Data Security for Research Administration: Protecting the Data, Duke, and Your Job

Richard Biever, CISSP
Chief Information Security Officer - Duke University

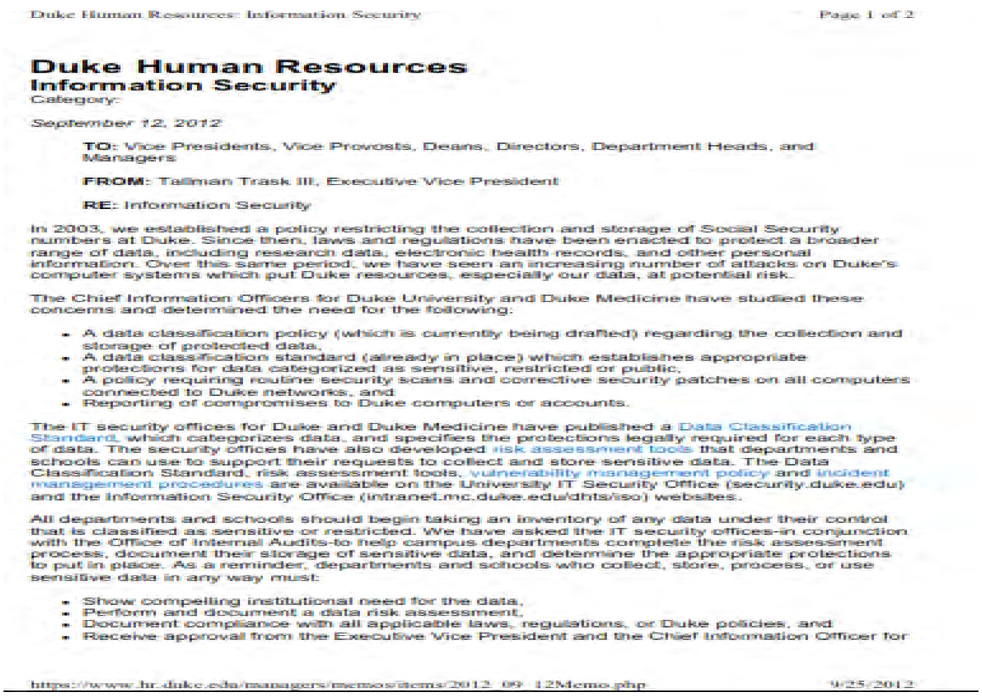
Chuck Kesler, MBA, CISSP, CISM, PMP
Chief Information Security Officer – Duke Medicine

Brian Lowinger, J.D.
Contracts and Compliance Officer - Office of Research Support

Why Are We Here?

- Laws that Require Data Protection
- Monetary Penalties
- Criminal Sanctions
- Breach Notice Requirements
- Goodwill
- Protect Duke’s Assets
- Protect Your Job
- Plus…..

It’s Institutional



Duke Human Resources: Information Security Page 1 of 2

Duke Human Resources
Information Security
Category:

September 12, 2012

TO: Vice Presidents, Vice Provosts, Deans, Directors, Department Heads, and Managers

FROM: Tallman Trask III, Executive Vice President

RE: Information Security

In 2003, we established a policy restricting the collection and storage of Social Security numbers at Duke. Since then, laws and regulations have been enacted to protect a broader range of data, including research data, electronic health records, and other personal information. Over this same period, we have seen an increasing number of attacks on Duke's computer systems which put Duke resources, especially our data, at potential risk.

The Chief Information Officers for Duke University and Duke Medicine have studied these concerns and determined the need for the following:

- A data classification policy (which is currently being drafted) regarding the collection and storage of protected data,
- A data classification standard (already in place) which establishes appropriate protections for data categorized as sensitive, restricted or public,
- A policy requiring routine security scans and corrective security patches on all computers connected to Duke networks, and
- Reporting of compromises to Duke computers or accounts.

The IT security offices for Duke and Duke Medicine have published a Data Classification Standard, which categorizes data, and specifies the protections legally required for each type of data. The security offices have also developed risk assessment tools that departments and schools can use to support their requests to collect and store sensitive data. The Data Classification Standard, risk assessment tools, vulnerability management policy and incident management procedures are available on the University IT Security Office (security.duke.edu) and the Information Security Office (intranet.mc.duke.edu/dhts/iso) websites.

All departments and schools should begin taking an inventory of any data under their control that is classified as sensitive or restricted. We have asked the IT security offices-in conjunction with the Office of Internal Audits-to help campus departments complete the risk assessment process, document their storage of sensitive data, and determine the appropriate protections to put in place. As a reminder, departments and schools who collect, store, process, or use sensitive data in any way must:

- Show compelling institutional need for the data,
- Perform and document a data risk assessment,
- Document compliance with all applicable laws, regulations, or Duke policies, and
- Receive approval from the Executive Vice President and the Chief Information Officer for

https://www.hr.duke.edu/managers/memos/items/2012_09_12Memo.php 9/25/2012

Understand What is Data

- Policy
- Classification
- Responsibilities

Find Your Data

- Risk Assessments
- Who to involve (Business managers and IT Staff and Compliance)
- DLP

Security Plans

- Based on risk assessments
- Prioritize needs
- Sample programs (policy, host sec, incident handling, etc)

Sample Technologies

- Host (encryption, end pt mgt, backups, hardening standards)
- Network (IDS/IPS, VPN)
- Application (Code testing)
- Vulnerability Management (scanning, pen testing)
- Sharing Technologies (encryption, options)

The Cloud

- Vendor risk assessments
- Vendor management