

Information Classification Framework

Version 2, updated September, 2009

Duke University

Faculty and Staff Responsibility for Handling University Data

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. It is important that faculty and staff understand their responsibilities for identifying, transmitting, redistributing, storing or disposing of this kind of information.

To handle data properly, faculty and staff need to know what kind of data it is and what laws or standards, if any, might govern its use (or misuse). Some data must be kept private under laws such as 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), and the NC Identity Theft Prevention Act (which defines personal information and requires notification if a data breach occurs). Some information is governed by industry standards such as PCI (which protects credit card holder information). Some information is legally public.

Data Classifications

To assist in determining how to talk about handling information in any format, Duke has defined three classes of information: Sensitive, Restricted, and Public.

Sensitive Information: Explicit institutional approval is needed in order to receive access to sensitive information. Sensitive data elements include those which Duke is either required by law to protect, or which Duke protects to mitigate institutional risk, or which has been classified as Sensitive.

Restricted Information: Restricted information is that which Duke has a contractual or proprietary obligation to protect, and disclosure of which would not significantly harm the university. Access to Restricted data elements is determined by business process needs.

Public Information: All other information, 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. (This does not include information that has been disclosed accidentally.)

Faculty and staff need to be aware of the classification of a piece of information and its associated risks in order to understand how you should properly and securely handle the information. Each classification tier requires a specific level of technical and procedural security controls due to the risk impact if the information is mishandled.

Roles and Responsibilities

Owner: the owner of an information element. The Data Owner 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.

Manager: The persons who are responsible for implementing the controls the owner identifies.

User: The persons who actually "touch" the information (enter, delete, even read).

Risk Impact Labels

Risk Impact Labels can be assigned to information after an assessment of the impact to the organization if the information is mishandled leading to the compromise of the information's confidentiality, integrity or availability.

High: A High Risk Impact is an event that would cause severe and long-term interference with the mission of the University or a business unit, or would result in major financial loss, or would result in severe harm to an individual's life or livelihood.

Moderate: A Moderate Risk Impact is an event that would cause significant interference with the mission of the University or business unit, result in significant financial loss; or result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Low: A Low Risk Impact is an event that would cause some interference with the mission of the University or business unit or result in minor harm to an individuals well being.

Best Practices

* Data storage – Any systems which store Sensitive or Restricted data must document their compliance with the University IT Security Office's Server Security standard. In addition, any systems which store Sensitive information are required to use whole disk encryption for all storage of that data. Public data can be stored anywhere.

* If you work with data that has not been classified, it should be considered Sensitive until the Owner assigns the classification.

* Questions about classifying or handling the information should be directed to the Owner, your supervisor, your departmental security liaison, or the University IT Security Office. The Information Security Triage Form (to be developed) can help you identify at what level your data should be classified. Your assigned security liaison in coordination

with the IT Security Office can assist you in developing appropriate controls and processes to protect sensitive or restricted information.

* The classification of information 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.

* Report the misuse or compromise of systems that handle, store or propagate restricted or internal data to security@duke.edu.

Sensitive Information Examples

Sensitive information includes data elements associated with a specific individual that are identified and protected by federal, state, local laws, regulations or adopted standards. Sensitive information includes (but may not be limited to) the following kinds of information that can be linked to an individual:

- * Social Security numbers
- * driver's license number or state identification number
- * financial account number (including credit/debit card) or any security code, access code or password that would permit access to an individual's financial account
- * unique biometric data, including fingerprint, voice print, retina or iris image or any other unique physical representation
- * protected health information (any information about the health status, provision of health care, or payment for health care)
- * student records, including grades, dates of attendance, and other elements not released in writing

Data classification overview

	Sensitive Information (highest, most sensitive)	Restricted Information (moderate level of sensitivity)	Public Information (low level of sensitivity)
Legal requirements	Protection of data is required by law (e.g., see list of specific HIPAA and FERPA data elements)	Duke University has a contractual obligation to protect the data	Protection of data is at the discretion of the owner or custodian
Reputation	High	Medium	Low

risk

Other Institutional Risks	Information which provides access to resources, physical or virtual	Smaller subsets of protected data from a school or department	General university information
Access	Only those individuals designated with approved access and signed non-disclosure agreements	DukeUniversity employees and non-employees who have a business need to know	DukeUniversity affiliates and general public with a need to know
Examples	<ul style="list-style-type: none">* Medical* Students* Prospective students* Personnel* Donor or prospect* Financial* Contracts* Physical plant detail* Credit card numbers* Certain management information	<ul style="list-style-type: none">* Information resources with access to restricted data* Research detail or results that are not Sensitive or Public data* Library transactions (e.g., catalog, circulation, acquisitions)* Financial transactions which do not include Sensitive data (e.g., telephone billing)* Information covered by non-disclosure agreements	<ul style="list-style-type: none">* Campus maps* Business contact data (e.g., directory information)* Faculty and Staff Email addresses

It is the recommendation of the University IT Security Office that all campus units which collect and store information document their policies, procedures, and architectures which 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.

Reference

Any questions on this standard should be referred to security@duke.edu.

Developed by: Duke University IT Security Office

Scheduled Review Date: September, 2010