Duke University Data Security Policy
Version 1.0

Authority:
Duke University Chief Information Officer
Duke Medicine Chief Information Officer
Duke University Chief Information Security Officer
Duke Medicine Chief Information Security Officer

1. Purpose
Duke University and Duke University Health System (Duke) are dedicated to excellence in education, research, and patient care. Data is a vital component of Duke’s operations and it is important to ensure that authorized individuals can access data appropriately.

As stewards of Duke’s resources, we are expected to exercise sound judgment in the performance of our responsibilities and to ensure that data is used prudently and ethically. Numerous federal and state laws and industry standards assign responsibility for the correct and appropriate use of data, including, but not limited to HIPAA, FERPA, FISMA, the North Carolina Identity Theft Protection Act and PCI-DSS. In addition, research grants and contracts may set further requirements on how research data is to be protected and preserved. As a result, it is important that all data (with appropriate priority given to Sensitive and Restricted data1), are managed to ensure confidentiality, integrity and availability, and to protect against accidental or unauthorized access, modification, disclosure, and destruction.

While every 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 encouraged to reach out to the appropriate security office (see Data Procedures section) for assistance determining the best course of action.

2. 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 enable them to fulfill their duties and responsibilities on behalf of Duke.

Data Maintenance & Disposal

1 As defined in the Duke Data Classification Standard located at: https://security.duke.edu/sites/default/files/documents/Duke%20Data%20Classification%20Standard.pdf
A user with authorized access to data will maintain the security (confidentiality, integrity and availability) of the data on behalf of Duke. When Sensitive and Restricted data must be disposed of, to the extent permissible under law that disposal must be in a manner that will render it unrecoverable.

**Data Procedures**
Each department at Duke should document its policies, procedures and architectures that pertain to the security of data. This documentation should comply with all Duke technical, administrative, business and other standards for protecting data. Security office contacts are provided below.

University Information Technology Security Office: security@duke.edu
Duke Medicine Information Security Office: infosec@dm.duke.edu

**Incidents**
Any security incident or suspected incident involving a Duke system, especially those containing Sensitive or Restricted data must be reported immediately to the University IT Security Office or Duke Medicine 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 Duke policy or standard may result in an adverse employment action or the imposition of personal liability, or both, as well as in damages imposed on Duke as an institution.

**Responsibilities**
Set forth in Appendix A are typical responsibilities for the executive officers for Duke University and Medicine, data steward, data owner, data manager and user. 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.

**3. Scope**
This policy is intended to ensure that all data, with appropriate priority given to Sensitive and Restricted data, are managed and secured as institutional assets consistent with the fulfillment of Duke’s mission.

This policy applies to all trustees, senior officials, faculty, staff, students, subcontractors, visitors, visiting scholars and any other agent of Duke who qualifies as a user. 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.

**4. Definitions**
Data. Any items of information that are created, collected, maintained, accessed, provided by a third party (e.g., as part of a sponsored research project or other collaboration) and used for the fulfillment of the mission of Duke, whether in electronic, digital or paper format.

Data Steward. The individual who has accountability and executive 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.

Data Manager. The individual who is responsible for maintaining security controls to protect data established under law and by this and any other Duke policy and standard.

User. The individual who creates, accesses, processes, enters, reads, deletes or otherwise "uses" data.
APPENDIX A: Roles and Responsibilities

The duties and responsibilities listed below are provided to ensure that all data, with appropriate priority given to Sensitive and Restricted data, are managed and secured as institutional assets consistent with fulfillment of Duke’s mission.

Executive Officers
The Executive Officers of Duke University and Duke University Health System who have oversight responsibility are responsible for establishing guidance and strategies for the protection of data through the Information Security Steering Committee (ISSC) 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. Ensuring that the applicable Chief Information Security Officer is apprised 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 ensure security, confidentiality, integrity, availability, and appropriate 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 and best practices designed to protect data from unauthorized access or disclosure.
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. Ensuring that the data steward is apprised of material issues related to the implementation of this policy.
b. Collaborating with the University IT Security Office or Duke Medicine Information Security Office, as necessary, to implement directives assigned by the data steward.
c. Ensuring that the appropriate security controls are in place on systems containing Sensitive and Restricted data.
d. Ensuring the backup and recovery of data.
e. Being aware of relevant laws and of the Duke policies, standards and guidelines regarding data security.
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 security appropriate for the classification level of data to ensure the security, confidentiality, integrity, and availability of data in her/his possession.
d. Avoiding disclosure of Sensitive or Restricted data to any unauthorized person without the explicit permission of the data steward or manager.
e. Fulfilling the principles and requirements set forth in this policy.
Appendix B: References and Links

Duke Data Classification Standard:

Policies for the Responsible Conduct of Research:
https://ors.duke.edu/ormanual/policies-responsible-conduct-research

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.php

Policy on Social Security Number Usage:
http://www.security.duke.edu/duke-policy-ssn-usage (Campus)
http://security.duke.edu/sites/default/files/documents/DUHS%20SSNs%202011.pdf (Health System)

Acceptable Use Policy:
http://security.duke.edu/duke-acceptable-use-policy

Duke University Vulnerability Management Policy:

Account or Data Access Policy:
https://security.duke.edu/account-or-data-access-policy

FERPA:
http://www.registrar.duke.edu/registrar/studentpages/student/ferpa.html

DMCA:
http://security.duke.edu/dmca-contact

Application Risk Assessment:

Faculty Handbook:
http://www.provost.duke.edu/policies/fhb.html

Staff Handbook:
http://www.hr.duke.edu/policies/staff_handbook.pdf

Human Resources Policies:
https://www.hr.duke.edu/policies/

Incident Management Procedures:
http://security.duke.edu/incident-management
Review Frequency: Annually
Updated: 2/13

In Compliance with:
Duke University Acceptable Use Policy