Operating Procedure

Effective Date June 1, 2018	**Number** 310.3
Amended	**Operating Level** Department
Supersedes Operating Procedure 310.3 (1/1/15)	
Authority COV §53.1-10, §53.1-25	
Subject **OFFENDER ACCESS TO INFORMATION TECHNOLOGY**	**ACA/PREA Standards** None
Incarcerated Offender Access Yes ☒ No ☐ / **Public Access** Yes ☒ No ☐ / **Attachments** Yes ☐ No ☒	**Office of Primary Responsibility** Chief Information Officer

I. PURPOSE

This operating procedure establishes controls that provide offenders regulated access to state owned computers for use in re-entry, education, training, and work programs in the Department of Corrections. This operating procedure includes standards that define the requirements to protect agency staff, offenders, 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 resources by agency staff and offenders.

II. COMPLIANCE

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

III. DEFINITIONS

Constant Sight Supervision - Each offender is continually under the observation of a trained staff member i.e., Corrections Officer, DOC Foreman, Supervisor, or Teacher, or VDOT Foreman

Information Technology (IT) - Equipment or 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, and 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

Offender - An inmate, probationer, parolee or post release supervisee or other person placed under the supervision or investigation of the Department of Corrections

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

Personal Information - Information that can be used to identify, contact, or locate a person such as a social security number, personal phone number, home address, IQ scores, psychological reports, or treatment plans

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 and/or offenders

Sensitive Information - Information that is critical to the operation of the DOC or is confidential in nature

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 are specific tasks for 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

IV. PROCEDURE

A. Offender Access to Information Technology

1. Information Technology (IT) systems resources are provided for use by employees and offenders in conjunction with the operation of and participation in authorized programs and activities.
2. It is the strategy of the Department of Corrections to properly utilize technology for offenders in academic programs, career and technical education programs, re-entry programs, work programs, food services, law library, and general library services.
3. 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 offenders.
4. Offenders shall only be permitted to use IT resources to perform approved job assignments, educational, instructional, research, and specific career and technical education duties as defined in this operating procedure.
5. All DOC staff and offenders shall be responsible for complying with DOC information technology system usage procedures as well as any applicable laws, including but not limited to software licensing agreements. (see also Operating Procedure 310.1, *Technology Management*, and Operating Procedure 310.2, *Information Technology Security*)
6. DOC employees are responsible for the appropriate use of technology by offenders 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*.
7. No user should have expectation of privacy when using DOC Information Technology Systems.
   a. 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.
   b. 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.
8. CTSU Security shall monitor use of all DOC Information Technology Systems for any activity that may be in violation of state and/or DOC policy and procedure. CTSU Security shall review all security settings, configurations, and patch management for security and violations of policy and procedure.

B. Controls

1. Offender Information Technology initiatives shall not commence without prior written notification and approval of the Chief Information Officer.
2. Access to any offender DOC Information Technology System, resource, or data shall be granted only in accordance with this operating procedure.
   a. Vendors, partners, or other non-DOC entities shall not be granted access to the offender DOC Information Technology Systems without the express written permission of the Chief Information Officer.
   b. When access is requested, CTSU Security shall provide the Chief Information Officer with a risk assessment.
   c. If access is granted by the Chief Information Officer to a vendor, partner, or non DOC entity; that entity shall agree in writing to abide by all applicable laws, regulations, and DOC operating procedures prior to receiving access.

3. Offenders are prohibited from using computers assigned to a specific employee, computers used for general administrative purposes, or any technology resources tagged with VITA/NG identification i.e.; computers, laptops, tablets, printers.
4. Offenders shall 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.
   a. Offenders must be under constant sight supervision of DOC staff when performing such tasks. At a workstation in a controlled area with locked doors (such as VCE shops or CTE classrooms) offender use of information technology equipment is allowed under the general supervision of a trained employee.
   b. DOC staff should inspect printed or copied items to guard against misuse of DOC resources.
5. Offenders are strictly prohibited access to encryption programs/algorithms.
6. Offenders are strictly prohibited access to programs designed to assist with hacking/cracking, or software which can be used for hacking/cracking purposes.
7. Offenders are strictly prohibited from unauthorized internet access. Offender internet access shall be strictly controlled and monitored at all times.
8. Offenders are strictly prohibited from accessing unauthorized electronic messaging services.
9. Offenders 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.
10. Offenders shall 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 or approved job assignment.
    a. The offender may create the educational application or materials to demonstrate the required competency and it will be used only by that offender for their personal learning and not outside of that program.
    b. Any application or materials created for an approved job assignment shall be monitored by DOC staff.
11. Offender 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 offender aide shall have access to any files containing sensitive or personal information.
12. The approved use of technology resources by offenders shall be:
    a. Limited to use for instructional/career purposes, research (such as law library), reentry and facility work assignments as stated by the program
    b. Limited to only access stand-alone computers and isolated offender use networks
13. Offenders are prohibited from password protecting data files.
14. Offenders accessing stand-alone computers will not have a distinct user ID or password, unless authorized by responsible DOC staff.
15. Offenders accessing free standing isolated networks will have a user ID and password assigned to them by DOC staff.
16. Offenders will not share user ID and passwords. Offenders found to share account information will be removed immediately from IT system access and be subject to possible program/job removal and disciplinary action.

C. Staff Supervision of Offender Technology

1. In areas where offenders have access to technology, supervisors must:
   a. Frequently monitor offender technology activity

b. Request assistance if necessary to ensure constant sight supervision
c. Periodically audit offender technology for use compliance
d. Provide clear instruction on the expectations regarding internet use, including how and when they can navigate and which sites they may access.
e. Provide immediate reporting and documentation to CTSU Security using an *IT Security Incident Report* 310_F6 to report any computer misuse or suspected misuse, regardless of the location.
f. At a workstation in a controlled area with locked doors (such as VCE shops or CTE classrooms) offender use of information technology equipment is allowed under the general supervision of a trained employee. Before any offender leaves the area, the supervising employee will account for all data storage devices and hardcopy documents.

2. Under no circumstances shall DOC offender 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 CTSU Security immediately.
3. DOC offender accessible information technology resources shall not be used to intimidate or create an atmosphere of harassment based upon sex, race, religion, ethnic origin, creed, or sexual orientation.
4. Administrative accounts shall have password protection and will be managed by agency IT specialists on all offender computers. DOC staff and offenders are strictly prohibited from having access to or knowledge of any administrative account information unless required by curriculum or software execution.
5. Staff accounts that are created for DOC staff members use only shall not be shared with offenders under any circumstances.

D. Hardware Requirements

1. Offenders shall 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.
   a. Offenders must be under constant sight supervision of DOC staff when performing such tasks. At a workstation in a controlled area with locked doors (such as VCE shops or CTE classrooms) offender use of information technology equipment is allowed under the general supervision of a trained employee.
   b. DOC staff should inspect printed or copied items to guard against misuse of DOC resources.
2. The purchasing of offender technology shall follow a set of procedures and standards that is consistent with the organization's overall procurement process and acquisition strategy to acquire IT-related infrastructure, hardware, software, and services.

E. Software Requirements

1. 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.
2. 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.
3. The installation of software products that are not compatible with current operating systems is prohibited.
4. Only software and software documentation authorized by CTSU may only 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.
5. Software licensing shall be maintained within the purchasing unit's inventories for auditing documentation.
6. Any computer game shall be solely for educational/instructional benefit and must be approved in

advance by the Chief Information Officer.

7. Any requests requiring additional internet access for offenders, new software, applications, websites, or any other need must be approved in advance by the Chief Information Officer.
8. Any requests for offender technology must follow the below process:
   a. Smaller projects can be requested by submitting a request utilizing the *School Dude Ticketing System*.
   b. Larger projects and initiatives can be requested by contacting any member of the Offender Technology Steering Committee:
      i. Chief of Corrections Operations
      ii. Deputy Director for Programs, Education, and Reentry
      iii. Superintendent of Education
      iv. Chief Information Officer
      v. Director of Food Services
      vi. Operations Support Manager
      vii. Offender Technology Manager
9. Offenders shall 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 offender may create the application or materials to demonstrate the required competency and it will be used only by that offender for their personal learning and not outside of that program.
10. Offenders are strictly prohibited access to encryption programs/algorithms.
11. Offenders are strictly prohibited access to programs designed to assist with hacking/cracking, or software which can be used for hacking/cracking purposes.

F. Sanctions

1. Offenders 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.
2. Offenders terminated will be restricted from involvement in other computer based programs.
3. Multiple violations could result in permanent restriction from a job or training assignment.

G. Questions concerning this operating procedure shall be directed to CTSU Security

V. REFERENCES

Operating Procedure 135.1, *Standards of Conduct*

Operating Procedure 310.1, *Technology Management*

Operating Procedure 310.2, *Information Technology Security*

VI. FORM CITATIONS

IT Security Incident Report 310_F6

VII. REVIEW DATE

The office of primary responsibility shall review this operating procedure annually and re-write it no later than three years after the effective date.

Signature Copy on File *4/18/18*

N. H. Scott, Deputy Director for Administration Date