

Syracuse University Information Security Standard

Introduction

Syracuse University has developed this Information Security Standard to ensure that SU's technical resources are properly protected, that the integrity and privacy of confidential information is maintained, that information resources are available when they are needed and that users of these resources understand their responsibilities.

Scope

This standard applies to individuals at Syracuse University who use University-owned information, and to the physical and computer environments that support their work.

Assessing Risk

A risk assessment is an important part of any information security process and will help in assigning priorities for mitigating risk. ITS IT Security is in the process of performing a survey-based risk assessment for all SU units and departments, with a key element being the identification of practices and processes surrounding the kinds of information discussed below.

Classification of Data

Risk is strongly tied to the sensitivity of the information, in terms of the potential for damage to individuals and to the University if information is mishandled. We therefore define the sensitivity based on factors including laws and regulations, disruption to business, privacy rights, potential damage to reputation, and potential lawsuits. Our classification scheme defines categories of University information ("University Data") as follows:

- a. Confidential: The most sensitive data to which the maximum reasonable protections must be applied. These data include all Personally Identifiable Information (PII), data covered by regulations and law (Personal Health Information within HIPAA, student records under FERPA, etc.), and other data designated as such by the Data Custodians. Risks from exposure of such data are high and include legal action, fines, and loss of public trust. "Confidential" information can only be shared on a "need to know" basis with individuals who have been authorized by the appropriate Data Custodian or designate, either by their association with specific job functions or explicitly by name.
- b. Enterprise or non-Public: The majority of University Data. Most financial data, e-mail, and internal systems information falls into this classification.
- c. Public: Data that does not fit the above classifications. Public University Data typically would pass the test of "could this be displayed on the campus home page?"

Syracuse University Information Security Standard

Data of higher classification demands a higher degree of protection in all parts of the IT System in which it is stored and accessed. Similarly, Users with access to Confidential must follow more rigorous security procedures and standards, as defined in the remainder of this standard and in other IT Security documents.

Compliance Responsibility

Compliance with Syracuse University IT Policies and Procedures is generally the responsibility of the individual units and departments. However, campus Risk Management, Audit and Management Advisory Services, ITS IT Security, and outside auditors may all investigate reported security problems or perform periodic assessments to verify compliance.

Exposure of Confidential or Enterprise Information

In the event of a breach of these kinds of information, the campus Information Security Officer (ISO) or the CIO must be informed immediately.

Questions

Questions, suggestions, recommendations on SU's Information Security Standard may be directed to the University Information Security Officer (sleonard@syr.edu) or the CIO (pgandel@syr.edu).

Syracuse University Information Security Standard

Information Technology Security Standard for Syracuse University Data

Security always requires a balancing between maximum protection and maximum access and convenience. In some cases, the attempt to protect every piece of information to the utmost level will make normal business operations impractical, if not impossible. Therefore, there are cases where limited collections of Confidential Data may be manipulated under the security requirements of Enterprise Data. The following table summarizes cases where this is acceptable and cases where it is not acceptable, but is not exhaustive. Unless noted, we assume that any Confidential Data requires the protections associated with it in the second table below. The normal IT Security Exception Processes may be used to request changes to these special cases.

Data type	Triggering Criteria for placing in this classification
Confidential	HIPAA information within the Covered Entities is always treated as Confidential. SSN's, credit card numbers, and other data covered by the NY State Disclosure Laws must always be treated as Confidential. Selected collections of student information, notably class lists and grade lists, may be treated as Enterprise Data. Similarly, employee lists that only include names, units, and SUID's may be treated as Enterprise Data.
Enterprise	Any data defined above as Enterprise, including single instances.
Public	All other data.

Requirements for data meeting above criteria:

Data type	Location	Policy
Confidential	Server	Server must be located in the campus data center or other approved data center and must be installed and maintained as prescribed by the ITS Server Security Standard, including meeting all requirements for Confidential Data. Servers must run an ITS-approved operating system that is fully maintainable by the operator.
	Desktop	Desktop computers located in areas open to non-employees and storing Confidential Data must use full disk encryption approved by ITS Security. Desktop PC's must meet all requirements of the ITS Desktop Security Standard.
	Laptop or other mobile storage devices associated with laptops and PDA's (CD's, flash drives,	Any physical transport of Confidential Data must be minimized and must use controls reviewed and approved by ITS Security, as covered in the ITS Desktop Security Standard. Encryption will be mandatory for all such media and devices. Confidential Data covered by New York State Disclosure laws <i>may not</i> be stored on mobile devices.

Syracuse University Information Security Standard

	disk images, etc.)	
	Backup media associated with servers or created by IT staff to backup departmental systems (CD's, flash drives, backup images and tapes, etc.)	Encryption will be mandatory for all such media and devices.
	Network	All Confidential Data must be encrypted at levels approved by ITS Security.
	Applications	Commercial software must comply with all relevant state and federal laws that pertain to the type of Confidential Data being handled and any contracts must reflect these requirements. Any applications developed in-house that provide campus-wide or Internet access to Confidential Data must be coordinated with ITS Security and are subject to a security review.
Enterprise	Server	Server must be located in a facility with auditable access logs. Servers must be installed and maintained as prescribed by the ITS Server Security Standard for Enterprise Data.
	Desktop	Desktop computers must meet the ITS Desktop Security Standard.
	Laptop or other mobile storage devices (CD's, flash drives, disk images and tapes, etc.)	Any physical transport of Enterprise Data must use controls reviewed and approved by ITS Security, as covered in the ITS Desktop Security Standard. Encryption will be mandatory for all such media and devices, except for backup media being handled as part of standard IT staff-provided backup procedures.
	Network	All Enterprise Data must be encrypted at levels approved by ITS Security when transiting insecure network links.
	Applications	Commercial software must comply with all relevant state and federal laws than pertain to the type of Enterprise Data being handled and any contracts must reflect these requirements.
Public	Server	Server must be located in a secured facility. Servers must be installed and maintained as prescribed by the ITS Server Security Standard.
	Desktop	Desktop computers must meet the ITS Desktop Security Standard.

Syracuse University Information Security Standard

	Laptop or other mobile storage devices	Laptops must meet ITS Desktop Security Standard.
	Network	No special requirements.
	Applications	Applications that are used to present Public data must protect against unauthorized modification of the data.