Information Security Policy

Approval Authority:	**Cabinet**
Responsible Officer:	**Vice President for Information Technology and Chief Information Officer**
Responsible Office:	**Division of Information Technology**
Effective Date:	**May 19, 2026**

I. Purpose of this Policy

The purpose of this Policy is to set forth technical and administrative responsibilities and requirements to protect the confidentiality, integrity and availability of Stevens Institute of Technology's ("Stevens" or the "university") Institutional Data and Institutional Systems.

This Policy defines the responsibilities regarding information security of all members of the Stevens community who manage or have access to Institutional Data and Institutional Systems. This Policy also defines the fundamental principles for the protection of Institutional Data and Institutional Systems at Stevens as applied by the Division of Information Technology ("IT"), 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

A. 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 IV.A of this Policy.
B. 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.
C. A **Cyber Incident** is an attempt, successful or unsuccessful, to damage, disrupt or gain unauthorized access to an Information System or the Campus Network.
D. A **Functional Area** is an organizational unit of the university that is led by a designated administrator (VP, AVP or Director) and is responsible for a distinct set of operations, programs, or services.

E. The **Information Security Incident Response Plan ("Incident Response Plan")** is an internal document which defines the roles and responsibilities of the Cyber Incident Response Team, a procedural outline and reporting requirements upon the detection or notification of a Cyber Incident. It is available to members of the Cyber Incident Response Team or via request and coordination with the Office of Information Security Services.
F. An **Information System** is any electronic system that can be used to process, store 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).
G. **Institutional Data** is all documents, records and other information which Authorized Users create, collect, maintain, transmit or record for university purposes.
H. An **Institutional System** is an Information System that houses or processes Institutional Data. An Information System connected to the Campus Network is not an Institutional System if it does not process, store or transmit Institutional Data (e.g., an on-campus gaming console, or a personal phone connected to the wireless network).
I. An **Institutional System Manager** is an individual within a Functional Area who oversees the development, operation and maintenance of an Institutional System. By default, IT will serve as the Institutional System Manager for any Functional Area which does not employ an individual with sufficient technical expertise and dedicated time to serve as an Institutional System Manager. The leader of a Functional Area is responsible for employing an Institutional System Manager, or if they do not employ one, coordinating with IT to onboard and manage their systems.
J. 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 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. Data is classified as Public, Non-Public, Sensitive or Restricted Information, as defined in Stevens' Data Classification Standard in Appendix A. Based on this categorization, Institutional System Managers must implement the reasonable and appropriate baseline security controls listed in Stevens' System Protection Profile in Appendix B. In circumstances where the implementation of appropriate security controls for or classification of

Institutional Data is atypical or unclear, Institutional System Managers must alert the leader of their Functional Area and consult the Office of Information Security Services before handling the data further.

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 particular scholarly, academic or research data or information are not classified as Public or Non-Public Information, a faculty member can, at their discretion and in consultation with IT and the leader of their Functional Area, 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.

In certain circumstances, Institutional Data may carry an inherent data classification that cannot be changed due to the technical definition or requirements for use of that data. This includes, but is not limited to, reporting requirements, publishing requirements, privacy obligations and security obligations imposed during contracting for or receipt of the Institutional Data by the sponsor of a research project, a government entity or state or federal law.

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 in coordination with the Office of General Counsel and Office of Compliance. Any such modifications or updates will be communicated to the Stevens community and posted to the university Policy Library.

IV. General Policies

A. Authorized User Access

IT 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, standards and procedures. IT follows the principle of "least privilege" and will provide an Authorized User only the minimum access permissions that the Authorized User requires, in accordance with applicable enrollment, onboarding and internal IT processes. For example, if an Authorized User requires only the ability to read Institutional Data, IT will not grant that Authorized User the ability to modify or delete Institutional Data.

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.

Authorized Users must only use approved remote connection solutions when making inbound connections to access Information Systems and the Campus Network, such as an approved Virtual Private Network (VPN), Remote Desktop Protocol (RDP) or Remote Access Software. Authorized Users must consult with IT prior to downloading or using any remote connection solutions to determine if the use of that technology is approved for inbound connections.

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, which can be found in the Stevens Support Portal. For avoidance of doubt, unregistered Information Systems are prohibited from connecting 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 Institutional Systems, as well as best practices for mitigating those risks and addressing additional compliance needs where applicable.

D. Third Parties, Information Security and Contractual Obligations

1. Information Security and Privacy Impact Assessment

The Office of Procurement shall work with divisional and departmental leaders to ensure that, prior to the procurement, development or adoption of any new system, technology or service that will collect, process, store or transmit Institutional Data classified as Non-

Public, Sensitive or Restricted, an Information Security and Privacy Impact Assessment (ISPIA) is conducted in consultation with IT, the Office of General Counsel and other administrators as needed.

The ISPIA must evaluate risks related to data privacy, information security, regulatory compliance and the overall impact to individuals' rights, identifying mitigating controls as appropriate. All projects must integrate privacy and security by design principles to ensure that safeguards are implemented throughout the entire lifecycle of the system, technology or service. Procurement will not grant final approval of the system, technology or service until the ISPIA process is complete and recommended security and privacy controls have been incorporated and verified.

2. Institutional Information Security Obligations

The university must adhere to all institutional obligations to protect Non-Public, Sensitive and Restricted Information stemming from contractual, legal and other responsibilities. Such obligations may arise in connection with non-disclosure agreements in the context of research collaborations and sponsorships, potential business arrangements, facility and individual government clearances and other research projects and programs.

The leader of each Functional Area, or a designee appointed by that leader, is responsible for providing oversight of compliance with such obligations. In each case, it is the responsibility of the designated individual, in coordination with IT, to develop and implement an appropriate plan for informing the relevant Institutional System Managers and Authorized Users of these obligations and ensuring that data is stored and secured appropriately.

As directed by the leader, or their designee, it is the responsibility of the relevant Authorized Users (the principal investigator on a sponsored research project or grant or the staff or faculty members handling the data for the Functional Area on other agreements) to comply with all relevant regulations, processes and policies as determined during review and acceptance of the award or agreement by the Office of Sponsored Research Administration in coordination with IT and the Office of General Counsel.

3. Vendor and Third-Party Security Requirements

The leader of each Functional Area, or their designee, must ensure that all contracts and agreements with vendors, service providers and other third parties who store, process or transmit Institutional Data classified as Non-Public, Sensitive or Restricted Information include explicit security and data privacy provisions. The leader, or their designee, must ensure that vendors implement safeguards commensurate with the classification of the data they handle and allow for periodic security assessments or audits by the university or

its authorized representatives. The leader, or their designee, must also ensure that contracts stipulate prompt breach notification requirements, mandating that vendors notify the university in the event of a security incident or data breach affecting university data. The leader, or their designee, must monitor compliance with these contractual security obligations throughout the contract lifecycle. If a vendor fails to meet these requirements, the university may pursue appropriate remedial measures, including without limitation: requiring a corrective action plan; suspension of data access or services; termination of the contract; and/or referral for further legal, risk or compliance action as appropriate.

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 to encrypt Institutional Data that they send or receive. IT shall maintain a standard detailing encryption requirements and application across differing circumstances.

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. IT shall maintain standards regarding the proper protection of digital media, physical media and physical spaces.

F. Risk Assessment; Audit

IT, in conjunction with the leader of each Functional Area, or their designee, and Institutional System Managers, will periodically assess risks related to Institutional 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 arising from those threats and vulnerabilities.

IT shall periodically scan for vulnerabilities in Institutional Systems and Information Systems that are connected to the Campus 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 in accordance with IT standards. Failure to do so will result in the Institutional System being disconnected from the Campus Network.

IT will configure managed 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 on or transmitted to or from Information Systems.

G. Incident Detection, Prevention and Response

IT shall equip all managed 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. IT shall maintain internal processes and tools for interpreting the results of these scans, and for escalating vulnerabilities and suspected Cyber Incidents.

In the event of a Cyber Incident, the leader of each impacted Functional Area and Institutional System Managers must cooperate with IT and the Cyber Incident Response Team or fulfill their assigned role as a member of the Cyber Incident Response Team, as described in the Incident Response Plan.

H. Passwords

Authorized Users shall protect their Institutional Systems with strong passwords. Authorized Users must not share passwords and the access they provide to Institutional Systems, regardless of any access the recipient may already possess. IT shall require multi-factor authentication for Institutional Systems housing Non-Public, Sensitive and Restricted Information (as defined in the Data Classification Standard in Appendix A) and configure Institutional Systems to lock out Authorized Users after five failed access attempts. IT retains the right to force a password reset for any Authorized User as needed for security purposes.

V. Exception Process

In limited and unusual circumstances, exceptions to the requirements of this Policy may be granted by the Chief Information Officer, in consultation with the Office of General Counsel, the relevant divisional vice president or dean and other relevant individuals. For exceptions related to research, whether contractual or technical in nature, the Provost or VP for research must be consulted. Any such exception shall be in writing and only for a specific period of time not to exceed one year. The Chief Information Officer may only grant such exceptions where the alternative presents a reasonable, justifiable business and/or research explanation supporting the exception.

VI. Compliance & Enforcement

All Authorized Users must comply with this Policy, its Appendices and all applicable IT standards, as made available on the IT Governance, Policy and Standards page. Violations

of this Policy may result in disciplinary action, up to and including suspension or termination of access privileges, termination of employment or expulsion.