# **Appendix A**

*Data Classification Standard*

The purpose of this Data Classification Standard is to establish a framework for classifying Institutional Data based on its level of sensitivity, value and criticality to the University as required by the University's Information Security Policy. Classification of data will aid in determining baseline security controls for the protection of data found in the System Protection Profile in Appendix B.

## I. Public Information

Information is Public when the unauthorized disclosure, alteration or destruction of that information would result in little or no risk to the University and its affiliates.

Examples of Public Information include, but are not limited to, the following:

- Publications approved for general release;
- Contact information that individual provided on business card;
- Institutional mission, vision, and values;
- Campus maps;
- Public facing institutional web pages;
- Course catalogs;
- Directory information that has been designated for public view;
- Job postings; and
- The University Policies which are publicly available in the University Policy Library.

## II. Non-Public Information

A Data Steward should classify information as Non-Public Information when the unauthorized disclosure, alteration or destruction of such information could result in a moderate level of risk to the University or its affiliates. Notwithstanding the internal non-public nature of this information, such information may be shared on a limited basis for purposes of academic collaborations, work with service providers or other contractual or non-contractual relationships which further Stevens' mission, provided that such sharing is covered by non-disclosure obligations in a contract or scholarly practices.

Examples of Non-Public Information include, but are not limited to, the following:

- Unpublished research data and other academic work that may be shared with third-party collaborators or other entities;
- Administrative data and reports that may be shared with third-party individuals or entities; and
- Data or information concerning University infrastructure.

## III. Sensitive Information

A Data Steward should classify information as Sensitive Information when the unauthorized disclosure, alteration or destruction of information could result in a moderate level of risk to the University or its affiliates. Any sharing of Sensitive Information must occur only via a contract or other written agreement containing non-disclosure obligations. By default, all Institutional Data that is not explicitly classified as Public, Non-Public or Restricted Information should be treated as Sensitive Information.

Examples of Sensitive Information include, but are not limited to, the following:

- Budget data, records and plans;
- University Policies which are not publicly available in the University Policy Library;
- Directory information that has not been designated for public view;
- Meeting minutes and notes;
- Sensitive research data and materials; and
- Data and reports that are not intended for public access or distribution with individuals or entities outside Stevens.

## IV. Restricted Information

Restricted Information requires the highest level of security and privacy protection. This is information that if disclosed, altered, or destroyed could cause a significant level of risk to the University, its affiliates or members or the Stevens community. Restricted Information may not be shared with any third party without prior written approval of the relevant Divisional Vice President.

Examples of Restricted Information include, but are not limited to, the following:

- Information protected by state or federal privacy regulations;
- Any personally identifiable student, parent, or employee records;
- Financial records;
- Admissions applications and related records;
- Student loan application information;
- Materials, records and items that are covered by export control regulations;
- Information or records subject to non-disclosure agreements with third parties;
- Health records (including mental health records);
- University contracts;
- Information concerning the types, location and security of potentially hazardous materials and equipment;
- Research data which may not be shared with individuals or entities outside Stevens;
- Alumni and donor records;
- All records related to minors; and
- Passwords.

## V. Restricted Information Subject to Additional Security Protocols

Occasionally, certain academic research or other projects or programs will necessitate additional security protocols required by a governmental or other entity. In these cases, Data Stewards will work with IT, Data Custodians, Information System Managers and, if appropriate, the Office of Sponsored Programs, to ensure all requisite security protocols are in place and monitored for full and continuous compliance.