Policy Owner:	Chief Information Officer
Last Revised:	11/2016
Last Full Review:	03/2017
Contact:	Division of the Chief Information Officer, 518-276-2122

Information Technology Security Policy

1 Purpose

Information security measures are intended to protect the information assets of Rensselaer Polytechnic Institute and the privacy of the Institute's employees, students, alumni, suppliers, and other affiliated entities. It is recognized that the academic mission of Rensselaer must be served, and so any security policy needs to be respectful of the principles of intellectual freedom and scholarly pursuits; however, an open academic environment does not imply an open environment in all aspects. The purpose of this policy is to establish general guidelines and specific recommendations for the protection of the Institute's information technology resources and the information they contain.

2 Scope

This policy applies to all departments and units and to all employees, students, and third-parties with access to Rensselaer Polytechnic Institute information technology resources.

3 Policy

The protection of Rensselaer information systems and the information they contain is a responsibility shared by all members of the campus community, with the Vice President for Information Services and Technology and Chief Information Officer having the ultimate authority to establish policy and practice in this regard.

Each member of the campus community is responsible for the security and protection of information technology resources over which he or she has control. Resources to be protected include networks, computers, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Activities outsourced to off-campus entities must comply with the same security requirements as in-house activities.

4 Implementation

4.1 Roles and Responsibilities

Responsibilities range in scope from security controls administration for a large system to the protection of one's own access password. A particular individual often has more than one role.

Director of Information Security or other designee of the Vice President for Information Services and Technology and Chief Information Officer has been assigned the responsibilities for:

- establishing, implementing, and monitoring the Institute's Information Security Program;

- assisting others in resolving conflicting desires and interests with respect to information security;
- coordinating response teams for security events.

Administrative Officers, those being individuals with administrative responsibility for campus organizational units (e.g., unit heads, deans, department chairs, principal investigators, directors, or managers) or individuals having functional ownership of data must:

- identify the information technology resources under their control;
- define the purpose and function of the resources and ensure that requisite education and documentation are provided to the campus as needed;
- establish acceptable levels of security risk for resources by assessing factors such as:
    - how sensitive the data is, such as research data or information protected by law or policy;
    - the level of criticality or overall importance to the continuing operation of the campus as a whole, individual departments, research projects, or other essential activities;
    - how negatively the operations of one or more units would be affected by unavailability or reduced availability of the resources,
    - how likely it is that a resource could be used as a platform for inappropriate acts towards other entities, limits of available technology, programmatic needs, cost, and staff support;
- ensure that requisite security measures are implemented for the resources.

Providers, those being individuals who design, manage, and operate campus information technology resources (e.g. project managers, system designers, application programmers, or system administrators), must:

- become knowledgeable regarding relevant security requirements and guidelines;
- analyze potential threats and the feasibility of various security measures in order to provide recommendations to Administrative Officers;
- implement security measures that mitigate threats, consistent with the level of acceptable risk established by Administrative Officers;
- establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements;
- communicate the purpose and appropriate use for the resources under their control.

Individuals who access and use campus information technology resources must:

- become knowledgeable about relevant security requirements and guidelines;
- protect the resources under their control, such as access passwords, computers, and data they download.

Insufficient security measures at any level may cause resources to be damaged, stolen, or become a liability to the campus. Therefore, responsive actions may be taken. For example, if a situation is deemed serious enough, computer(s) posing a threat will be blocked from network access.

4.2 Key Security Elements

4.2.1 Logical Security

Computers must have the most recently available and appropriate software security patches, commensurate with the identified level of acceptable risk. For example, installations that allow unrestricted access to resources must be configured with extra care to minimize security risks.

Adequate authentication and authorization functions must be provided, commensurate with appropriate use and the acceptable level of risk.

Attention must be given not only to large systems but also to smaller computers which, if compromised, could constitute a threat to campus or off-campus resources. This includes computers maintained for a small group or for an individual's own use.

4.2.2 Physical Security

Appropriate controls must be employed to protect physical access to resources, commensurate with the identified level of acceptable risk. These may range in scope and complexity from extensive security installations to protect a room or facility where server machines are located, to simple measures taken to protect a User's display screen.

4.2.3 Privacy and Confidentiality

Applications must be designed and computers must be used so as to protect the privacy and confidentiality of the various types of data they process, in accordance with applicable laws and policies.

Users who are authorized to obtain data must ensure that it is protected to the extent required by law or policy after they obtain it. For example, when sensitive data is transferred from a well-secured central system to a User's location, adequate security measures must be in place at the destination computer to protect this "downstream data".

Technical staff assigned to ensure the proper functioning and security of Rensselaer information technology resources and services are not permitted to search the contents of electronic communications or related transactional information except as provided for in Rensselaer policy and guidelines. For example, any scanning of network traffic to detect intrusive activities must follow established campus guidelines or organizational procedures to ensure compliance with laws and policies protecting the privacy of the information.

5 Compliance with Law and Policy

Campus departments, units, or groups should establish security guidelines, standards, or procedures that refine the provisions of this Policy for specific activities under their purview, in conformance with this Policy and other applicable policies and laws.

The following activities are specifically prohibited under this Policy:

- interfering with, tampering with, or disrupting resources;
- intentionally transmitting any computer viruses, worms, or other malicious software;
- attempting to access, accessing, or exploiting resources without authorization;
- knowingly enabling inappropriate levels of access or exploitation of resources by others;

- downloading sensitive or confidential electronic information to computers that are not adequately configured to protect it from unauthorized access;
- disclosing any electronic information without the right to disclose.

In addition to any possible legal sanctions, violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion, pursuant to Rensselaer policies, collective bargaining agreements, codes of conduct, or other instrument governing the individual's relationship with the Institute. Recourse to such actions shall be as provided for under the provisions of those instruments.

6 Approval

This policy is approved under the authority of the President of Rensselaer Polytechnic Institute.

{original signed}	June 27, 2017
Signature	Date

Dr. Shirley Ann Jackson

7 Acknowledgements

The production of this policy borrowed heavily from other sources, including University of California at Berkeley, University of Louisville, University of Minnesota, and the SANS Institute.

8 Revision History

11/22/2016 – Initial version released for comment.