STATE OF WASHINGTON DEPARTMENT OF CORRECTIONS	APPLICABILITY **DEPARTMENT WIDE**		
	REVISION DATE 9/29/21	**PAGE NUMBER** 1 of 5	**NUMBER** **DOC 280.515**
POLICY	**TITLE** **DATA CLASSIFICATION AND SHARING**		

REVIEW/REVISION HISTORY:

Effective: 8/22/11
Revised: 1/8/20
Revised: 9/29/21

SUMMARY OF REVISION/REVIEW:

II.E. - Adjusted for person-centered language

APPROVED:

Signature on file

CHERYL STRANGE, Secretary
Department of Corrections

8/30/21
Date Signed

REFERENCES:

DOC 100.100 is hereby incorporated into this policy; RCW 42.52.050; DOC 130.200 Lawsuit Processing/Liability Protection; DOC 220.010 Contracts; DOC 280.510 Public Disclosure of Records; DOC 280.525 Records Management; DOC 280.925 Access to Information Technology Systems and Data for Individuals; DOC 400.100 Incident and Significant Event Reporting (RESTRICTED); Data Classification Guidelines; Data Classification Standards; Federal Information Processing Standards 140-2; OCIO 141.10 Securing Information Technology Assets; Records Retention Schedule

POLICY:

I. The Department has established guidelines to classify Department data based on sensitivity. Data classification does not apply to the release of data for:

A. Public disclosure requests, which will follow DOC 280.510 Public Disclosure of Records.

B. Discovery or litigation hold requests, which will follow DOC 130.200 Lawsuit Processing/Liability Protection.

II. Data will only be created, stored, or accessed for official use.

III. Exceptions to this policy must be authorized via email by the Chief Information Officer/ designee.

DIRECTIVE:

I. Responsibilities

A. The Chief Information Security Officer will be the point of contact for addressing:

1. Privacy and data classification issues, and
2. Data breaches.

B. Department personnel are responsible for data in their care, and will:

1. Protect data at all times to avoid unauthorized access, loss, theft, or improper disclosure,

2. Request/access, use, and release data as necessary to satisfy the business need,

3. Handle data in compliance with applicable laws and data sharing agreements, and

4. Ensure data is stored and transferred consistent with the classification category unless a more restrictive data sharing agreement is in place.

II. Data Classification and Handling

A. Data will be classified into 4 categories per the Data Classification Standards and Office of the Chief Information Officer (OCIO) 141.10 Securing Information Technology Assets:

1. Category 1 Data: Public Information - Data that can be or is currently available to the public. Requires security/protection features (e.g., password protect) but does not require authorization to be released.

2. Category 2 Data: Sensitive Information - Data that may not be specifically protected from disclosure and is for an official use. May not be released to the public unless specifically requested. Does not require authorization to be released for official state business.

3. Category 3 Data: Confidential Information - Data that is specifically protected from release by law.

4. Category 4 Data: Confidential Information Requiring Special Handling - Data that is specifically protected from release by law and:

a. Has especially strict handling requirements by statute, regulation, or agreement.

b. May result in serious consequences arising from unauthorized release (e.g., legal sanctions, endanger health/safety).

B. A data sharing agreement is required to release Category 3 or higher data outside the Department (e.g., research, public health/safety, software/database), unless authorized per statute or policy. Agreements will be established and maintained per DOC 220.010 Contracts.

1. Category 4 data requires approval from the data owner and Appointing Authority/designee before access.

2. The contract manager will conduct audits to ensure proper handling of requested data as outlined in the applicable data sharing agreement.

3. Agreements will be valid for a maximum of 2 years.

C. Data containing information from multiple classification groups will be handled based on the most restrictive classification.

D. Per the Federal Information Processing Standards 140-2 or higher:

1. Category 3 and 4 data must be encrypted when storing/transferring data.
2. Portable storage devices must be hardware encrypted when transferring data.

E. Individuals under Department jurisdiction may only have access to Category 2 or higher data through public disclosure or as authorized per DOC 280.925 Access to Information Technology Systems and Data for Individuals.

F. Data will be retained per the Records Retention Schedule and DOC 280.525 Records Management.

G. Data must be destroyed in accordance with its data classification category.

1. DOC 01-089 Records Destruction Request will be completed when destroying Category 2 or higher data.

III. Obligation to Report

A. Department personnel will immediately report to the Chief Information Security Officer any:

1. Unauthorized access or release of Category 2 or higher data.

2. Lost or stolen computing/portable storage devices containing Category 2 or higher data.

a. Lost/stolen computing/portable storage devices must also be reported per DOC 400.100 Incident and Significant Event Reporting (RESTRICTED).

B. A report must be submitted in the Incident Management Reporting System for data breaches of Category 3 or higher data.

C. Anyone affected by the unauthorized release of data will be notified per federal and state laws.

IV. Violations

A. Failure or refusal to perform assigned responsibilities or willful violation of data classification policy or standards may result in disciplinary action, up to and including dismissal.

B. Wrongful release of Department data resulting in a violation of federal or state law may be prosecuted and could result in civil or criminal penalties, including fines or imprisonment.

DEFINITIONS:

The following words/terms are important to this policy and are defined in the glossary section of the Policy Manual: Data, Data Owner, Encrypted, Official State Business, Official Use, Portable Storage Device. Other words/terms appearing in this policy may also be defined in the glossary.

ATTACHMENTS:

None

DOC FORMS:

DOC 01-089 Records Destruction Request