



STATE OF WASHINGTON
DEPARTMENT OF CORRECTIONS

APPLICABILITY
DEPARTMENT WIDE

REVISION DATE
1/12/16

PAGE NUMBER
1 of 7

NUMBER
DOC 280.310

POLICY

TITLE
INFORMATION TECHNOLOGY SECURITY

REVIEW/REVISION HISTORY:

Effective: 4/7/04
 Revised: 10/24/07
 Revised: 12/19/08
 Revised: 12/20/10
 Revised: 2/18/13
 Revised: 1/12/16

SUMMARY OF REVISION/REVIEW:

I.C., II.C.2., II.D.-II.G., VI.A., VII.A., and VII.B. - Adjusted language for clarification
 I.A.2. - Deleted language for clarification
 I.B., II.C.1.b., and II.D. - Added language for clarification
 II.B. - Adjusted user access procedures
 II.G.1.b. - Adjusted wireless portable technology authorization procedures in Prisons
 Added II.G.1.b.1) and 2) to clarify process of obtaining approval for bringing wireless portable technology within the secure perimeter of a Prison
 Added Section III. to address process for donating IT equipment

APPROVED:

Signature on file

12/9/15

DAN PACHOLKE, Secretary
Department of Corrections

Date Signed

 <p>STATE OF WASHINGTON DEPARTMENT OF CORRECTIONS</p> <p>POLICY</p>	APPLICABILITY DEPARTMENT WIDE		
	REVISION DATE 1/12/16	PAGE NUMBER 2 of 7	NUMBER DOC 280.310
	TITLE INFORMATION TECHNOLOGY SECURITY		

REFERENCES:

DOC 100.100 is hereby incorporated into this policy; [DOC 280.100 Acceptable Use of Technology](#); [DOC 280.515 Electronic Data Classification](#); [DOC 400.030 Security Guidelines for Wireless Portable Technology in Facilities](#); [DOC 810.015 Criminal Record Disclosure and Fingerprinting](#); [IT Security Standards](#); [OCIO IT Standards](#)

POLICY:

- I. Department Information Technology (IT) resources are Department property, and the Department is obligated to protect them. The Department will take physical and technical precautions to prevent misuse, unauthorized use, and accidental damage to IT resources, including equipment and data. IT use and access must follow state law, regulations, and Department policies and IT Security Standards.

DIRECTIVE:

- I. General Requirements
 - A. Provisions of this policy apply to any:
 1. IT devices, data, equipment, software, services, and products installed on Department resources or used within Department facilities/offices.
 2. Person with access to Department IT resources, including remote access (e.g., Virtual Private Network (VPN)).
 - B. Anyone with access to Department IT resources who violates this policy, Office of the Chief Information Officer (OCIO) IT Standards, Department IT Security Standards, or DOC 280.100 Acceptable Use of Technology may have his/her access immediately terminated and may be subject to disciplinary action.
 - C. The Assistant Secretary for Administrative Operations/designee will implement a security program, procedures, and training to promote compliance with OCIO IT Standards and Department IT Security Standards.
- II. Access Rights and Privileges
 - A. Mandatory criminal history background checks, as required in DOC 810.015 Criminal Record Disclosure and Fingerprinting, must be completed and cleared prior to granting access to IT resources.
 - B. Access rights and privileges to IT resources will require prior authorization.

 <p>STATE OF WASHINGTON DEPARTMENT OF CORRECTIONS</p> <p>POLICY</p>	<p>APPLICABILITY DEPARTMENT WIDE</p>		
	<p>REVISION DATE 1/12/16</p>	<p>PAGE NUMBER 3 of 7</p>	<p>NUMBER DOC 280.310</p>
	<p>TITLE INFORMATION TECHNOLOGY SECURITY</p>		

1. New or transferred employee user accounts and deletion of employee user accounts will be generated by the Human Resources Management System (HRMS) through the IT service request process.
 - a. If the request has not been generated before the employee needs access, the supervisor, Appointing Authority, or Logon Identification (LID) Coordinator may send an email to the Account Administrative Unit to request.
 - b. DOC 08-076 Information Technology Security Data Request will be used if immediate deletion of an employee's user account is required.
 2. The LID Coordinator will use DOC 08-012 IT-DOC Systems Access Request (SAR) to request user account creation or suspension for contract staff and volunteers.
 3. For other non-Department personnel, authorization to use IT resources requires approval from the appropriate Appointing Authority and the Chief Information Officer (CIO)/designee. Access to electronic data will be considered a release of data outside the Department and requires a data sharing agreement per DOC 280.515 Electronic Data Classification.
- C. Physical access to IT resources will be controlled to prevent unauthorized use.
1. Rooms used to house in-use network, computing, or electronic security equipment are designated as IT controlled areas and will not be used for any other purpose. Access to these areas will only be granted to personnel who require access.
 - a. Contract staff, volunteers, and other non-Department personnel that require access to IT controlled areas must be escorted by an authorized employee.
 - b. Anyone granted access to IT controlled areas must not grant access to any other person unless authorized by the appropriate authority identified by facility leadership.
 2. With the exception of authorized Department-owned mobile computing devices, only authorized IT employees/designees will connect/disconnect computing or storage devices to/from the Department computer network or a computer at the Department.

 <p>STATE OF WASHINGTON DEPARTMENT OF CORRECTIONS</p> <p>POLICY</p>	<p>APPLICABILITY DEPARTMENT WIDE</p>		
	<p>REVISION DATE 1/12/16</p>	<p>PAGE NUMBER 4 of 7</p>	<p>NUMBER DOC 280.310</p>
	<p>TITLE INFORMATION TECHNOLOGY SECURITY</p>		

3. Physical access to all Department IT equipment must be protected using an appropriate method, such as keyed door locks, proximity badges, and/or placing the equipment in an area requiring photo identification.
 4. Physical interfaces to the Department's network (e.g., network jacks) must be protected using an appropriate method, such as being located in a controlled access area, monitored to prevent offender access, and disabled if not needed.
- D. Only approved, Department-owned devices may be connected to the network. The CIO/designee may approve exceptions for contract staff, employee-owned, or non-standard Department-owned devices (e.g., other state agencies). Approval will be requested by submitting a help ticket through the IT service request process.
- E. Software installed on any Department IT resource requires CIO/designee approval and will be requested through the IT service request process.
1. Software application installations will have the required licenses and installation keys.
- F. Remote access will be controlled to prevent unauthorized use and will require authorization before installation or removal.
1. VPN services will be requested through the IT service request process.
 2. Dial-in services will be requested on DOC 08-012 IT-DOC Systems Access Request (SAR).
- G. Any computer or network equipment installed or used within a Department facility/office must be approved through the IT service request process. Approval must be requested regardless of whether or not the computing or network equipment is Department-owned and/or connects to the Department network or any other Department resource, except as follows:
1. Contract staff and vendors may use their non-Department computing equipment in Department facilities/offices for business purposes, provided they are not connected to any Department network or computing system. This includes the use of Wi-Fi (i.e., 802.11 protocols) and cellular packet Internet technology (e.g., aircards, broadband cards).
 - a. In facilities, this use requires approval from the Superintendent/Community Corrections Supervisor or designee.

 <p>STATE OF WASHINGTON DEPARTMENT OF CORRECTIONS</p> <p>POLICY</p>	APPLICABILITY DEPARTMENT WIDE		
	REVISION DATE 1/12/16	PAGE NUMBER 5 of 7	NUMBER DOC 280.310
	TITLE INFORMATION TECHNOLOGY SECURITY		

- b. In Prisons, prior written approval must be granted by the Superintendent/designee for other wireless portable technology (i.e., cameras, tablets, laptop computers) not issued by the Department to be permitted within the secure perimeter.
 - 1) DOC 21-573 Wireless Portable Technology Security Exemption Request will be submitted to the Superintendent/designee for approval.
 - 2) The individual who has been authorized must carry a signed copy of the form with the authorized device while within the secure perimeter of the facility per DOC 400.030 Security Guidelines for Wireless Portable Technology in Facilities.

- 2. Internet and network capable cell phones or smartphones are permitted in non-Prison facilities and offices. Wi-Fi capability must be disabled to the extent feasible, unless approved through the IT service request process.
 - a. Cell phones and smartphones in Prisons must comply with DOC 400.030 Security Guidelines for Wireless Portable Technology in Facilities.

III. Donated IT Equipment

- A. All donated IT equipment must be processed through local IT support, who will submit an IT service request to validate security, compatibility, and sustainability.
 - 1. The donated equipment will be validated for hardware compatibility for offender computers minimum configuration.
 - 2. All hard drives will be wiped with Department approved software (e.g., DBAN).
 - 3. All computers will be configured with the current approved hardened Department image for offenders.

IV. Authentication Process

- A. Passwords or other means of authenticating user identity will be required for access to IT computer resources. At a minimum, every user accessing a Department computer will be required to authenticate with a unique login name and password.
 - 1. Passwords will meet the IT Security Standards and guidelines for hardened passwords.

 <p>STATE OF WASHINGTON DEPARTMENT OF CORRECTIONS</p> <p>POLICY</p>	APPLICABILITY DEPARTMENT WIDE		
	REVISION DATE 1/12/16	PAGE NUMBER 6 of 7	NUMBER DOC 280.310
	TITLE INFORMATION TECHNOLOGY SECURITY		

2. Passwords will be changed at least every 120 days.
3. Passwords are confidential and must not be shared, with the exception of temporary passwords communicated to the user by authorized employees during password resets.

V. Obligation to Protect

- A. Passwords, keys, or any access control device will be stored in a secure manner and will be used only by the person to whom they are assigned.
- B. Removal of IT resources from Department premises must be authorized by the supervisor.
- C. Employees who are assigned mobile computing devices must take reasonable precautions to protect the devices from potential theft and misuse.
- D. All users with access to confidential Department data must maintain the integrity of the data per DOC 280.515 Electronic Data Classification.

VI. Obligation to Report

- A. Users will report potential intrusions, virus outbreaks, or other IT related issues to the Headquarters IT help desk.

VII. Monitoring and Auditing

- A. Under the direction of the CIO, the Cyber Security Unit will:
 1. Install computer security devices,
 2. Monitor IT resources,
 3. Audit Department use of IT resources for compliance, and
 4. Enforce IT security standards and procedures.
- B. Any IT resource may be monitored and audited for compliance by the Cyber Security Unit, including, but not limited to:
 1. All email sent, received, or stored on the Department email system. This includes personal email not related to Department business.
 2. All network traffic received, sent, or travelling across the Department's network, such as internet use and communication traffic. This includes personal use not related to Department business.

DEFINITIONS:

 STATE OF WASHINGTON DEPARTMENT OF CORRECTIONS POLICY	APPLICABILITY DEPARTMENT WIDE		
	REVISION DATE 1/12/16	PAGE NUMBER 7 of 7	NUMBER DOC 280.310
	TITLE INFORMATION TECHNOLOGY SECURITY		

The following words/terms are important to this policy and are defined in the glossary section of the Policy Manual: Mobile Computing Device. Other words/terms appearing in this policy may also be defined in the glossary section.

ATTACHMENTS:

None

DOC FORMS:

[DOC 08-012 IT-DOC Systems Access Request \(SAR\)](#)

[DOC 08-076 Information Technology Security Data Request](#)

[DOC 21-573 Wireless Portable Technology Security Exemption Request](#)