Data Security Policy [1]

Version 1.1

Authority

Duke University Chief Information Officer
Duke Health Chief Information Officer
Duke University Chief Information Security Officer
Duke Health Chief Information Security Officer

Purpose

As stewards of Duke’s resources, we are expected to exercise sound judgment using data prudently and ethically. Additionally, various federal and state laws impose obligations on Duke, including, but not limited to HIPAA [2], FERPA [3], FISMA, the NC Identity Theft Protection Act and PCI-DSS [4]. Grants and contracts may impose requirements for the protection and preservation of associated data. As a result, it is important that all data (with appropriate priority given to Sensitive and Restricted data\(^1\)), are reasonably and appropriately managed to maintain data integrity, availability, and when required, confidentiality to protect against accidental or unauthorized access, modification, disclosure and destruction.

Special consideration to research data is warranted, as some research data may be classified as public and open, while other research data may require greater protections due to the sensitivity of the data. This policy is not intended to impede the use or sharing of unrestricted (e.g. public) research data, but rather provide the framework for determining where controls are required for sensitive or protected research.
While every reasonable effort has been made to document the appropriate protections and responsibilities for data, it is possible that a specific case or issue may not be addressed or may raise a question. In such a case, the department or user is strongly encouraged to reach out to the appropriate security office (see Data Procedures section) for assistance determining the appropriate course of action.

Policy

Data Classification

Each user is responsible for knowing Duke’s data classification standard and the associated risks in order to understand how to classify and secure data. Duke data classifications are Sensitive, Restricted or Public. Sensitive data requires the highest level of security controls, followed by Restricted and then Public. A link to the Duke Data classification standard is provided in Appendix B.

Data Access & Usage

Consistent with its classification, data shall be accessible to authorized users to fulfill their duties and responsibilities.

Data Maintenance & Disposal

A user with authorized access to data will maintain the security (confidentiality, integrity and availability) of the data, consistent with Duke requirements. When Sensitive and Restricted data must be disposed of, to the extent permissible under law, that disposal must be in a manner that renders it unrecoverable. Only authorized services can be used for storage of Duke sensitive data; an approved list is available online: https://security.duke.edu/policies/duke-services-and-data-classification [5]. Should you have questions about use of a service to store sensitive data, we encourage you to contact the Security Offices at security@duke.edu [6].

Data Encryption

Sensitive data must be encrypted during network transmission, and if stored on mobile devices or removable media like a USB thumb drive. Any exceptions must be documented via a ServiceNow ticket and filed with the Duke IT Security Office or Duke Health Information Security Office for review. Additional information on encryption requirements for campus departments may be found here [7], while additional guidance for Duke Health may be found here.

Data Procedures

All Data Stewards at Duke must document their procedures, and other requirements that pertain
to the security of the data for which they are responsible. This documentation must comply with all Duke standards regarding data. The university Information Technology Security Office and Duke Health Information Security Office can be reached at security@duke.edu.

Incidents

Any security incident or suspected security incident involving a Duke system, especially those containing Sensitive or Restricted data, must be reported immediately to the University IT Security Office or Duke Health Information Security Office, Data Manager and Data Steward, as applicable, pursuant to the incident management procedures referenced in Appendix B.

Violations

Any violation of federal or state law, or this or other applicable policies, standards or contracts may result in corrective action up to and including dismissal/termination.

Responsibilities

Set forth in Appendix A are typical responsibilities for the executive officers for Duke University and Duke Health, Data Stewards, Data Owners, Data Managers and users. An individual may fulfill the responsibilities of more than one position. Data stewards and data managers also qualify as users with regard to fulfilling their duties and responsibilities on behalf of Duke.

Scope

This policy is intended to safeguard all data, with priority given to Sensitive and Restricted data.

This policy applies to all trustees, senior officials, faculty, staff, students, subcontractors, or other persons who may have access to Duke data. See Definitions below.

This policy applies to all data on Duke’s communications resources, whether those resources are individually controlled, shared, stand-alone, or networked. It applies to all computers (including mobile devices) and communications facilities owned, leased, operated, or provided by Duke, or that are otherwise connected to Duke’s communications resources. This policy also applies to all personally owned devices used to store, process, or transmit Duke data.

Definitions
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data</strong></td>
<td>Any items of information that are received, created, collected, maintained, accessed, provided by a third party (e.g., as part of a sponsored research project or other collaboration) and used, transmitted or disclosed for the fulfillment of the mission of Duke, whether in electronic, paper or other format.</td>
</tr>
<tr>
<td><strong>Data Steward</strong></td>
<td>The individual who has accountability and authority to make decisions about a specific set of data, and is responsible for defining the access and protection rules for a specific set of data.</td>
</tr>
<tr>
<td><strong>Data Manager</strong></td>
<td>The individual who is responsible for maintaining security controls to protect data established under law and by this and any other Duke requirements.</td>
</tr>
<tr>
<td><strong>FERPA</strong></td>
<td>Family Educational Rights and Privacy Act. The policy permits students to inspect their education records, limits disclosure to others of personally-identifiable information from education records without students’ prior written consent, and provides students the opportunity to seek correction of their education records where appropriate.</td>
</tr>
<tr>
<td><strong>FISMA</strong></td>
<td>Federal Information Security Management Act. Mandates security for information systems subject to federal contracts.</td>
</tr>
<tr>
<td><strong>HIPAA</strong></td>
<td>Health Insurance Portability and Accountability Act. Restricts the release of health-related data about individuals. The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information.</td>
</tr>
<tr>
<td><strong>NC ITPA</strong></td>
<td>North Carolina Identity Theft Protection Act. Requires protection of individually identifiable data and mandates notification of individuals in the case of breaches and disposal of unneeded personal information.</td>
</tr>
<tr>
<td><strong>PCI-DSS</strong></td>
<td>Payment card industry data security standards. Rules for limiting access to financial information.</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Security Incident</strong></td>
<td>An adverse event in an information system. An incident may include a violation of an explicit or implied security policy, attempt to gain unauthorized access, unwanted denial of resources, unauthorized use, or changes without the owner’s knowledge, instruction or consent.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>The individual who creates, accesses, processes, enters, reads, deletes or otherwise &quot;uses&quot; data.</td>
</tr>
</tbody>
</table>

**APPENDIX A: Roles and Responsibilities**

The duties and responsibilities listed below are provided to safeguard all data, with priority given to Sensitive and Restricted data, consistent with the fulfillment of Duke’s mission.

**Executive Officers**

The Executive Officers of Duke University and Duke Health who have oversight responsibility for establishing guidance and strategies for the protection of data through the Information Security Steering Committee (ISSC) and the Duke Health Privacy and Security Steering Committee (PSSC), and may delegate their implementation to the appropriate data steward(s).

**Data Steward**

A data steward is typically responsible for:

a. Classifying data in accord with the data classification standard.
b. Apprising the applicable Chief Information Security Officer of material issues related to the implementation of this policy.
c. Maintaining the accuracy and completeness of data for which they are responsible whether that data is contained in a centrally managed system or in a locally managed system.
d. Documenting and evaluating controls to maintain security, confidentiality, integrity, availability, and access of/to data that is in the custody of the data steward.
e. Designating a data manager(s) to implement security controls for the data in the custody of the data steward and providing necessary guidance and management assistance to the data manager(s).

f. Communicating data protection procedures to each data manager and user who is granted access to data in the custody of the data steward.

g. Monitoring compliance with applicable law, and with Duke policies, standards or contracts.

h. Facilitating consensus on data definitions, data usage, etc.

i. Fulfilling the principles and requirements set forth in this policy.

Data Manager

A data manager is typically responsible for:

a. Apprising the data steward of material issues related to the implementation of this policy.

b. Collaborating with the University IT Security Office or Duke Health Information Security Office, as necessary, to implement directives assigned by the data steward.

c. Ensuring that security controls are in place on systems containing Sensitive and Restricted data.

d. Data backup and recovery.

e. Being aware of relevant laws and of applicable Duke policies, standards or contracts.

f. Detecting and responding to violations and vulnerabilities.

g. Fulfilling the principles and requirements set forth in this policy.

User

In addition to the duties and responsibilities described in the policy, a user is typically responsible for:

a. Identifying, on a regular basis, data that qualifies as Sensitive or Restricted and reporting its existence to the appropriate data manager.

b. Following the security controls established by the data steward or data manager, as applicable.

c. Maintaining the security of data in her/his possession or control appropriate for the classification level of such data.

d. Avoiding disclosure of Sensitive or Restricted data to any unauthorized person without the documented permission of the data steward or manager.

e. Fulfilling the principles and requirements set forth in this policy.

Appendix B: References and Links

Acceptable Use Policy [8]
Account or Data Access Policy [9]
Application Risk Assessment
DMCA
Duke University Vulnerability Management Policy
Duke HR Payroll Data Policy: http://www.hr.duke.edu/forms/secure/hrdata_policy.php
Duke Corrective Action Policy:
http://www.hr.duke.edu/policies/expectations/standards/corrective_action...
Duke Data Classification Standard
Faculty Handbook: http://provost.duke.edu/faulty-resources/faculty-handbook
FERPA: http://registrar.duke.edu/student-records
HIPAA: http://www.hhs.gov/ocr/privacy/
Human Resource Policies: https://www.hr.duke.edu/policies/
Incident Management Procedures
NC Identity Theft Protection Act:
PCI-DSS: https://www.pcisecuritystandards.org/security_standards
Policies for the Responsible Conduct of Research: https://ors.duke.edu/orsmanual/policies-responsive-conduct-research
Policy on Social Security Number Usage
(Campus) http://security.duke.edu/sites/default/files/documents/DUHS%20SSNs%202021...
(Health System)
Staff Handbook: http://www.hr.duke.edu/policies/staff_handbook.pdf

1As defined in the Duke Data Classification Standard located here.

Review Frequency: Annually
Updated: 09/13
Updated: 05/14
Updated: 10/15

In Compliance with:
Duke University Acceptable Use Policy

Document Type: Policy
Topic: Data Security
Applicable To: Duke Health
Source URL: https://security.duke.edu/policies/data-security

Links
[1] https://security.duke.edu/policies/data-security