Data Classification Standards

DOC Policy 280.515, Data Classification

Effective: 01/31/2020 Version: 3.0

Policy Authorization

This document is authorized under DOC Policy 280.515, Electronic Data Classification and establishes standards for appropriate handling of electronic data according to its classification.

Scope

A. These standards apply to all electronic data, including email, that is created, stored or transmitted by the Department of Corrections.

For examples of data that fall under this standard, see Data Classification Guidelines.

B. All Department of Corrections staff are required to follow these standards.

C. All non-Department staff working within a Department facility such as, volunteers, business partners, contractors, and vendors are required to follow these standards.

Electronic Data Handling Requirements

A. Category 4 Data: Confidential Information Requiring Special Handling

1. *Definition.* Information that has especially strict handling requirements by statute, regulation, or law. Serious consequences could arise from unauthorized release of this data, such as the release of chemical dependency information or medical records.

2. *Internal Access.* Category 4 data has restricted access within the Department. Only staff authorized by the data owner are permitted to access, store, or release the data. This does not apply to data requested by the Public Disclosure Office.

3. *Release.* Category 4 data must not be released outside the Department unless through a formal process, such as public disclosure or through a data sharing agreement.

4. *Storage.* Requirements for storage of Category 4 data, include:

a. It must be encrypted when stored on mobile devices, such as laptops or thumb drives. Category 4 data stored inside the Department on non-mobile devices does not require encryption. However, encryption should be applied to stored data when deemed necessary by the data owner.

b. It must be stored only on Department computing devices or Department portable storage media such as, flash drives.

c. It must not be stored on personally owned computing devices or personal portable storage devices.

d. It is permissible to access Outlook Web Access (OWA) email from a personal computer. However, it is not permissible to store Department category 2, 3, or 4 data from OWA on your personal computer, your personal computing device, or your personal storage device, such as your thumb drive.

5. *Transmission.* When Category 4 data is transmitted outside of the State Government Network (SGN), it must have industry standard encryption applied, as outlined in the Data Classification Guidelines.

6. *Destruction.* Category 4 data stored on portable media must be shredded or wiped using data destruction software. Category 4 data stored on computers or servers must be wiped using approved wiping software. A Records Destruction Request Form (DOC 01-089) is required.

B. Category 3 Data: Confidential Information

1. *Definition.* Information that is specifically protected from release, by law. It includes, but is not limited to:

a. Some types of personal information about individuals as defined in RCW 42.56.590 and RCW 19.255.10 ,regardless of how that information is obtained. This may include but is not limited to an individual's social security number, staff home address, or bank account number.

b. Some information concerning employee personnel records as defined in RCW 42.56.250. This may include but is not limited to a public employee application.

c. Information regarding but is not limited to Information Technology infrastructure and computer security and telecommunications systems such as logon ids, passwords, or Internet Protocol (IP) numbers as defined in RCW 42.56.420.

2. *Release.* Category 3 data must not be released outside the Department unless through a formal process, such as public disclosure, lawful order or through a data sharing agreement.

3. *Storage. Requirements for storage of Category 3* data*, include:*

   a. It must be encrypted when stored on mobile devices, such as laptops or thumb drives. Category 3 data stored inside the Department on non-mobile devices does not require encryption. However, encryption should be applied to internal stored data when deemed necessary by the data owner.

   b. It must be stored only on Department computing devices or Department portable storage media such as, flash drives.

   c. It must not be stored on personally owned computing devices or personal portable storage devices.

   d. It is permissible to access Outlook Web Access (OWA) email from a personal computer. However, it is not permissible to store Department category 2, 3, or 4 data from OWA on your personal computer, your personal computing device, or your personal storage device, such as your thumb drive.

4. *Transmission.* When Category 3 data is transmitted outside of the State Government Network (SGN), it must have industry standard encryption applied, as outlined in the Data Classification Guidelines.

5. *Destruction.* Category 3 data stored on portable media must be shredded or electronically wiped using data destruction software. Category 3 data stored on computers or servers must be electronically wiped using data destruction software. A Records Destruction Request Form (DOC 01-089) is required.

C. Category 2 Data: Sensitive Information

1. *Definition.* Information that is intended for internal Department use and is not readily available outside the Department, such as project documents or facility rosters. More examples of Category 2 data and how it is handled can be found in the Data Classification Guidelines.

2. *Release*. Category 2 data does not require authorization to be released to the public for Official State Business.

3. *Storage.* Requirements for storage of Category 2 data, include:

   a. It does not require encryption while being stored.

b. It must be stored only on Department computing devices or Department portable storage media such as, flash drives.

c. It must not be stored on personally owned computing devices or personal portable storage devices.

4. It is permissible to access Outlook Web Access (OWA) email from a personal computer. However, it is not permissible to store Department category 2, 3, or 4 data from OWA on your personal computer, your personal computing device, or your personal storage device, such as your thumb drive.

5. *Transmission*. Category 2 data does not require encryption while being transmitted, such as through email.

6. *Destruction*. Category 2 data does not have a required method for destruction. A Records Destruction Request Form (DOC 01-089) is required.

D. Category 1 Data: Public Information

1. *Definition.* Information that is currently made available to the public by the Department, such as data posted to the DOC external Internet site. Category 1 data cannot be data that is defined as confidential or restricted, under any circumstances. More examples of Category 1 data can be found in the Data Classification Guidelines.

2. *Release*. Category 1 data does not require authorization to be released to the public for Official State Business.

3. *Storage.* Category 1 data does not require encryption.

4. *Transmission.* Category 1 data does not require encryption when being transmitted, such as through email.

5. *Destruction.* Category 1 data does not have a required method for destruction. A Records Destruction Request Form (DOC 01-089) is not required.

ELECTRONIC DATA SHARING AGREEMENTS

A. When sharing Category 3 or 4 Department electronic data with any agency, business partner, contractor, or other non-DOC entity, a Data Sharing Agreement must be in place unless otherwise prescribed by law. Data Sharing Agreements must be initiated and approved through the DOC Contracts Office. More information on how to create a Data Sharing Agreement can be found in the Data Classification Guidelines.

B. Data Sharing Agreements (such as a contract, a service level agreement, or a dedicated data sharing agreement) must address the following:

1. The data that will be shared.
2. The specific authority for sharing the data.
3. The classification of the data shared.
4. Access methods for the shared data.
5. Authorized users and operations permitted.
6. Protection of the data in transport and at rest.
7. Storage and disposal of data no longer required.
8. Backup requirements for the data if applicable.
9. Other applicable data handling requirements
10. .

When a Data Sharing Agreement exists with more strict requirements than DOC Policy or Standards, staff should follow the electronic data handling requirements outlined in the Data Sharing Agreement.

ENCRYPTION OF DATA

DOC uses industry standard algorithms validated by the National Institute of Standards and Technology. (NIST). These algorithms include, but are not limited to Advanced Encryption Standard (AES) 256 bit and higher and Triple Data Encryption Standard (3DES) 192 bit and higher. These algorithms cannot be deciphered if intercepted in transit.

APPROVED:

Debbie Kendall, Chief Information Officer	Date Signed