



Plain English Guide to the Information Security Policy

RIT has issued an Information Security Policy. The Policy provides the strategic direction needed to implement appropriate information safeguards for RIT information and the Institute network. This Plain English Guide provides explanation and illustration of the Policy and is provided as an aid to help you understand and implement the requirements of the Policy. **The Policy itself is authoritative.** The policy is effective **immediately.**

Why did RIT issue the policy?

The Policy authorizes RIT to take reasonable measures to protect RIT information and computing assets in an age that is both reliant on electronic media and characterized by increasing Internet-borne threats. These measures apply to RIT information and the technology infrastructure.

In recent years, state and federal legislation have mandated specific protections for different types of information, including educational records (FERPA), financial customer information (Gramm-Leach-Bliley Act), health information (HIPAA), and private information (NYS Information Security Breach and Notification Act).

Why is the information lifecycle important?

The information lifecycle concept and its associated stages (creation, storage, transfer, and destruction) provide a useful framework for information handling. For example, during the creation stage, the creator of the information determines who should have access to the information and how that access is to be granted. During the destruction stage, “out-of-date” information or information used only occasionally may be without appropriate protection and be at greater risk.

What are the roles of Safeguards and Controls?

Most of the legislation above requires affected organizations to explain how they know people don't have unauthorized access to information. Controls provide the best way of ensuring information protection. Controls can be process based (administrative controls), or technology based (technical controls). Controls focus on one or more of the following: problem *prevention*, problem *detection*, or problem *correction*.

How has RIT implemented this policy?

RIT has implemented the Information Security Policy by conducting risk assessments, issuing and enforcing standards, raising awareness of threats, recognizing best practices, and maintaining relationships with a number of security-focused external entities for benchmarking and sharing of resources.

More specifically,

- RIT has designated specific individuals, including the RIT Information Security Officer, to identify and assess the risks to non-public or business-critical information within the Institute and establish an Institute-wide information security plan
- The RIT Information Security Office creates and maintains standards to protect RIT information systems and its supporting infrastructure, ensure workforce information security, and guide RIT business associates and outsource partners. The creation of these standards is mandated by policy and is in response to the risks that the Institute faces. They are Institute-wide standards, created with representation from across RIT. See security.rit.edu/standards for a list of current standards and information about how standards are developed.
- The RIT Information Security Office provides awareness and training workshops, including its Digital Self Defense classes to help RIT users in the responsible use of information, applications, information systems, networks, and computing devices.
- The RIT Information Security Office encourages the exchange of information security knowledge through ongoing engagements with security-focused groups, such as Educause, the New York State Cyber-Security Critical Infrastructure Coordination group, InfraGard, and others.
- RIT periodically evaluates the effectiveness of information security controls in technology and process through risk assessments.

To whom does the policy apply?

The policy applies to the entire RIT community, including RIT employees, student employees, volunteers, and external business associates. Standards articulate how you follow the policy. Each standard has a different scope and may apply to different parts of or activities engaged in by the RIT population.

What do I have to do?

You need to follow all Information Security Policy requirements as articulated in the standards. See security.rit.edu/standards/ for a current list of standards.

Where do I go for more information?

Visit our website at security.rit.edu to read the policy and its associated standards. Contact the RIT Information Security at infosec@rit.edu if you have more questions.