90.2 Information Security Policy

Approval Authority:	**Audit Committee**
Responsible Officer:	**Chief Information Officer and Vice President for Information Technology**
Responsible Office:	**Division of Information Technology**
Effective Date:	**October 15, 2020**

I. Purpose of this Policy

The purpose of this Policy is to set forth guidelines and procedures to protect the confidentiality, integrity and availability of Stevens Institute of Technology's ("Stevens" or the "University") Institutional Data,[1] as well as supporting technologies ("Information Systems") that store, process or transmit Institutional Data ("Institutional Systems"). All members of the Stevens community who make use of Information Systems ancillary to the use of Institutional Systems must ensure that any Information Systems they use are registered with the Division of Information Technology ("IT"), and otherwise abide by this Policy.

This Policy defines the roles and responsibilities of all members of the Stevens community who manage or have access to Institutional Data and Institutional Systems and defines the fundamental principles for the protection of Institutional Data and Institutional Systems at Stevens, including the principles of data classification and the controls required to ensure compliance with federal, state and other laws and University policies.

This Policy does not replace or supersede any information security controls with which Stevens is required to comply as part of its contractual obligations to a third party including, without limitation, a sponsor of research.

II. Definitions

An **Authorized User** is any Stevens employee, student or third party with permission to access an Institutional System. IT provides Authorized Users with permission to access Institutional Systems pursuant to the guidelines outlined in Section V.A of this Policy.

The **Campus Network** is the campus-wide wired and wireless network and associated network services established and funded by the University and supported by IT for general academic and administrative use.

A **Cyber Incident** is an attempt, successful or unsuccessful, to damage, disrupt or gain unauthorized access to an Information System or the Campus Network.

The **Cyber Incident Response Protocol** is the series of procedures and steps that the Cyber Incident Response Team (as defined in the Cyber Incident Response Protocol) must take upon the detection or notification of a Cyber Incident.

[1] All defined terms are defined in Section II.

A **Data Custodian** is a University employee who is appointed by a Data Steward, and who has operational responsibility (e.g., collection, maintenance and dissemination) for data in their functional area.

A **Data Steward** is the member of the Administrative Council who has planning and decision-making responsibilities for Institutional Data in their functional area.

An **Information System** is any electronic system that can be used to store, process or transmit data. An Information System can be a device (e.g., a server, desktop computer, laptop, printer, smart phone or tablet device) or a technology hosted by a vendor or third-party service provider (e.g., cloud services).

Institutional Data is all documents, records and other information which Authorized Users create, collect, maintain, transmit or record for University purposes.

An **Institutional System** is an Information System that houses or processes Institutional Data.

An **Institutional System Manager** is an individual appointed by a Data Steward who procures and/or oversees the development, operation and maintenance of an Institutional System.

Every Authorized User has one or more **User Accounts**, which provide the Authorized User access to the Campus Network and the Institutional Systems that they use for University purposes.

III. Classification of Institutional Data

Data Stewards, in coordination with Data Custodians and Institutional System Managers, must secure Institutional Data and Institutional Systems in a reasonable and appropriate manner. In order to determine the reasonable and appropriate baseline security controls for Institutional Data, Data Stewards must engage in data classification.

Data classification is the categorization of Institutional Data based on its level of sensitivity and the impact to the University should a Cyber Incident or other event cause the unauthorized disclosure, alteration or destruction of such Institutional Data. After consultation with IT, Data Stewards will determine whether the Institutional Data under their purview is Public, Non-Public, Sensitive or Restricted Information (as defined in Stevens' Data Classification Standard in Appendix A). Based on this categorization, Data Custodians and Institutional System Managers will implement the reasonable and appropriate baseline security controls listed in Stevens' System Protection Profile in Appendix B.

Stevens is committed to the free exchange and dissemination of fundamental research data, traditional works of scholarship and other academic materials. To the extent that a Data Steward has not classified particular scholarly, academic or research data or information as Public or Non-Public Information, a faculty member may, in consultation with the relevant Data Steward, re-classify such data or information as Public or Non-Public Information in order to facilitate collaboration, presentation, publishing and other scholarly activities which involve such data or information. Any sharing of information with a third party may require a non-disclosure agreement or other measures to maintain the non-public status of such information, as provided below and in Appendix A.

Further information concerning Stevens' Data Classification Standard and Stevens System Protection Profile is set forth in Appendices A and B. Appendices A and B may be modified or updated from time to time in writing by IT. Any such modifications or updates will be communicated to the Stevens community and posted to the University Policy Library.

IV. Roles and Responsibilities

A. Data Stewards

Data Stewards have overall responsibility for the Institutional Data managed by their functional areas, including the following:

1. Identifying, in consultation with the Office of General Counsel and the Chief Compliance Officer, the laws and regulations, University policies, procedures, standards, contracts and licenses that govern the Institutional Data within their functional areas;

2. Classifying the data managed by their units in consultation with Data Custodians, Institutional System Managers and IT (*see* Appendix A);

3. Understanding how Institutional Data is stored, processed and transmitted by the University;

4. Ensuring that Data Custodians and Institutional System Managers implement reasonable and appropriate security controls to protect the confidentiality, integrity and availability of Institutional Data according to this Policy, its appendices and other policies promulgated by IT; and

5. In the event of a Cyber Incident, working with IT, Data Custodians and Institutional System Managers to follow the University's Cyber Incident Response Protocol.

B. Data Custodians

Data Custodians are responsible for collecting, maintaining and disseminating Institutional Data in their functional areas, as well as the following:

1. Assuring compliance with data access security standards, training users and adhering to policies and federal regulations regarding the responsible use of and access to data;

2. Determining the type of access given to University users for the data sets within their area of responsibility;

3. Understanding how Institutional Data is stored, processed and transmitted by the University;

4. Coordinating with IT to document administrative and operational procedures to ensure consistent storage, processing and transmission of Institutional Data; and

5. In the event of a Cyber Incident, working with IT, Data Stewards and Institutional System Managers to follow the University's Cyber Incident Response Protocol.

C. Institutional System Managers

Institutional System Managers exist in each of the University's functional areas and maintain each Institutional System's functionality and operational documentation (including hardware, software inventory, support contact and contract information). In addition, Institutional System Managers:

1. Oversee compliance with this Policy with respect to the Information System that they manage and inform the Data Steward, the Data Custodian and IT if a breach of this Policy occurs;

2. Ensure that all Information Systems that they manage have assigned personnel who are responsible for performing maintenance to keep Information Systems in good working order;

3. Oversee the installation and configuration of the appropriate security services and technologies, as listed in the System Protection Profile in Appendix B; and

4. In the event of a Cyber Incident, work with IT, Data Stewards and Data Custodians to follow the University's Cyber Incident Response Protocol.

If a functional area does not employ an individual with sufficient technical expertise to serve as an Institutional System Manager, IT will serve as the Institutional System Manager for that functional area.

D. Authorized Users

Authorized Users must access and use Institutional Data in an appropriate manner consistent with this Policy. In particular, Authorized Users must:

1. Protect the Institutional Data they access and use in accordance with this Policy and any other policies and procedures promulgated by IT;

2. Report actual or suspected vulnerabilities in the confidentiality, integrity or availability of Institutional Data to their supervisor or IT; and

3. Report actual or suspected information security incidents affecting the confidentiality, integrity, or availability of Institutional Data to their supervisor or IT.

V. General Policies

A. Authorized User Access

IT, in consultation with Data Stewards, Data Custodians and Institutional System Managers, provides permission for all Authorized Users to access the Campus Network via Stevens' single-sign-on system or other means described in IT's internal policies and procedures.

Data Stewards, Data Custodians and Institutional System Managers must request access for a prospective Authorized User following IT's internal processes. IT will only provide an Authorized User the minimum access permissions that the Authorized User requires. For example, if an Authorized User only requires the ability to read Institutional Data, IT will not grant that Authorized User the ability to modify or delete Institutional Data.

Upon the request of a Data Steward, Data Custodian and Institutional System Manager, IT shall revoke the access of an Authorized User when the Authorized User no longer requires access to a specific Institutional System and/or Institutional Data including, but not limited to, when an Authorized User who is an employee or student no longer works at Stevens or maintains active student status, or when such an Authorized User's job responsibilities change and they no longer require access to the Institutional System or Institutional Data.

In general, Authorized Users may not share User Accounts or passwords. Occasionally, an Institutional System Manager will request that IT create a User Account for the purposes of performing a specific function, and for which multiple individuals will have access to the password (e.g., a service account, a shared mailbox, an account to manage file shares). In these cases, the Authorized Users with access to the account must only use the account for the specific function for which it was created. In addition, IT must change the password for such an account when one of the Authorized Users of the account no longer requires access to the account.

Authorized Users may use remote access and network technologies to access Information Systems connected to the Campus Network, provided that the University has approved the technology (e.g., VPN).

B. Information System Access

An Authorized User may connect an Information System to the Campus Network after registering the Information System with IT by following IT's internal processes. For avoidance of doubt, unregistered Information Systems may not connect to the Campus Network. Once registered, Information Systems will only be able to access resources on the Campus Network if there is a legitimate need to access those resources and the Information System has the proper security protocols in place pursuant to the System Protection Profile in Appendix B.

Information Systems, or applications or operating systems running on Information Systems, that are unsupported (or otherwise cannot receive updates or security patches) may not connect to the Campus Network.

C. Implementation, Awareness and Training

IT shall coordinate and monitor the implementation of, and compliance with, this Policy. All Authorized Users shall complete security awareness training developed and assigned by IT and the Division of Human Resources. Such training shall address the security risks associated with Authorized Users' activities and the applicable policies, standards and procedures related to the security of Information Systems.

D. Third Parties; Contractual Obligations

1. Information Security Assessment

The Office of Procurement and the relevant Data Steward must ensure that any vendor or third-party service provider that stores, processes or transmits Institutional Data classified as, Non-Public, Sensitive or Restricted Information (as defined in Appendix A) undergoes an information security assessment. IT shall develop and implement such an assessment in cooperation with the Office of Procurement and the relevant Data Steward.

2. Institutional Information Security Obligations

The University must adhere to all institutional obligations to protect Non-Public, Sensitive or Restricted Information stemming from contractual or other responsibilities. Such obligations may arise in connection with non-disclosure agreements in the context of research collaborations or sponsorships, potential business arrangements and other research projects and programs. Data Stewards are responsible for providing oversight of compliance with such obligations. In each case, it is the responsibility of the relevant Data Steward, in coordination with IT, to develop and implement the appropriate plan for informing the relevant Data Custodians, Institutional System Managers and Authorized Users of the institutional obligation and ensuring that the Non-Public, Sensitive or Restricted Information is adequately stored and secured.

As directed by the relevant Data Steward, it is the responsibility of the relevant Data Custodian (the principal investigator on a sponsored research project or grant or the primary Stevens liaison on other agreements) to comply with all relevant regulations, processes and policies (including any and all additional security protocols required to protect information subject to higher security protections by a governmental or other entity) as instructed by the Office of Sponsored Programs ("OSP") or the relevant Stevens business unit following OSP's or the business unit's review and acceptance of the award or agreement on the University's behalf.

E. Physical and Media Protection

IT shall encrypt all Institutional Systems (e.g., servers, desktop computers, laptops) that it manages and shall provide Authorized Users with the tools (e.g., Box) to encrypt Institutional Data that they send or receive.

Authorized Users must protect digital media (e.g., external/removable hard disk drives, printer hard drives, USB flash drives, compact disks) and non-digital media which contain Institutional Data,

during storage, transportation and disposal. Best practices for protecting Information Systems and media include using strong passwords (*see* Section V.H), locking office doors when unoccupied, ensuring Information Systems are locked and password protected when not in use and positioning screens used to view sensitive information in order to prevent unauthorized viewing.

F. Risk Assessment; Audit

IT, in conjunction with Data Stewards, Data Custodians and Institutional System Managers, will periodically assess risks related to Information Systems by identifying relevant threats and the likelihood they will occur, vulnerabilities both internal and external to the University, and the potential impact to Stevens given the potential threats and vulnerabilities.

IT shall periodically scan for vulnerabilities in Institutional Systems and Information Systems that are connected to the Stevens network. When IT identifies a vulnerability affecting an Institutional System, it will notify the Institutional System Manager who, in coordination with IT, is responsible for remediation of the vulnerability.

IT will configure Institutional Systems, including networks and software applications, to create, protect and retain system audit records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate system activity. Such auditing will focus on the identity and generalized activity of the Information Systems that are connected to the Campus Network and not on substantive and academic content housed or transmitted to or from Information Systems.

G. Anti-Virus and Anti-Malware Software

IT shall equip all desktops, laptops and servers with updated anti-virus and anti-malware software in accordance with the System Protection Profile in Appendix B and shall configure such software to perform a full system scan at least once each week.

H. Passwords

Authorized Users shall protect their Institutional Systems with strong passwords. IT shall require multi-factor authentication for Institutional Systems housing Non-Public, Sensitive or Restricted Information (as defined in the Data Classification Standard in Appendix A) and configure Institutional Systems to (1) require a password reset at least every 180 days and (2) lock Authorized Users out of Institutional Systems after three failed access attempts.

VI. Exception Process

In a small number of circumstances, the Chief Information Officer, in consultation with the Office of General Counsel, the relevant divisional vice president or dean and other relevant individuals, may grant written exceptions to compliance with this Policy. The Chief Information Officer may only grant such exceptions where the alternative presents a reasonable, justifiable business and/or research explanation supporting such an exception.

The Chief Information Officer may grant exceptions only in writing and only for a specific period of time, not to exceed one year. An Exception Request must include:

A. A description of the relevant provision of this Policy;

B. The anticipated length of non-compliance;

C. A proposed assessment of risk associated with non-compliance;

D. A proposed plan for managing the risk associated with non-compliance; and

E. A proposed review date to evaluate progress toward compliance.

VII. Compliance & Enforcement

All Authorized Users, Data Stewards, Data Custodians and Institutional System Managers are expected to comply with this Policy and its Appendices. Violations of this Policy may result in suspension or termination of access privileges. Employees and students who violate this Policy will be subject to disciplinary action, up to and including termination or expulsion.