased Software - Software that is purchased from a vendor for use by staff, inmates, and probationers/parolees.

Sensitive Information - Data that must be protected from unauthorized access or disclosure to safeguard the privacy and security of an individual or organization. Sensitive information can be on paper, electronic (computer or phone), or verbal.

Specific Career and Technical Education (CTE) Competencies - Tasks or actions that are appropriate in certain CTE classrooms/labs because they are part of the curriculum, but are not appropriate in other areas of the facility. The use of printers, copiers, and scanners for specific tasks in courses including but not limited to, Business, Digital Imaging, Printing, and Commercial Arts programs.

Stand-Alone/Free Standing Computer - A computer that is not attached to any network.

User - An individual assigned authorized use of Information Technology systems.

User ID - The name given to a user or account that enables access to the computer system/network.

PURPOSE

This operating procedure establishes controls that provide inmates/probationers/parolees regulated access to state owned computers for use in re-entry, education, training, and work programs in the Department of Corrections (DOC). This operating procedure includes standards that define the requirements to protect agency employees, inmates/probationers/parolees, and DOC data and information from loss, unauthorized use, modification, disclosure, or reproduction by the implementation of and compliance with controls, standards, and procedures for use of DOC information systems technology. (5-ACI-1F-05; 2-CI-2C-1, 2-CI-2C-2)

PROCEDURE

I. Inmate/Probationer/Parolee Access to Information Technology (IT)

A. IT system resources are provided for use by employees and inmates/probationers/parolees in conjunction with the operation of and participation in authorized programs and activities.

B. It is the strategy of the DOC to properly utilize technology for inmates/probationers/parolees in academic programs, Career and Technical Education (CTE) programs, re-entry programs, work programs, food services, law library, and general library services.

C. The goal of this operating procedure is to prevent the unacceptable, inappropriate, or unauthorized access, use, disclosure, alteration, manipulation, destruction, or misuse of DOC technology by inmates/probationers/parolees.

D. Inmates/probationers/parolees will only be permitted to use IT resources to perform approved job assignments, educational, instructional, research, and specific CTE duties as defined in this operating procedure.

E. All DOC employees and inmates/probationers/parolees will be responsible for complying with DOC IT system usage procedures as well as any applicable laws, including but not limited to software licensing agreements; see Operating Procedure 310.1, *Technology Management*, and Operating Procedure 310.2, *Information Technology Security*.

F. DOC employees are responsible for the appropriate use of technology by inmates/probationers/parolees and may be held accountable for the misuse of technology, which may result in disciplinary action in accordance with Operating Procedure 135.1, *Standards of Conduct*.

G. No user should have expectation of privacy when using DOC IT systems.

1. The DOC has the right to monitor all aspects of DOC IT systems, and such monitoring may occur at any time, without notice, and without the user's permission.

2. Monitoring of IT systems and data may include but is not limited to network traffic, application and data access, keystrokes, user commands, email and internet usage, and message and data content.

H. Information Technology Unit (ITU) Security must monitor use of all DOC IT systems for any activity that may be in violation of state and/or DOC policy and procedure. ITU Security will review all security settings, configurations, and patch management for security and violations of policy and procedure.

II. Controls

A. Inmate/probationer/parolee IT initiatives will not commence without prior written notification and approval of the Chief Information Officer (CIO).

B. Access to any inmate/probationer/parolee DOC IT system, resource, or data will be granted only in accordance with this operating procedure.

1. Vendors, partners, or other non-DOC entities will not be granted access to any inmate/probationer/parolee DOC IT systems without the express written permission of the CIO.

2. When access is requested, ITU Security will provide the CIO with a risk assessment.

3. If access is granted by the CIO to a vendor, partner, or non DOC entity, that entity must agree in writing to abide by all applicable laws, regulations, and DOC operating procedures prior to receiving access.

C. Inmates/probationers/parolees are prohibited from using computers assigned to a specific employee, computers used for general administrative purposes, or any technology resources tagged with VITA/NG/COV identification, i.e.; computers, laptops, tablets, printers.

D. Inmates/probationers/parolees will not have direct, unsupervised access to output and storage peripherals such as printers, scanners, DVD burners, and copy machines unless to perform specific educational or job tasks.

1. Inmates/probationers/parolees must be under constant sight supervision of DOC employees when performing such tasks. At a workstation in a controlled area with locked doors (such as Virginia Correctional Enterprises (VCE) shops or CTE classrooms) inmate/probationer/parolee use of IT equipment is allowed under the constant supervision of a trained employee.
2. No inmates/probationers/parolees will be present in any room with technology without an employee being present and maintaining constant sight supervision.
3. Inmates/probationers/parolees are strictly prohibited from possessing or using any flash drives and/or hard drives.
4. Inmates/probationer/parolees cannot have any passwords or codes to peripherals such as printers, flash drives, or copy machines.
5. DOC employees should inspect printed or copied items to guard against misuse of DOC resources.
6. Inmates/probationers/parolees must not have direct access to printers.
   a. Only employees can print to printers but inmates/probationers/parolees will have access to send prints to a print queue/print folder. Every print from the queue must be approved by an employee and then printed by an employee; or
   b. An inmate/probationer/parolee can send a print to a secured printer, but the printer needs to be in a secure non inmate/probationer/parolee access area (printer locked in a cage or printer in a locked office) with every print being retrieved by an employee and verified before the print is provided to the inmate/probationer/parolee.

E. Inmates/probationers/parolees are strictly prohibited access to encryption programs/algorithms.

F. Inmates/probationers/parolees are strictly prohibited access to programs designed to assist with hacking/cracking, or software, which can be used for hacking/cracking purposes.

G. Inmates/probationers/parolees are strictly prohibited from unauthorized internet access. Inmate/probationer/parolee internet access must be strictly controlled and monitored at all times.

H. Inmates/probationers/parolees are strictly prohibited from accessing unauthorized electronic messaging services.

I. Inmates/probationers/parolees participating in distance learning will be assigned a proctor, who will be responsible for supervising their activities and administering exams for that course. The proctor will also be responsible for making arrangements for the student to use a computer, if necessary.

J. Employees and inmates/probationers/parolees are strictly prohibited from developing, designing, or deploying ay software/programs, web applications, databases, or computer based learning materials or the delivery of such materials without the approval from the Director of Field Technology or designee.

1. Access databases or any other databases are strictly prohibited except to demonstrate the required competency in approved education competency.
2. If a database is approved for education competency, it will be used only by an inmate/probationer/parolee for their personal learning, and not outside of that program, and must be

removed at the conclusion of the program.

K. Inmates/probationers/parolees will not develop, design, or deploy software/programs, web applications, databases, computer based learning materials, or the delivery of such materials unless it is specifically required for an educational program or approved job assignment.

1. The inmate/probationer/parolee may create the educational application or materials to demonstrate the required competency and it will be used only by that inmate/probationer/parolee for their personal learning and not outside of that program.
2. Any application or materials created for an approved job assignment must be monitored by a DOC employee. Any new job assignments requiring new use of technology must be reviewed and approved by the Director of Field Technology or designee.

L. Inmate/probationer/parolee classroom aides may have access to classroom student files pertaining to a student's abilities and progress within an Academic or CTE program; however, no inmate/probationer/parolee aide will have access to any files containing sensitive or personal information.

M. The approved use of technology resources by inmates/probationers/parolees will be:

1. Limited to use for instructional/career purposes, research (such as law library), reentry, and facility work assignments as stated by the program.
2. Limited to only access stand-alone computers and isolated inmate/probationer/parolee use networks authorized and approved by the Field Technology Team.

N. Inmates/probationers/parolees are prohibited from password protecting data files.

O. Inmates/probationers/parolees accessing stand-alone computers will not have a distinct user ID or password, unless authorized by responsible DOC employees.

P. Inmates/probationers/parolees accessing freestanding isolated networks will have a user ID and password assigned to them by DOC employees.

Q. Inmates/probationers/parolees will not share user ID and passwords. Inmates/probationers/parolees found to share account information will be removed immediately from IT system access and be subject to possible program/job removal and disciplinary action.

III. Employee Supervision of Inmate/Probationer/Parolee Technology

A. In areas where inmates/probationers/parolees have access to technology, supervisors must:

1. Frequently monitor technology activity.
2. Request assistance if necessary to ensure constant sight supervision.
3. Periodically, but at least monthly, audit technology for use compliance.
4. Periodically, but at least monthly, conduct sweeps of audit computer use and audit data on computers used by inmates/probationers/parolees.
5. Provide clear instruction on the expectations regarding internet use, including how and when they can navigate and which sites they may access.
6. Provide immediate reporting and documentation to ITU Security using an *ITU Security Incident Report* 310_F6 to report any computer misuse or suspected misuse, regardless of the location.
7. At a workstation in a controlled area with locked doors (such as VCE shops or CTE classrooms) use of IT equipment is allowed under the general supervision of a trained employee. Before any inmate/probationer/parolee leaves the area, the supervising employee will account for all data storage devices and hardcopy documents.

B. Under no circumstances will DOC inmate/probationer/parolee technology (Non-VITA) leave the facility grounds except in the possession of an IT technician or with prior written approval by the Facility Unit

Head. Issues resulting from using a DOC laptop while out of the facility will not be supported by the IT Partnership and must be reported to ITU Security immediately.

C. No computers will be moved, removed, or added without prior approval from the Field Technology Team.

D. DOC inmate/probationer/parolee accessible information technology resources will not be used to intimidate or create an atmosphere of harassment based upon sex, race, religion, ethnic origin, creed, or sexual orientation.

E. Administrative accounts must have password protection and will be managed by agency IT specialists on all inmate/probationer/parolee computers. DOC employees and inmates/probationers/parolees are strictly prohibited from having access to or knowledge of any administrative account information unless required by curriculum or software execution.

F. Employee accounts that are created for DOC employee use only will not be shared with inmates/probationers/parolees under any circumstances.

IV. Hardware Requirements

A. Inmates/probationers/parolees will not have direct, unsupervised access to output and storage peripherals such as printers, scanners, DVD burners, and copy machines unless to perform specific educational or job tasks.

1. Inmates/probationers/parolees must be under constant sight supervision of DOC employees when performing such tasks. At a workstation in a controlled area with locked doors (such as VCE shops or CTE classrooms) inmate/probationer/parolee use of IT equipment is allowed under the general supervision of a trained employee.
2. DOC employees should inspect printed or copied items to guard against misuse of DOC resources.

B. The purchasing of inmate/probationer/parolee technology will follow a set of procedures and standards that is consistent with the agency's overall procurement process and acquisition strategy to acquire IT-related infrastructure, hardware, software, and services.

C. All hardware items must be inventoried and accounted for at all times by employees.

1. All computers must remain intact and in good working condition.
2. Any damaged equipment must be secured and put on surplus.
3. Surplus equipment will be removed as soon as possible from inmate/probationer/parolee access areas.
4. Hardware needed as part of curriculum must follow tool control procedures; see Operating Procedure 430.2, *Tool, Culinary, and Medical Equipment Control*.

D. Field technology assets and computers are prohibited from being used on the VITA network.

V. Software Requirements

A. Software and software documentation may only be copied as specified by the publisher. No versions of any purchased software are permitted beyond the number for which DOC has authorized licenses.

B. The installation of software products that the software publisher has designated as end-of-life (i.e. the software publisher no longer provides security patches for the product) is prohibited.

C. The installation of software products that are not compatible with current operating systems is prohibited.

D. Only software and software documentation authorized by the Field Technology Team may be installed and copied as specified by the publisher. No versions of any purchased software are permitted beyond the number for which DOC has authorized licenses.

E. Software licensing will be maintained within the purchasing unit's inventories for auditing documentation.

F. Any computer game will be solely for educational/instructional benefit and must be approved in advance by the CIO.

G. Any requests requiring additional internet access for inmates/probationers/parolees, new software, applications, websites, or any other need must be approved in advance by the CIO.

H. Any requests for inmate/probationer/parolee technology must follow the below process:

1. Smaller projects can be requested by submitting a request utilizing the *School Dude Ticketing System*.
2. Larger projects and initiatives can be requested by contacting any member of the Inmate/Probationer/Parolee Technology Steering Committee:
   a. Chief of Corrections Operations
   b. Deputy Director for Programs, Education, and Reentry
   c. Superintendent of Education
   d. CIO
   e. Director of Food Services
   f. Operations Support Manager
   g. Director of Field Technology

I. Inmates/probationers/parolees will not develop, design, or deploy software/programs, web applications, databases, or computer based learning materials or the delivery of such materials unless it is specifically required for an educational program. The inmate/probationer/parolee may create the application or materials to demonstrate the required competency and it will be used only by that inmate/probationer/parolee for their personal learning and not outside of that program.

VI. Sanctions

A. Inmates/probationers/parolees found in violation of this operating procedure will be subject to immediate removal from IT system access and be subject to possible program/job removal and disciplinary action.

B. Inmates/probationers/parolees terminated will be restricted from involvement in other computer-based programs.

C. Multiple violations could result in permanent restriction from a job or training assignment.

D. DOC employees are responsible for the appropriate use of technology by inmates/probationers/parolees and may be held accountable for the misuse of technology, which may result in disciplinary action in accordance with Operating Procedure 135.1, *Standards of Conduct*.

E. Questions concerning this operating procedure should be directed to the Field Technology Team.

REFERENCES

Operating Procedure 135.1, *Standards of Conduct*

Operating Procedure 310.1, *Technology Management*

Operating Procedure 310.2, *Information Technology Security*

Operating Procedure 430.2, *Tool, Culinary, and Medical Equipment Control*

ATTACHMENTS

None

FORM CITATIONS

ITU Security Incident Report 310_F6