STATE OF WASHINGTON DEPARTMENT OF CORRECTIONS	APPLICABILITY **DEPARTMENT WIDE**		
	REVISION DATE 3/30/23	PAGE NUMBER 1 of 7	NUMBER **DOC 280.310**
POLICY	TITLE **INFORMATION TECHNOLOGY ACCESS AND 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
Revised:	11/27/17
Revised:	1/4/19
Revised:	10/11/21
Revised:	3/30/23

SUMMARY OF REVISION/REVIEW:

I.B., II.B.3., II.C., III.A., and III.A.1. & 2. - Removed unnecessary language

I.C., II.A., II.B.1.a., II.B.2.a., II.B.5., II.C.2., II.C.3.a. & b., II.F. & G., II.G.1., II.G.1.a.-c., III.A.3., IV.A., IV.A.1., V.A., V.A.1., VI.B.1. & 2., VII.A., and VII.C. & D. - Adjusted language for clarification

Added II.B.1. that supervisors will request access required for official duties within 7 days of an employee starting work

Added II.B.1.a.2) that accounts will be deleted 45 days after separation

Added II.B.1.b. that elevated accounts require approval and will not be granted internet/email access

Added II.B.2. that the Appointing Authority will approve contract staff/volunteer access

Added II.B.4. that individuals may be granted access per Department policy

Added II.B.3.a. that the Appointing Authority/CIO may authorize access suspension via phone/email

Removed II.C.1.c. that access to IT controlled areas will only be granted by the appropriate authority identified by facility leadership

Removed II.F.1. that VPN and dial-in services will be requested through the IT service request process

APPROVED:

Signature on file

3/2/23

CHERYL STRANGE, Secretary
Department of Corrections

Date Signed

REFERENCES:

DOC 100.100 is hereby incorporated into this policy; DOC 280.100 Acceptable Use of Technology; DOC 280.515 Data Classification and Sharing; DOC 280.925 Access to Information Technology Systems and Data for Individuals; DOC 400.030 Wireless Portable Technology in Prisons; DOC 810.015 Criminal Record Disclosure and Fingerprinting; Computer Password Standards; Computer Password Guidelines; OCIO 101 IT Standards; OCIO 141.10 Securing Information Technology Assets; Records Retention Schedule

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.

II. IT use and access must follow state law, regulations, IT security standards located on the Department's internal website, and Department policies.

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. The Chief of Staff/designee will implement a security program, procedures, and training to promote compliance with Office of the Chief Information Officer (OCIO) and Department IT security standards.

C. Failure to comply with this policy may result in corrective or disciplinary action, up to and including dismissal.

II. Access Rights and Privileges

A. Mandatory criminal history background checks must be completed and cleared per DOC 810.015 Criminal Record Disclosure and Fingerprinting before granting access to IT resources.

B. Access rights and privileges to IT resources will require prior authorization.

1. Supervisors will request access required for official duties (e.g., SharePoint, drives) within 7 days of an employee starting work.

a. Employee user accounts, including transferred employees, will be created, suspended, or deleted in the Human Resources Management System through the IT service request process.

1) If the request has not been generated before the employee needs access, the supervisor, Appointing Authority, or Logon Identification (LID) Coordinator may send a request via email to the Account Administrative Unit.

2) Accounts will be deleted 45 days after the employee's separation from the Department unless requested by the Appointing Authority/supervisor.

b. Elevated accounts (e.g., administrative functions) require Deputy of Technology/designee approval and will not be granted internet or email access.

2. The Appointing Authority will approve access for contract staff and volunteers.

a. The LID Coordinator will use the IT service request process to request user account creation, suspension, or deletion.

3. For other non-Department personnel, authorization to use IT resources requires approval from the Appointing Authority and the Chief Information Officer (CIO)/designee.

a. Access to electronic data will be considered a release of data outside the Department and requires a data sharing agreement per DOC 280.515 Data Classification and Sharing.

4. Individuals under the Department's jurisdiction may be granted access to IT resources per DOC 280.925 Access to Information Technology Systems and Data for Individuals.

5. DOC 08-076 Information Technology Security Data Request will be used to immediately suspend a user's access for any reason approved by an Appointing Authority.

a. During non-business hours, the Appointing Authority/CIO may authorize access suspension via phone or email. DOC 08-076 Information Technology Security Data Request must be submitted within 24 hours of the request.

C. Physical access to IT resources.

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.

a. Access to these areas will only be granted to personnel who require access.

b. Non-Department personnel that require access to IT controlled areas must be escorted by an authorized employee.

2. Except for 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.

3. The following will be protected using an appropriate method:

a. Physical access to all Department IT equipment (e.g., with keyed door locks, proximity badges, photo identification).

b. Physical interfaces (e.g., network jacks) to the Department's network (e.g., establishing a controlled access area, monitored to prevent access by individuals, disabled if not needed).

D. The CIO/designee may approve exceptions through the IT service request process for the connection of personal computing and/or non-standard devices, including mobile computing devices, to a Department IT system.

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 (e.g., VPN) will be controlled to prevent unauthorized use and will require authorization through the IT service request process before installation or deletion.

G. Any computer or network equipment installed or used within a Department facility/office must be approved through the IT service request process and used only for Department business.

1. Approval must be requested when the computing or network equipment is owned by the Department and/or connects to the Department network/ resources, except as follows:

a. If formally authorized in the contract, contract staff and vendors may use non-Department computing equipment in Department facilities/offices for business purposes when authorized by the Superintendent/Community Corrections Supervisor or designee.

1) Equipment will not be connected to any Department network or computing system unless it is approved by the CIO.

b. Wi-Fi capability should be disabled unless necessary to facilitate business needs.

c. Bluetooth capabilities must be disabled inside a secure perimeter unless approved through the IT service request process.

2. Mobile computing devices and cameras must comply with DOC 400.030 Wireless Portable Technology in Prisons.

III. Donated IT Equipment

A. Donated IT equipment must be processed through local IT support, who will submit an IT service request.

1. Hard drives will be wiped with Department approved software (e.g., KillDisk).

2. Donated equipment will be validated for security, hardware compatibility, and sustainability.

3. Computers used by individuals will be configured with the current, approved hardened Department image.

IV. Authentication Process

A. Authenticating user identity (e.g., passwords, tokens) will be required for access to IT computer resources and account changes (e.g., resets).

1. Passwords will comply with the Computer Password Standards and Computer Password Guidelines located on the Department's internal website.

V. Obligation to Protect

A. Access control devices (e.g., passwords, keys) will be securely stored and only used by the person to whom they are assigned.

1. Temporary passwords may be communicated to the user by authorized employees during password resets.

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

E. Users with access to confidential Department data must maintain the integrity of the data per DOC 280.515 Data Classification and Sharing.

VI. 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
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 all:

1. Email sent, received, or stored on the Department email system, including personal email.

2. Network traffic received, sent, or travelling across the Department's network (e.g., internet use, communication traffic), including use for non-business purposes.

C. Headquarters IT will annually provide supervisors a list of assigned IT resources for all employees/contract staff/volunteers under their supervision. The supervisor will verify all resources and notify Headquarters IT that the list is correct or if any discrepancies were found.

1. Inventories will be maintained by IT per the Records Retention Schedule.

VII. Security and System Updates

A. Users must connect to the Department’s network and leave their IT systems on overnight every 30 days for security updates (e.g., anti-virus software, group policies, application/information system patches).

B. Users must logon using their password at least every 45 days or the account will be disabled. Users may request IT enable their account.

C. The Appointing Authority must make the request to enable an account that was disabled as the result of DOC 08-076 Information Technology Security Data Request being submitted.

D. Accounts will be deleted if a request is not made to enable an account 45 days from the date it was disabled.

DEFINITIONS:

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

ATTACHMENTS:

None

DOC FORMS:

DOC 08-076 Information Technology Security Data Request