Guidelines

Guidance related to classification and handling of electronic data
Published: 08/22/11 Version: 1.0

SCOPE

This document is meant to serve as a reference guide for DOC Policy 280.515 Data Classification and for the Data Classification Standards. This Guideline will expand on the Standards and is meant to be recommendations.

GENERAL GUIDELINES

1. Public Disclosure/ Records Retention

These guidelines do not determine when data can be released through the public disclosure process and do not determine records retention. All requests for public disclosure should follow DOC 280.510 Public Disclosure of Records. Records released under public disclosure, to individuals, are not necessarily Category 1 data.

2. Electronic Records Discovery and Litigation Hold Requests

These guidelines do not determine when electronic data can be released for electronic records discovery or litigation hold requests. All electronic discovery and/or litigation hold requests should follow DOC Policy 130.200, Lawsuit Processing/Staff Liability Protection.

3. Inappropriate Release of Data

If category 3 or 4 data is accidentally released or released without authorization to the public, the data does not become Category 1 data or public data. The data classification and handling requirements for that data remain the same.

4. Steps for Data Release

Before you release ANY electronic data, you should:

a. Determine the classification of the data you are releasing. (link)
b. Determine what restrictions there are for its storage, transmission, and release. (link)
c. For Category 3 and 4 data, check with the DOC Contracts Office to make sure there is a Data Sharing Agreements.
d. Make sure you are authorized, by the data owner, to release the data.

5. Email

a. Email is electronic data.

b. Email containing Category 3 and 4 data must be protected with encryption.

c. To find out how to encrypt an email message see instructions on How to Email Encrypted Data.

6. Encryption

Requesting Encryption

For help applying encryption or identifying the appropriate encryption method, contact the IT Customer Assistance Center.

Desktops and Laptops

When encryption is required, for desktops and laptops, the Department uses GuardianEdge Hard Disk Encryption. The following may be reasons to encrypt a desktop or laptop:

- It is a mobile device, such as a laptop that stores or processes Category 3 or 4 data.
- It stores data that if lost or stolen may endanger the safety of others or would result in a high financial risk to the Department.
- It is assigned to an agency executive.
- It is located in a high-risk area such as an unsecured office or outstation in an inner-city area.

Portable Storage Devices

For encryption of portable storage devices such as thumb drives, staff should use the encryption tool that is supplied with the device. If the portable storage device was not supplied with an encryption tool, follow the process for requesting encryption.

DOC data should only be stored on DOC devices.

Microsoft Documents

For documents or files created in Microsoft Office , including Word, Excel, Publisher, PowerPoint, and Access, staff should use the built-in encryption tool.

PDF Documents

For documents created in Adobe Acrobat, staff should use the built-in encryption tool.

Encryption of batch files and data

When preparing batch files and data for transmission or release, staff may employ methods such as:

- Transfer files through a Secure File Transfer Protocol (SFTP) service.
- Encrypt files and transfer on portable media such as CD, DVD, or DOC approved portable storage device.

Receipt of Encrypted Data

When confirmation of receipt of encrypted data is required the sending party will email or call the receiving party and let them know. You can use any of the following methods to confirm receipt:

- The receiving party will email the sending party that they received the encrypted data, or
- The receiving party will contact the sending party and let them know they have received the encrypted data.
- If the receiving party did not receive the data, you do not need to notify the Chief Information Security Officer (CISO) regarding misdirected data since the data is encrypted and cannot be deciphered by an unauthorized person. However, before resending the encrypted data, do the following:
    - Reconfirm the Internet or email address of the receiving party.
    - Send non-confidential test data to the address to confirm with the receiving party that the address is valid.
    - After confirmation of receipt of the test data, resend your encrypted package.

7. Offender Access

Under all circumstances, except public disclosure requests, offender access to electronic data should follow DOC 280.925 Offender Access to Electronic Data.

Staff should not grant offenders access to Category 2, 3, or 4 Department electronic data including displaying information such as offender chronos on a computer screen. Offenders may access DOC electronic data through information systems or components designed for their use such as, Genie kiosks.

8. Data Sharing

To check to see if there is an existing Data Sharing Agreement or to request a new Data Sharing Agreement you need to check the DOC Contracts SharePoint Site. Go to InsideDoc>Administrative Services>Contracts. Scroll to the bottom of the page. Click on the Contracts SharePoint Site link. If you do not have permission you will need to click on the Request Access link. Then type in your request and click on the Send Request button.

9. How to Report Data Breaches

If you know that DOC Category 3 or 4 data has been lost, stolen, misdirected, accessed without authorization, or released without authorization, report the data breach through the Incident Management Reporting System (IMRS). When reporting data breaches, you should include:

- A description of how and when the data was lost.
- A description of the data that was lost.

10. How to Destroy Data

Category 2, 3, and 4 data all require a Records Destructoin Request Form (DOC 01-089) before being destroyd. Category 3 and 4 data require shredding or electronic wiping using data destruction software. For help obtaining or locating the appropriate destruction method, contact the IT Customer Assistance Center.

CLASSIFYING YOUR DATA

See the Data Handling Quick Reference Guide for examples of each data type

1. Identifying Category 4 Data

If you can answer 'yes' to any of the questions below, your data is most likely Category 4:

- If released, would the data pose a risk to public safety?
- If released, would the data pose a risk to staff or offender safety?
- Would the data put an employee's personal financial information at risk?

2. Identifying Category 3 Data

If you can answer 'yes' to any of the questions below, your data is most likely Category 3:

- Is the data specifically protected by law or statute?
- Does the data include computer network information?
- Does the data include personal employee information such as home address or date of birth?

3. Identifying Category 2 Data

If your data was created for internal department use and::

- If released, this data does not pose a risk to the Department or public safety, and;
- The data is not specifically protected by law or statute

Your data is most likely Category 2

4. Identifying Category 1 Data

If you can answer 'yes' to any of the following questions, your data is most likely Category 1:

- Has the Department made this data available to the general public?
- Is the information available on the DOC Internet Site?

If you are unable to categorize your data or you have questions about how to categorize your data, contact the Chief Information Security Officer at DOC DL IT Security.

DATA HANDLING QUICK REFERENCE GUIDE

Category 1	Category 2	Category 3	Category 4
Information about services provided by the Department, like Family and Friends Services and Victim Services Programs	Work schedules, digital calendars, meeting agendas and minutes (but not for health care)	Social Security Numbers	Personal credit card and bank account numbers.
Department informational brochures	Organizational charts and facility or staff rosters	Staff's computer logon IDs	Facility blueprints or physical security details.
Facility Addresses, driving directions and visiting information	Project documents, such as schedules, charters or training materials	Employee personal information such as home address, photos, age, or date of birth.	Any computer login ID with a Password.
Public news releases	Desk manuals and other instructional documents (but not COACH or Tactical Manuals)	Computer infrastructure information such as network diagrams, computer names, or IP addresses	Individual public health information which may endanger the person's safety or welfare such as, HIV or other communicable disease status.
Non-restricted DOC Policies	Purchasing and Leasing Information	Performance evaluations and attendance records	Identity and personal information related to victims or witnesses.
Incarcerated offender name, DOC number, location, DOB	Offender case information such as, conviction history, earned release date (ERD), conditions and terms of supervision,	Offender case information such as, non-conviction criminal history information, arrests, medical information, psychiatric evaluation, drug and alcohol treatment information.	Offender gang affiliations and ongoing PREA or Staff Sexual Misconduct investigation information
Data posted on www.doc.wa.gov	OMNI Reports	Incident related photos or surveillance videos.	
		Liberty documentation images, Email and data from Incident Management Reporting System (IMRS).	

	Category 1	Category 2	Category 3	Category 4
RELEASE	Staff may release this data for official Department business without approval.	Staff may release this data for official Department business. Requests for this data for non-business purposes should be referred to Public Disclosure.	Releasing this data requires a Data Sharing Agreement to be in place before releasing the data. These agreements should be approved and be on file with DOC Contracts unless release of the data has already been approved by DOC Policy. Staff may release this data as defined in the Data Sharing Agreement. Any release of this data outside of a Data Sharing Agreement or DOC Policy, must follow Section V. Exceptions of the Data Classification Policy, except for public disclosure.	Releasing this data requires a Data Sharing Agreement. These agreements should be approved by the appropriate Assistant Secretary and on file with DOC Contracts. Staff should document the release of this data and receive approval from the Appointing Authority via email. The release of this data should occur as defined in the Data Sharing Agreement. Any release of this data outside of a Data Sharing Agreement, must be approved by the Assistant Secretary, except for public disclosure.

DATA HANDLING QUICK REFERENCE GUIDE

	Category 1	Category 2	Category 3	Category 4
STORAGE	This data does not need to be encrypted when stored.	This data does not need to be encrypted when stored.	This data requires encryption when stored on mobile devices like thumb drives or laptops. This data does not need to be encrypted when stored inside the DOC Network.	This data requires encryption when stored on mobile devices like thumb drives or laptops. This data does not need to be encrypted when stored inside the DOC Network.
TRANSMISSION	This data does not require encryption when being transmitted.	This data does not require encryption when being transmitted.	This data should be encrypted when being transmitted outside the State Government Network (SGN). Data can be transmitted using built-in encryption tools like those in Microsoft Office products, Adobe Acrobat, and other programs. Data transmission can be encrypted using Secure File Transfer Protocol (SFTP). Data can be stored on encrypted media such as a thumb drive or CD that has had encryption applied.	This data should be encrypted when being transmitted outside the State Government Network (SGN). Data can be transmitted using built-in encryption tools like those in Microsoft Office products, Adobe Acrobat, and other programs. Data transmission can be encrypted using Secure File Transfer Protocol (SFTP). Data can be stored on encrypted media such as a thumb drive or CD that has had encryption applied.

DATA HANDLING QUICK REFERENCE GUIDE

	Category 1	Category 2	Category 3	Category 4
DESTRUCTION	This data does not require special handling when being destroyed. Records Destruction Request Form (DOC 01-089) not required.	This data does not require special handling when being destroyed. Records Destruction Request Form (DOC 01-089) is still required.	Portable media, such as CDs used to store this data should be shredded when no longer necessary. Prior to disposing of hardware that is used to store this data, the device should be wiped by IT using a tool such as DBAN. Records Destruction Request Form (DOC 01-089) is still required.	Portable media, such as CDs used to store this data should be shredded when no longer necessary. Prior to disposing of hardware that is used to store this data, the device should be wiped by IT using a tool such as DBAN. Records Destruction Request Form (DOC 01-089) is still required.