



*Operational—Awaiting Final Approval*

## New York University GUIDELINES

**Title:** Security Guidelines for System Administrators  
**Effective Date:** December 1, 2010  
**Supersedes:** N/A  
**Issuing Authority:** Executive Vice President for Finance and Information Technology;  
Vice President, Information Technology and Chief Information  
Technology Officer  
**Responsible Officer:** Vice President, Information Technology and Chief Information  
Technology Officer

### **Purpose of these Guidelines:**

This document serves as a guide for IT personnel to help them understand the obligations laid out in the security Measures.

### **Scope of these Guidelines:**

The *Policy on Computer and Data Security* requires that computers and data be protected in a manner appropriate to their level of importance. The *Basic, Intermediate, Advanced, and Data Security Measures* provide guidance on what safeguards are considered reasonable and appropriate for computer and data resources of each level of criticality.

### **Statement/Description of the Guidelines:**

The Security Measures are designed to provide resiliency against the current and rapidly changing threat landscape that changes rapidly, and today includes complex and targeted attacks that are often focused on theft of data. They are also designed to provide a sound foundation from which to address external compliance regulations, both legal and contractual, the number and complexity of which continue to grow at a rapid pace. The Measures have been created with consideration of industry best practices, external compliance requirements, and existing NYU policy. This document serves as a guide for IT personnel, to help them understand the obligations laid out in the Security Measures. Questions regarding this document should be sent to ITS Technology Security Services at [security@nyu.edu](mailto:security@nyu.edu).

### **1. Covered Systems:**

These *Measures* are applicable to a wide variety of IT resources which are connected to NYU-NET or are used for any NYU business purpose. A *system* may be any IT resource to which the safeguards outlined in *Security Measures* may be applied. Examples of *systems* include, but are not limited to:

- A. Desktop, laptop, or server computers running general purpose operating systems such as Windows, Mac OS, and Unix
- B. Mobile devices, such as PDAs and cell phones, to the extent that they interact with NYU resources, such as email
- C. Network server applications, such as an FTP-server application
- D. Web applications, such as a wiki
- E. Databases

All of the above *systems* may perform their own authentication and authorization, logging and auditing, and have their own configurations which must be managed, and each of them are a considered a compliance object to be protected

**2. Auditing:**

In order to minimize IT security risk, it is recommended that you integrate compliance auditing into your existing inventory management and auditing framework. Auditing requirements for external standards, such as HIPAA or PCI, are not affected by this document.

**3. Exceptions:**

In some cases, a system may be incapable of implementing a control required by this policy. In such cases, the exception should be documented and approved by the appropriate chain of authority. For high criticality systems managed by ITS, this involves the Risk Review Process. Information about the Risk Review Process is available from ITS Technology Security Services.

**4. Compliance Requirements:**

This section outlines how the various security policies and Measures fit together from the perspective of a system administrator attempting to determine the compliance requirements for a system that they manage.

- A. The first step is to classify the system and the data it processes according to the *Policy on Computer and Data Security, including the Reference for Data and System Classification*. These documents provide a framework for describing the importance of information technology systems and data. They outline three system classifications that represent how severe the impact would be to the University if a system or piece of data were accessed without authorization, or were unavailable to perform its function. The *Data and System Security Measures* rely on these classifications to determine what requirements are applicable.
- B. The second step is to apply the appropriate system controls, based on that system classification. There are three levels of Security Measures, which correspond to the three system classification levels and define the Security Measures that must be applied to each class of system.

System Classification	Security Measures		
	Basic	Intermediate	Advanced
High Criticality	✓	✓	✓
Medium Criticality	✓	✓	
Low Criticality	✓		

The measures are additive, meaning that a low criticality system must implement only the Basic Security Measures, while a high criticality system must implement the Basic, Intermediate, and Advanced Security Measures in order to be compliant. Whenever requirements for different Measures conflict, the requirements in the stricter Measures take precedence.

- C. In addition to the Security Measures for systems, there are Security Measures for handling non-public data. A workstation is able to store small amounts of restricted data and continue to be classified as a low criticality system, but the restricted data stored on that system remains important and must be protected. The Data Handling Security Measures defines protections that "follow the data" and must always be applied regardless of whether the data is on a high, medium, or low criticality system. The protections defined in the Data Handling Security Measures are cumulative with the Security Measures for systems.

## 5. Definitions:

- A. **Availability:** a statement about the need for a system to be operational and accessible by the people who need to use it. There are three (3) categories:
  - a) High: Systems in this category have the highest availability requirements of any group of NYU systems.
  - b) Medium: Systems in this category have the above average availability requirements compared to other NYU systems.
  - c) Standard: Systems in this category have no special availability requirements.
- B. **Data Classification Table:** Classifies data-types which are commonly used at NYU according to the impact to the University if they are disclosed without authorization. There are four categories of data:
  - a) Restricted Data: A category in the Data Classification Table. Unauthorized disclosure of data in this category would have a large impact on the University.
  - b) Protected Data: Unauthorized disclosure of data in this category would have a moderate impact on the University.
  - c) Confidential Data: Unauthorized disclosure of data in this category would have a low impact on the University.
  - d) Public Data: Disclosure of data in this category would have no impact on the University; it is intended for public distribution.
- C. **Data Steward:** Data Stewards are typically operational managers in a functional area with day-to-day responsibilities for managing business processes and establishing the business rules for the production transaction systems and are appointed by the respective Data Trustees. The Data Steward will be responsible for developing an overall data access plan following the categorization in the *Reference for Data and System Classification*. See definition and explanation in the University Data Management Policy (place link or URL here).
- D. **Personal Workstations:** Personal workstations typically do not have network accessible services, and are typically accessed by a single user at a time.

- E. **Security Measure:** Defines the security controls that must be implemented to achieve compliance.
- F. **Server:** Servers are characterized by the presence of network accessible services, they are typically accessed simultaneously by many remote users concurrently, via the network services they provide.
- G. **System:** An information technology resource that can be classified and to which security controls listed in a security measure may be applied. A system may be a workstation, laptop, server, web-application, database, or similar.
- H. **System Classification:** A framework for classifying the relative importance of NYU systems based on their data processing and availability requirements. There are three classes of criticality:
- a) High: Systems in this category are of the greatest importance to the University.
  - b) Medium: Systems in this category are of moderate importance to the University.
  - c) Low: Systems in this category are of average importance to the University.

**Related Policies:**

- *Data and Computer Security Policy*
- *Reference for Data and System Classification*
- *Data and System Security Measures*
- *Security Guidelines for Desktop and Laptop Computers*
- *Policy on Responsible Use of NYU Computers and Data*
- *University Data Management Policy*
- *Policy on Personally Identifiable Information*

Send questions or comments to: [security@nyu.edu](mailto:security@nyu.edu)