STATE OF WASHINGTON DEPARTMENT OF CORRECTIONS	APPLICABILITY **DEPARTMENT WIDE** FACILITY/SPANISH MANUAL		
	REVISION DATE 8/9/23	**PAGE NUMBER** 1 of 5	**NUMBER** **DOC 280.925**
POLICY	**TITLE** **ACCESS TO INFORMATION TECHNOLOGY SYSTEMS AND DATA FOR INDIVIDUALS**		

REVIEW/REVISION HISTORY:

Effective:	12/31/96
Revised:	11/4/04
Revised:	4/15/08
Reviewed:	3/17/09
Revised:	1/3/11
Revised:	4/15/11
Revised:	4/16/20
Revised:	2/11/22
Revised:	8/9/23

SUMMARY OF REVISION/REVIEW:

I.A., II.B.2., II.A., III.B., III.D., and III.D.2. - Adjusted language for clarification
I.B. III.A., and III.D.1. - Added clarifying language
I.B1. - Removed unnecessary language
Added I.B.9. that Bluetooth devices must be approved through the IT service request process

APPROVED:

Signature on file

CHERYL STRANGE, Secretary
Department of Corrections

7/7/23
Date Signed

REFERENCES:

DOC 100.100 is hereby incorporated into this policy; DOC 280.100 Acceptable Use of Technology; DOC 280.310 Information Technology Access and Security; DOC 280.515 Data Classification and Sharing; Incarcerated Individual Electronic Data File Transfer to Department (DOC) Network Procedures

POLICY:

I. The Department has established guidelines for individuals under the Department's jurisdiction to access Information Technology (IT) systems or data.

DIRECTIVE:

I. General Requirements

A. Individuals will only be granted access to IT systems or data designated for approved uses (e.g., employment, education, work programs, reentry, hearings, kiosks).

1. Individuals will not be given more privilege than is necessary.

2. Access by individuals in Prison will be physically supervised by employees/contract staff assigned to the area where the IT system/data is located.

B. Unless approved, individuals are prohibited from:

1. Direct or indirect access, either physically or electronically, to IT systems or data, including employee/contract staff workstations.

2. Using media players in Prisons other than in the recreational yard or assigned living unit. Exceptions may be approved by the Superintendent for individuals that do not have access in the living unit.

3. Accessing the internet, portable storage devices, or any system on the State Government Network (SGN) except kiosks.

a. In Prisons, Law Librarians may use portable storage devices to transfer legal data for printing.

b. In Reentry Centers, individuals may use the internet and portable storage devices not connected to the SGN for job-related purposes only (e.g., resumes, searches, applications).

4. Connecting media players to any Department IT system, except kiosks designated for media player use.

5. Performing repairs/modifications to any Department IT system/application.

6. Having elevated privileges (e.g., Administrator) or access to groups with elevated access to any Department IT system/application.

7. Personal use of state-owned IT systems.

8. Accessing personally-owned IT systems in Prison.

9. Using Bluetooth devices unless approved through the IT service request process.

II. Reentry Centers

A. Reentry Centers will assign one Department-owned, nonencrypted portable storage device to each individual for job-related purposes only. Portable storage devices will be maintained by designated employees/contract staff in a secure location and comply with DOC 280.100 Acceptable Use of Technology.

1. Devices will be clearly marked with the name and DOC number.
2. Only one device will be assigned per individual.
3. Devices will be returned to the designated employee/contract staff at the end of the approved time.

B. The Assistant Secretary for Reentry/designee will establish procedures for the acceptable use, logging, auditing, and monitoring of IT systems/data, including the issuance/control of portable storage devices.

III. System Security

A. Employees/contract staff/volunteers will follow Department-approved electronic security protocols (e.g., password protection, Department authorized credentials) and ensure necessary physical barriers (e.g., locked offices, boxes, or computer screens) to prevent unauthorized access.

B. Unless approved in Prisons, IT systems designated for use by individuals will be on closed systems (i.e., internal network) with no external access (e.g., internet, email, electronic bulletin boards) or capability to transfer data through portable storage devices to an external IT system.

C. IT systems designated for use by individuals under the Department's jurisdiction (e.g., kiosk) will only be connected to the SGN when approved by the Superintendent/Reentry Center Manager (RCM) and Chief Information Officer/designee.

D. IT systems connected to the Off State Network (OSN)/Local Area Network (LAN)/SGN will only be supported by Department IT employees/contract staff or authorized vendors (e.g., community college IT).

1. IT systems supported by the Department will have an approved, hardened DOC image with group policies to prevent compromise/modification.

2. IT systems supported by authorized vendors will use supported base images, including approved antivirus software and security patches.

3. Employees/contract staff may request for an IT system, including leased systems, to be reimaged through the IT service request process.

4. Vendors requiring physical access to IT systems will be controlled to prevent unauthorized use per DOC 280.310 Information Technology Access and Security.

E. In Prisons, the Chief Information Officer/designee may approve employees/ contract staff to use Department-owned portable storage devices to transfer data from the OSN to the SGN through the IT service request process.

1. Category 3 and 4 data per DOC 280.515 Data Classification and Sharing and data containing macros/programming code (e.g., spreadsheets, databases) will not be transferred to the SGN.

2. Employees/contract staff transferring data will follow Incarcerated Individual Electronic Data File Transfer to Department (DOC) Network Procedures located on the Department's internal website.

IV. Reporting and Compliance Monitoring

A. If unauthorized/suspicious data is found on IT systems designated for use by individuals under the Department's jurisdiction, employees/contract staff will notify the Cyber Security Unit through the IT service request process.

B. Biannually, Cyber Security Unit employees/contract staff will conduct random searches of IT systems dedicated for use by individuals under the Department's jurisdiction.

C. Every 6 months, Cyber Security Unit employees/contract staff will audit selected facilities to ensure compliance with this policy.

D. Findings will be reported in writing to the Superintendent/RCM and Chief Information Security Officer, including any unauthorized/suspicious access or data, deficiencies, and action for noncompliance.

1. The Intelligence and Investigations Unit will be notified for unauthorized/ suspicious data found on IT systems.

2. Reports will be maintained per the Records Retention Schedule.

DEFINITIONS:

The following words/terms are important to this policy and are defined in the glossary section of the Policy Manual: Data, Direct Use, Indirect Use, Information Technology System, Local Area Network (LAN), Portable Storage Device, State Government Network (SGN). Other words/terms appearing in this policy may also be defined in the glossary.

ATTACHMENTS:

None

DOC FORMS:

None