NYU Information Technology

Operational—Awaiting Final Approval

New York University
MEASURES

Title: Data and System Security Measures
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 Measures:
This policy applies to anyone who accesses, uses, or controls University computer and data resources, including, but not limited to faculty, administrators, staff, students, those working on behalf of the University, guests, tenants, contractors, consultants, visitors and/or individuals authorized by affiliated institutions and organizations.

Scope of these Measures:
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:

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

Description of these Measures:
The following sections describe the Basic System Security Measures, the Intermediate System Security Measures, the Advanced System Security Measures, and the Data Security Measures.

Alternate Forms of Compliance:

In some cases, a system may be incapable of implementing a control required by these Measures. 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.

A. Basic System Security Measures

The *Basic System Security Measures* apply to all systems at NYU, regardless of the level of their *System Classification*. It is a baseline, which all systems must meet. Note that for most personal workstations, these are the only Measures that apply. The requirements are:

I. **Password Protection:** All accounts and resources must be protected by passwords which meet the following requirements, which must be automatically enforced by the system:
   1. Must be at least eight characters long
   2. Must NOT be dictionary or common slang words in any language, or be readily guessable
   3. Must include at least three of the following four characteristics in any order: upper case letters, lower case letters, numbers, and special characters, such as *!@#$%^&*.
   4. Must be changed at least once per year.

II. **Software Updates:** Systems must be configured to automatically update operating system software, server applications (webserver, mailserver, database server, etc), client software (web-browsers, mail-clients, office suites, etc), and malware protection software (anti-virus, anti-spyware, etc). For *Medium or High Availability* systems, a plan to manually apply new updates within a documented time period is an acceptable alternative.

III. **Firewall:** Systems must be protected a firewall which allows only those incoming connections necessary to fulfill the business need of that system. Client systems which have no business need to provide network services must deny all incoming connections. Systems that provide network services must limit access those services to the smallest reasonably manageable group of hosts that need to reach them.

IV. **Malware Protection**: Systems running Microsoft or Apple operating systems must have anti-virus software installed and it must be configured to automatically scan and update.

B. Intermediate System Security Measures

The *Intermediate System Security Measures* define the Security Measures that must be applied to *medium criticality* and *high criticality* systems. Note that except under special circumstances, they do not apply to desktop and laptop computers. The requirements are:

I. **Authentication and Authorization**
   1. **Remove or disable accounts upon loss of eligibility:** Accounts which are no longer needed must be disabled in a timely fashion using an automated or documented procedure.
   2. **Separate user and administrator accounts:** Administrator accounts must not be used for non-administrative purposes. System administrators must be provisioned with non-administrator accounts for end-user activities, and a separate administrator account that is used only for system-administration purposes.

3. **Use unique passwords for administrator accounts:** Privileged accounts must use unique passwords that are not shared among multiple systems. Credentials which are managed centrally, such as the NetID/password combination, are considered a single account, regardless of how many systems they provide access to.
4. **Throttle repeated unsuccessful login-attempts:** A maximum rate for unsuccessful login attempts must be enforced. Account lockout is not required, but the rate of unsuccessful logins must be limited.
5. **Enable session timeout:** Sessions must be locked or closed after some reasonable period.
6. **Enforce least privilege:** Non-administrative accounts must be used whenever possible. User accounts and server processes must be granted the least-possible level of privilege that allows them to perform their function.

II. **Audit and Accountability**

1. **Synchronize system clock:** The system clock must be synchronized to an authoritative time server run by NYU (currently tick.nyu.edu and tock.nyu.edu) at least once per day.
2. **Enable system logging and auditing:** The facilities required to automatically generate, retain, and expire system logs must be enabled.
3. **Follow an appropriate log retention schedule:** System logs must be retained for 30-90 days and then destroyed unless further retention is necessary due to legal, regulatory, or contractual requirements.
4. **Audit successful logins:** Generate a log message whenever a user successfully logs on.
5. **Audit failed login attempts:** Generate a log message whenever a user attempts to log on without success.
6. **Audit when a system service is started or stopped:** Generate a log message when a system service is started or stopped.
7. **Audit serious or unusual errors:** Generate a log message when a serious or unusual error occurs, such as crashes.
8. **Audit resource exhaustion errors:** Generate a log message when a resource exhaustion error occurs, such as an out-of-memory error or an out-of-disk error.
9. **Audit failed access attempts:** Generate a log message when an attempt to access a file or resource is denied due to insufficient privilege.
10. **Audit permissions changes:** Generate a log message when the permissions of a user or group are changed.
11. **Include appropriate correlation data in audit events**: For each audit event logged be sure to include sufficient information to investigate the event, including related IP address, timestamp, hostname, username, application name and/or other details as appropriate.

III. **Configuration and Maintenance**

1. **Security Partitioning:** Systems may share hardware and resources only with other systems that have similar security requirements, regardless of their *criticality* classification. Systems which share similar security requirements have user communities of similar size and character, similar firewall profiles, and similar technical requirements. For example:
    1) Multiple systems of the same *criticality* may be aggregated together to share hardware and resources provided they have similar security requirements.

2) *Medium criticality* systems may share hardware and resources with *low criticality* systems provided that all systems meet the *intermediate systems Security Measures*, and share similar security requirements.

2. **Follow vendor hardening guidelines:** This document cannot be comprehensive for all systems available. Follow basic vendor recommendations to harden and secure systems.
3. **Disable vendor default accounts and passwords:** Many systems come with default accounts which are publicly known. These accounts should be disabled.
4. **Disable all unnecessary network services:** Processes and services which are not necessary to complete the function of a system must be disabled.

IV. **Additional Requirements**

1. **Report potential security incidents:** Potential security incidents must be reported to ITS Technology Security Services.
2. **Security review:** During the design of the technical architecture, a review of the system must be requested from ITS Technology Security Services.
3. **Vulnerability assessment:** Before system deployment, a vulnerability assessment must be requested from ITS Technology Security Services.
4. **Physical access:** The system must reside in a locked facility, to which only authorized personnel have access.
5. **Documentation:** Create and maintain documentation summarizing the business-process, major system components, and network communications associated with a system.

C. Advanced System Security Measures

The *Advanced System Security Measures* define the Security Measures that must be applied to *high criticality* systems. The requirements are:

I. **Audit and Accountability**

1. **Enable process auditing or accounting:** Enable process auditing or accounting, which generates logs information about the creation of new processes and their system activity.
2. **Audit privilege escalation or change in privilege:** Generate a log message whenever a user changes their level of privilege.
3. **Audit firewall denial:** Generate a log message when the host-based firewall denies a network connection.
4. **Audit all significant application events:** Log all significant application events.
5. **Write audit events to a separate system:** System logs must be written to a remote system in such a way that they cannot be altered by any user on the system being logged.

II. **Configuration and Maintenance**

1. **Follow advanced vendor security recommendations:** This document cannot be comprehensive for all systems and applications available. Conform to best practices and recommendations outlined in vendor security whitepapers and documentation.
2. **Host-based and network-based firewalls:** Systems must be protected by both a host-based and a network-based firewall that allows only those incoming connections necessary to fulfill the business need of that system.

3. **Configuration management process:** Configuration changes must be regulated by a documented configuration and change management process.
4. **Partitioning:** Systems may share hardware and resources only with other systems that have similar security requirements, regardless of their *criticality* classification. Systems which share similar security requirements have user communities of similar size and character, similar firewall profiles, and similar technical requirements. For example:
    1) Multiple systems of the same *criticality* may be aggregated together to share hardware and resources provided they have similar security requirements.
    2) *High criticality* systems may share hardware and resources with *medium* and *low criticality* systems provided that all systems meet the *advanced systems Security Measures*, and share similar security requirements.

III. **Additional Requirements**

1. **Physical access:** The system must reside in a secured, managed data-center.

D. Data Handling Security Measures

These *Data Security Measures* define the minimum security requirements that must be applied to the data types defined in the *Reference for Data and System Classification*. Some data elements, such as credit card numbers and patient health records, have additional security requirements defined in external standards. In addition, access and use of University Data is covered by the *University Data Management Policy*. Please be sure to consult all appropriate documents when determining the appropriate measure to safeguard your data.

The best way to safeguard sensitive data is not to handle it at all, and business processes that can be amended to reduce or eliminate dependence on *restricted data* should be corrected. For example, the University ID number can often be substituted for a social security number and poses much less risk if accidentally disclosed.

I. **Requirements for Handling Confidential Data**

a. **Access control:** Access to *confidential data* must be provided on a least-privilege basis. No person or system should be given access to the data unless required by business process. In such cases where access is required, permission to use the data must be granted by the *data steward*.
b. **Sharing:** *Confidential data* may be shared among the NYU community. It may be released publicly only according to well-defined business processes, and with the permission of the data steward.
c. **Retention:** *Confidential data* should only be stored for as long as is necessary to accomplish the documented business process.

II. **Requirements for Handling Protected Data**

a. **Access control:** Access to *protected data* must be provided on a least-privilege basis. No person or system should be given access to the data unless required by business process. In such cases where access is required, permission to use the data must be granted by the *data steward*.
b. **Sharing:** *Protected data* may be shared among the among University employees according to well-defined business process approved by the *data steward*. It may be released publicly only according to well-defined business processes, and with the permission of the *data steward*.

c. **Retention:** *Protected data* should only be stored for as long as is necessary to accomplish the documented business process.
d. **Incident Notification:** If there is a potential security incident that may place *protected data* at risk of unauthorized access, ITS Technology Security Services must be notified.

III. **Requirements for Handling Restricted Data**

a. **Collection:** Restricted data should only be collected when all of the following conditions are met:
    i. The data is not available from another authoritative source,
    ii. The data is required by business process, and
    iii. You have permission to collect the data from the appropriate *data steward*.
b. **Access control:** Individuals must be granted access to restricted data on a least-privilege basis. No person or system may access the data unless required by a documented business process. In such cases where access is required, permission to use the data must be granted by the *data steward*.
c. **Access auditing:** Enable file access auditing to log access to files containing restricted data.
d. **Labeling**: Portable media containing restricted data should be clearly marked.
e. **Sharing:** Access to restricted data can be granted only by a *data steward*. No individual may share restricted data with another individual who has not been granted access by a *data steward*.
f. **Idle Access:** Devices which can be used to access *restricted data* must automatically lock after some period of inactivity, through the use of screensaver passwords, automatic logout, or similar controls.
g. **Transit encryption:** Restricted data must be encrypted during transmission with a method that meets the following requirements.
    i. Cryptographic algorithm(s) are listed in FIPS 140-2 Annex A, the list of approved security functions.
    ii. Cryptographic key lengths meet best-practices for length, given current computer processing capabilities.
    iii. Both the source and destination of the transmission must be verified.
h. **Storage encryption:** Restricted data must be encrypted using strong, public cryptographic algorithms and reasonable key lengths given current computer processing capabilities. Keys must be stored securely, and access to them provided on a least-privilege basis (see ISO 11568 for recommendations on securing keys). If one-way hashing is used in lieu of reversible encryption, salted hashes must be used.
    i. Encrypt files containing restricted data using different keys or passwords than those used for system logon.
    ii. Encrypt data stored in databases at the column-level.
    iii. In addition to file and/or database encryption, implement full-disk encryption on portable devices containing restricted data.
i. **Retention:** Restricted data should only be stored for as long as is necessary to accomplish the documented business process.
j. **Destruction:** When restricted data is no longer needed it should be destroyed using methods that are resistant to data-recovery attempts such as cryptographic

data destruction utilities, on-site physical device destruction, or NAID certified data destruction service.

k. **Incident Notification:** If there is a potential security incident which may place *restricted data* at risk of unauthorized access, ITS Technology Security Services must be notified.

Definitions:

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.

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*.

Personal Workstations: Personal workstations are typically accessed by a single person at a time, and do not offer services to multiple account holders. These may be laptops, desktops, or other portable computing devices, such as PDAs or smart phones.

Server: Servers are systems typically accessed by many remote users concurrently, via the network services they provide, such as an email server.

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.

System Classification: A framework for classifying the relative importance of NYU systems based on their data processing and availability requirements.

For assistance with applying these Measures appropriately, see *Security Guide for Desktop and Laptop Computers* or *Security Guidelines for System Administrators.* **Send questions or comments to:** security@nyu.edu

Related Policies:

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