Information Security Policy Addendum: Data Classification

Final: Approved by TSAC May 16, 2013

I. PURPOSE

Loyola University Maryland is committed to maintaining appropriate security controls over information systems and data. This addendum to the Information Security Policy contains additional policy and guidelines for classifying data elements based on their confidentiality requirements, and for classifying data collections and information systems based on their confidentiality, integrity and availability requirements.

This document is intended, in combination with other policies, standards, guidelines, and procedures, to help the University to appropriately apply its security resources in a manner that reduces the greatest amount of risk.

II. SCOPE

As defined by the Security Policy, with the following additions.

1) This classification document is not a risk assessment policy. The likelihood of potential breaches is not to be considered when determining security classification, just the expected impact of any potential breach. The classification of data and information systems may be used as input to risk assessment processes as defined by risk assessment policies.

2) This classification policy is not a configuration policy or standard. The security classification of data collections and systems may be used as input to decisions regarding configuration policy and procedures.

III. PRINCIPLES

1) The primary purpose of security classification is to guide the implementation of administrative, technical, and physical security controls for data and systems. Security classification is not the primary determinant of who should be given what permissions. As stated in the Information Security Policy, authorization to access, modify, or destroy data and systems should be provided only to individuals who need such authorization in the course of fulfilling their roles at the University.

2) Both direct and indirect impacts (as those arising from civil or criminal lawsuits, loss of reputation, etc.) of potential breaches to organizational operations, organizational assets, or to individuals will be considered when classifying data, data collections and information systems.

IV. DEFINITIONS

Terms in this policy addendum are used as they are defined in the Information Security Policy, with the following exceptions and clarifications.

Data Classifications: This policy addendum replaces the three definitions for the terms *public, sensitive,* and *restricted* as they were defined in the Information Security Policy. The four terms: *public, internal, sensitive,* and *highly-sensitive,* as defined below will now be used for security classification of data elements.

V. POLICY AND GUIDELINES

A. CLASSIFICATION OF DATA TYPES

1) Policy:

- The following four terms will be used when classifying data elements. Examples of data elements include: Social Security numbers, student grades, faculty email addresses, University financial account numbers, course schedules, course syllabi, faculty research, and many others.

  - **Public** – Data elements for which there is ***no confidentiality requirement***, regardless of the quantity of data being considered.

  - **Internal** – Data elements not intended to be published, but where ***no significant harm*** to the University or others would likely occur were the data to be disclosed inadvertently.

  - **Sensitive** – Data elements for which the University has determined inappropriate disclosure may expose the University or others to ***significant but not serious harm***. There may or may not be regulatory or contractual obligations regarding data types deemed sensitive.

  - **Highly-Sensitive** – Data elements that if disclosed inappropriately could cause ***serious or catastrophic harm*** to the University or to others. This harm could be in the form of identity theft or other major financial loss, or serious loss of reputation. There may or may not be regulatory or contractual obligations regarding data deemed highly-sensitive.

- The security classification of a particular data element remains the same regardless of the quantity of data of that element, the locations or systems where the data is stored, the data collections that contain it, or the information systems that handle it.

- Data elements as such do not have any inherent integrity or availability requirements. Only particular information systems and data collections have integrity and availability requirements, and even systems that only handle public data may have integrity or availability requirements. The security levels of data collections and information systems are covered in section V. B.

2) Guidelines:

- **Public:**
  - Data that *could* be published or posted to a public website or otherwise made available to the entire world with no limits, *even if it is not actually published*.
  - Examples of public data include: departmental contact information and phone numbers, course catalogs, etc.
- **Internal:**
  - Data that the University would prefer not to publish, perhaps for competitive or public relations reasons, but where no significant damage would be done if it were to be disseminated.
  - Examples of internal data include: many departmental memos, most meeting minutes, future course offerings plans, etc.
- **Sensitive:**
  - Most data covered by the Federal Education Rights and Privacy Act (FERPA) but not otherwise considered highly-sensitive, is likely to be deemed sensitive.
  - Examples of sensitive data include: student identification numbers, student grades, student directory information, employee home phone numbers, passwords or password hashes for accounts with access only to internal or public data.
- **Highly-Sensitive:**
  - Data covered by Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industries Data Security Standard (PCI-DSS), and the Maryland Personal Information Privacy Act (PIPA), among others, is likely to be deemed Highly-Sensitive.
  - Examples of highly-sensitive data include: Social Security numbers, Driver's License numbers, Personal Health Information, passwords or password hashes for accounts with access to sensitive or highly-sensitive data, and customer payment card numbers or payment card authentication data.

B. CLASSIFICATION OF INFORMATION SYSTEMS AND DATA COLLECTIONS

1) Policy:

- When classifying data collections and information systems, the following three security levels will be used:
  - **Low-Impact**
  - **Medium-Impact**
  - **High-Impact**
- The classification will be based on the corresponding direct or indirect impact to the University that could be expected as a result of a security breach to the system or data collection. Guidelines for determining impact levels are given below.
- The classification of information systems and data collections is primarily aimed at supporting the three high-level security goals of confidentiality, integrity and availability. Any given information system or data collection may have differing requirements for each of these three goals, and all three will be considered when determining its security level.
- Both the elements and quantities of data stored or processed will be considered when determining the security level of an information system or data collection.

2) Guidelines:

- Adapted from the Federal Information Processing Standards Publication 199 (FIPS 199):
  - Low Impact – a breach could be expected to have a ***limited*** adverse effect (for University purposes this may be thought of as a total loss and/or cost of remediation of less than $50,000)
  - Medium Impact – a breach could be expected to have a ***serious*** adverse effect (may be thought of as a total loss and/or cost of remediation between $50,000 and $500,000).
  - High Impact – a breach could be expected to have a ***severe or catastrophic*** adverse effect (may be thought of as a total loss and/or cost of more than $500,000).

VI. PENALITIES AND ENFORCEMENT

As described in the Information Security Policy.

VII. EFFECTIVE DATE, REVIEW AND REVISION OF POLICY

As described in the Information Security Policy.

VII. APPROVALS:

Reviewed and approved by the Technology Services Advisory Committee

Reviewer Name and Title: **Louise Finn, Chief Information Officer**

Reviewer Signature: *Louise Finn*

Date: **May, 16 2013**