Data Classification Standard [1]

Version 2.2

Author

University IT Security Office (ITSO)

Authority

Duke University Chief Information Officer
Duke University Chief Information Security Officer

Definitions

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Steward</td>
<td>The individual who has accountability and executive authority to make decisions about a specific set of data. The Data Steward is the role of the person who is responsible for: the function that uses the information, determining the levels of protection for the information, making decisions about appropriate use of the information, classifying the information, and for the business results of the system or the business use of the information.</td>
</tr>
<tr>
<td><strong>Data Manager</strong></td>
<td>The persons who are responsible for implementing the controls the Data Steward identifies.</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Data Users</strong></td>
<td>The persons who actually &quot;touch&quot; the information (enter, delete, even read).</td>
</tr>
<tr>
<td><strong>Protected Data</strong></td>
<td>Any information classified as either Sensitive or Restricted by the Duke standard.</td>
</tr>
</tbody>
</table>

**Purpose**

While performing their assignments at Duke University, all users will likely come into contact with many types of information or data, some of which may be considered Sensitive or Restricted according to Duke’s data classifications and regulatory requirements. It is the responsibility of Duke to implement procedures and standards to help users protect their data.

The purpose of this standard is to define Duke’s data classifications and data types for each classification. Please be aware that applicable federal and state statutes and regulations that guarantee either protection or accessibility of certain data records will take precedence over this standard. These regulations and laws include:

- FERPA (which protects many kinds of student educational data)
- HIPAA (which protects personal health information)
- HHS Title 45 CFR Part 46 - Protection of Human Subjects (which applies to research supported by a federal agency)
- NC GS 125-19 (which protects the privacy of library patrons’ records)
- NC Identity Theft Protection Act (which defines personal information and requires notification if a data breach occurs)
- PCI (which protects credit card holder information)

**Scope**

This standard applies to all data collected, stored, or processed by university staff or by third parties via contractual agreements with university departments or other organizational groups.
Standards

Data and Risk Classifications

To assist in handling information in any format, Duke as defined three classes of information: Sensitive, Restricted, and Public. Each classification tier requires a specific level of technical and procedural security controls due to the risk impact if the information is mishandled. These Technical Standards may be found [here](#2).

Data that has not yet been classified should be considered Restricted until the Data Steward assigns the classification.

The classification of data is independent of its format. For example, if personal health information is revealed in a video recording of a lecture, then that video file should be classified as Sensitive. If paper credit card receipts are stored, then they should be classified as Sensitive.

Questions about classifying or handling the data should be directed to the Data Steward, your supervisor, your departmental security liaison, or the University IT Security Office. The departmental security liaisons, in coordination with the IT Security Office, can assist departmental users in developing appropriate controls and processes to protect Sensitive or Restricted data.

<table>
<thead>
<tr>
<th>Data Category &amp; Risk</th>
<th>Definition &amp; Access</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive  (High)</td>
<td>Sensitive data is the most restrictive data classification category and is reserved for data that Duke is either required by law to protect, or which Duke protects to mitigate institutional risk. Explicit institutional approval is needed in order to receive access to Sensitive data.</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
|                    | • Social Security numbers [3]  
|                    | • Credit Card numbers [4]  
|                    | • PHI (HIPAA - protected data)  
|                    | • FERPA-protected data (non-directory information)  
|                    | • Prospective student data  
|                    | • Donor data  
|                    | • CUI (controlled unclassified information)  
|                    | • Contract data  
|                    | • Financial data  
|                    | • HR data  
|                    | • Physical Plant details  
|                    | • Research data  
|                    | • Certain management information |
| Restricted  (Medium) | Restricted information is the default data classification category. Restricted data is data that is not necessarily for public consumption, but also does not fit into the Sensitive category. Duke may have a proprietary obligation to protect Restricted data, but disclosure would not significantly harm the university. Access to Restricted data elements is determined by business process needs. |
|                    | • Anything not Public or Sensitive  
|                    | • Data that is restricted to specific groups  
|                    | • Research detail that is not classified as Public or Sensitive  
|                    | • Library transactions  
|                    | • Financial transactions not including Sensitive data  
|                    | • NDA data |
Public (Low)

All other data, which can be accessible to the general public. Information that has been approved for publication, such as a press release or information published on www.duke.edu [5]. (This does not include information that has been disclosed accidentally.) Access includes Duke University affiliates and general public.

• Public-facing websites
• Campus Maps
• FERPA directory data
• Faculty/Staff directory data
• Research data

Roles and Responsibilities

To handle data properly, Duke faculty and staff need to be aware of the classification of a piece of information and the associated risks in order to understand how to properly and securely handle the information.

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Steward</td>
<td>The individual who has accountability and executive authority to make decisions about a specific set of data. The Data Steward is the role of the person who is responsible for: the function that uses the information, determining the levels of protection for the information, making decisions about appropriate use of the information, classifying the information, and for the business results of the system or the business use of the information.</td>
</tr>
<tr>
<td>Data Manager</td>
<td>The persons who are responsible for implementing the controls the Data Steward identifies. The data managers are responsible for ensuring that the appropriate security controls are in place on systems containing Sensitive and Restricted data (see Technical standards).</td>
</tr>
<tr>
<td>Data Users</td>
<td>The persons who actually &quot;touch&quot; the information (enter, delete, even read). Users are responsible for taking reasonable precautions against disclosure of data they have access to. Users should not grant access to data without proper authorizations from the Data Steward.</td>
</tr>
</tbody>
</table>
It is the recommendation of the Duke University IT Security Office that all campus units that collect and store information document their policies, procedures, and architectures that pertain to collection and storage, regardless of the information format (electronic, paper, image, sound, etc.). This documentation should detail account creation and deletion, records retention and destruction, backup retention and destruction, and any other relevant procedures.

**Sensitive Server Registration**

The University IT Security Office tracks servers containing Sensitive data. Campus units are asked to document which of their servers contain Sensitive and Restricted data, and update the ITSO on which systems contain Sensitive information.

**Incident Reporting**

Report the misuse or compromise of systems that handle, store, or propagate Sensitive data IMMEDIATELY to security@duke.edu [6].

**Review Frequency:** Annually

**Updated:** 07/14

**In Compliance with:**
Duke University Technical Standards [2]

**Document Type:** Policy
**Topic:** Data Security
**Applicable To:** Duke Health

**Source URL:** https://security.duke.edu/policies/data-classification-standard
Links
[1] https://security.duke.edu/policies/data-classification-standard
[2] https://security.duke.edu/policies-standards-procedures?keys=&amp;document_type_value=2&amp;topic_tid=All&amp;duke_dept_value=All
[6] mailto:security@duke.edu
[7] https://security.duke.edu/policies/acceptable-use