RIT INFORMATION SECURITY POLICY

(with Cross References)

The information assets of Rochester Institute of Technology ("RIT") must be available to the RIT community, protected commensurate with their value, and must be administered in conformance with federal and state law. Reasonable measures shall be taken to protect these assets against accidental or unauthorized access, disclosure, modification or destruction, as well as to reasonably assure the confidentiality, integrity, availability, authenticity of information. Reasonable measures shall also be taken to reasonably assure availability, integrity, and utility of information systems and the supporting infrastructure, in order to protect the productivity of members of the RIT community, in pursuit of the RIT mission.

Definitions:

Information Safeguards: Administrative, technical, and physical controls that support the confidentiality, integrity, availability, and authenticity of information.

Information systems and supporting infrastructure: Information in its analog and digital forms and the software, network, computers, tokens, and storage devices that support the use of information.

Lifecycle Protection: Information systems and supporting infrastructure have a lifecycle that begins with evaluation and selection, and advances through planning, development/acquisition, and operations through to disposal or retirement. Information safeguards are needed at all phases of the lifecycle.

Controls depend on the system, its capabilities, and expected usage, as well as anticipated threats against the information.

> **Preventive controls** include use of encryption, information integrity measures, security configuration, media reuse, use of antivirus, and physical protection
>
> **Detective controls** include network and information access monitoring, and intrusion detection (host based or network based), manual or automated review of security logs
>
> **Corrective controls** include recovery plans from handling isolated information safeguard failure incidents to business continuity plans.

Therefore, RIT will take reasonable steps to:

- Designate one or more individuals to identify and assess the risks to non-public or business-critical information within the Institute and establish an Institute-wide information security plan. (GLB 314, GLB 314.4(a) + HIPAA 164.308(a)(1) + Insurance)
- Develop, publish, maintain, and enforce standards for lifecycle protection of RIT information systems and supporting infrastructure in the areas of networking, computing, storage, human or device/application authentication, human or device/application access control, incident response, applications or information portals, electronic messaging, and encryption. (GLB 314.4(b & c)+ HIPAA - 164.308(a)(1,4,6,7), 164.310, 164.312(a,d,e) + NYS Information Security Breach and Notification Act, + Insurance)

- Develop, publish, maintain, and enforce standards for RIT workforce security related to the responsible use of information. (GLBA 314.4(b)(1) + HIPAA 164.308(a)(1-5))
- Provide training to authorized Institute users in the responsible use of information, applications, information systems, networks, and computing devices. (GLBA 314.4(b)(1) + HIPAA 164.308(a)(2-5))
- Develop, publish, maintain and enforce standards to guide RIT business associates and outsource partners in meeting RIT's standards of lifecycle protection when handling RIT information or supporting RIT information systems and supporting infrastructure. (GLB 314.4(d)(1-2) + HIPAA 164.308(b)(1) + Insurance).
- Encourage the exchange of information security knowledge, including threats, risks, countermeasures, controls, and best practices both within and outside the Institute. (HIPAA 164.308(a)(5))
- Periodically evaluate the effectiveness of information security controls in technology and process. (GLB 314.4(c) + HIPAA 164.308(a)(8), 164.312(b))

*Note: The Gramm-Leach-Bliley Act (GLB) can be viewed at:
http://frwebgate4.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=36433430085+24+0+0&WAISaction=retrieve

HIPAA Security Regulations can be viewed at:

Section 164.306-308 Scope and Administrative Safeguards—http://tinyurl.com/nrhz7
Section 164.3.10 Physical Safeguards—http://tinyurl.com/p9sak
Section 164.312 Technical Safeguards—http://tinyurl.com/qdaud
Section 164.314 Organizational Requirements—http://tinyurl.com/r5sez
Section 164.316 Policy, Procedures and Documentation Requirements—http://tinyurl.com/nlrg5

Analysis of HIPAA at:

Administrative Safeguards—
http://privacy.med.miami.edu/glossary/xd_administrative_safeguards_matrix.htm
Physical Safeguards—http://privacy.med.miami.edu/glossary/xd_physical_safeguards_matrix.htm
Technical Safeguards—http://privacy.med.miami.edu/glossary/xd_technical_safeguards_matrix.htm

"Insurance" indicates that RIT's cyber-risk insurance carrier also has requested information in the area.

For actual legal text see of the NYS law see:

Chapter 442—
http://nysosc9.osc.state.ny.us/product/mbrdoc.nsf/0/e098d3d90ff83fad852570920046f709?OpenDocument
Chapter 491—
http://nysosc9.osc.state.ny.us/product/mbrdoc.nsf/0/5cee53cf1469ba0b852570ca0062b6a1?OpenDocument

Note: The notification law is 442 and chapter 491 provides technical amendments (clarification). Together these add a section 208 to the State Technology Law (to require notification by state entities) and article 39F is added to the General Business Law requiring businesses to provide notification.