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.

Capitalized terms used in this Appendix shall have the same meanings as defined in the university's Information Security Policy.

I. Public Information

Data is classified as Public Information when the unauthorized disclosure, alteration or destruction of that information would result in little or no risk to the university or its affiliates or members or the Stevens community.

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

- Publications approved by the relevant Functional Area's leader, or their designee, for general release;
- Contact information as provided on a business card or the like;
- 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
- University Policies which are publicly available in the University Policy Library.

II. Non-Public Information

Data is classified 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 or members or the Stevens community. Notwithstanding the internal non-public nature of this information, such information may be shared on a limited basis only as necessary for purposes such as academic collaborations, work with service providers or other contractual or non-contractual relationships which further Stevens' mission, provided appropriate non-disclosure obligations are in place in a contract.

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- Unpublished research data and other academic work that may be shared with third-party collaborators or other entities;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

Data is classified as Sensitive Information when the unauthorized disclosure, alteration or destruction of information could result in a high level of risk to the university or its affiliates or members or the Stevens community. Sensitive Information may be shared only via a contract or other written agreement containing non-disclosure obligations. In circumstances where the classification of Institutional Data is unclear, it must be treated as Sensitive Information until a definitive classification can be determined.

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

- Budget data, records and plans;
- University protocols, practices or policies that 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

Data is classified as Restricted Information when the unauthorized disclosure, alteration, or destruction of information could cause a significant level of risk to the university, its affiliates or members or the Stevens community. Restricted Information requires the highest level of security and privacy protection and may not be shared with any third party without prior written approval of the relevant Divisional Vice President, or their designee.

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

- Social Security numbers, government identifiers, biometric identifiers and financial account numbers;
- Student records containing highly sensitive data such as medical records, disciplinary records or records created for law enforcement or legal purposes;
- Employee records containing highly sensitive data such as medical information, background check results, or investigative materials;
- Bank account numbers, credit/debit card numbers, payment credentials, or other information where disclosure could create risk of fraud, identity theft, or financial exploitation;
- 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;
- 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, credentials or encryption keys that could permit access to critical university systems.

V. Restricted Information Subject to Additional Security Protocols

In some cases, certain academic research or other projects or programs will necessitate additional security protocols required by a governmental or other entity. In these cases, the relevant Authorized Users will work with IT, the relevant Functional Area's leader (or their designee) and Information System Managers, and if appropriate, the Office of Sponsored Research Administration, and Office of General Counsel, to ensure all requisite security protocols are implemented and continuously monitored for compliance. Data that falls into this classification is likely to be categorized in such a way that a thorough and specific set of controls is inherently expected to be in place when handling the information. The most common type of data to be categorized in this manner is controlled unclassified information.

Controlled Unclassified Information (CUI)

CUI is unclassified information that is possessed, produced, or otherwise exists for some function authorized by the United States Government. In the context of Stevens, it is most frequently encountered through research agreements and is secured following the controls described in National Institute of Standards and Technology (NIST) Special Publication 800-171.

Examples of CUI at Stevens could include, but are not limited to, the following:

- Defense information produced or shared as part of an ongoing research effort;
- Critical infrastructure information produced or shared as part of an ongoing research effort;
- Patent information for inventions or discoveries produced as part of an ongoing research effort;
- Any sensitive information or materials produced or shared as part of a contracted research agreement in which NIST 800-171 or an equivalent control set is prescribed to secure data;
- Communications regarding any materials, information, or processes relating to any of the research examples listed above; and

- Potentially any details of contracts and research agreements relating to any of the research examples listed above.

IT shall detail further requirements regarding the accessing, labeling, storage and transmission of CUI at Stevens in standards available alongside other research-related resources from the Office of Research Integrity, Compliance, Education and Systems.