NYU Information Technology

Operational—Awaiting Final Approval

New York University

Reference for Data and System Classification

Covered Systems:
This classification is 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 security safeguards may be applied. Examples of *systems* include, but are not limited to:

1. Desktop, laptop, or server computers running general purpose operating systems such as Windows, Mac OS, and Unix
2. Network server applications, such as an FTP-server application
3. Web applications, such as a wiki
4. 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 is considered a compliance object to be protected.

Follow these steps to determine a system's classification:
1. Determine the *Data Classification* of the data stored on the system
2. Determine the *Availability Requirements* of that system, including whether it is a server, or personal workstation
3. Select the appropriate Classification from the *System Criticality Table*

A system owner may choose to classify a system as higher criticality than that indicated by the table. However, if they choose to do so, the system must meet the security measures for that higher level.

Data Classification:
The authoritative source of information on data classification at NYU is the University *Data Classification Table*. It outlines four levels of data classification which are related to the impact of an unauthorized disclosure of the data in question. For the convenience of the reader, the data types are listed below along with descriptions and examples; however the table linked above is always the most accurate and up-to-date source of information on data classification.

Data Classification	Institutional Risk from Disclosure	Description	Examples
Restricted	High	Data whose unauthorized access or loss could	• Social Security Number • Driver's License Number

		seriously or adversely affect NYU, a partner, or the public.	• Bank/Financial Account Number • Credit/Debit Card Number (see Special Data Types) • Electronic Protected Health Information • Central Authentication Credentials, when stored in large numbers • University Financial Data on Central Systems
Protected	Medium	Data with a less high level of importance, but that should be protected from general access.	• University Intellectual Property • University Proprietary Data • Passport Numbers • Final Course Grades • FERPA-covered records • External Steward Data • Human Resources Data
Confidential	Low	All other non-public data not included in the Restricted or Protected classes	• NetID • University Identification Number • Licensed Software • Other University Owned Non-Public Data
Public	None	All public data	• General access data, such as that on unauthenticated portions of www.nyu.edu

DRAFT

Special Data Types:

- Credit Card numbers are subject to specific industry standards and thus may need to be handled differently in some situations.
- Other data covered by export controls are subject to additional rules on distribution, in particular sharing with non-U.S. persons (link here to NYU export control policy).

The system classification framework draws a distinction between systems which store data directly, systems which have privileged access to data, but which do not store it directly, and systems which make general use of data, as follows:

- "Storing" data indicates that the data is transparently available through normal file system access methods. For example, data residing in NFS mounts or Windows mapped drives (e.g., an X: drive) is considered to be stored on any client systems which actively mount the shares, as well as the system which physically houses the disks. However, data residing in a database is considered to be stored only on the database server itself since no file system access methods allow clients to obtain direct access to the data.

- "Privileged Access" exists when there is a non-file system method of accessing data that is stored on another system. For example, a web server that connects to a separate back-end database server has privileged access to data stored on that system. Similarly, the workstation of a system administrator who commonly logs into both servers with administrator credentials has privileged access to both systems.
- "General use" includes access or processing of data by end-user workstations, using a non-privileged account.

Availability Requirements:
There are three availability classifications, which represent the impact to the University if a given system were unavailable to perform its task.

Availability Classification	**Institutional Risk from Downtime**	**Description**	**Examples**
High Availability	High	Loss of access to the system could have a significant impact on NYU, a partner, or the public.	• Systems participate in a University-level disaster preparedness plan • Systems participate in the ITS XSC initiative • Systems have redundant hardware in separate geographic regions • Systems that serve 10,000 or more users
Medium Availability	Medium	Loss of access to the system could have a significant impact on a large number of users or multiple business units.	• Systems participate in the disaster preparedness plan of a large University unit • Systems have redundant hardware in a single geographic region • Systems serve 1,000 to 10,000 users
Standard Availability	Low	Loss of access to the system could have a significant impact on an individual user or Unit.	• Systems do not participate in a disaster preparedness plan • Systems have no redundant hardware provisioned • Personal workstations • Small workgroup servers

Server/Personal Context:

DRAFT

- *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.
- *Personal Workstations* typically do not have network accessible services, and are typically accessed by a single user at a time.

System Criticality Categories:
System Criticality is determined according to the following table, when more than one category applies, the system should be classified in the highest applicable category.

System Classification	Classification Guidelines	Examples
High Criticality	Servers that store *Restricted Data* OR servers that host *High Availability* applications	• A human resources database which stores employee social security numbers for tax purposes • The nyu.edu homepage which is designated as a channel for distributing information in the event of a campus emergency
Medium Criticality	Servers that store *Protected Data* OR servers that have privileged access to systems that store *Restricted Data* OR servers that host *Medium Availability* applications	• A departmental file server where salary and benefits information is stored • A web-server which stores no data locally, but which runs an application that accesses a human resources database stored on a separate database server that contains social security numbers of employees for tax purposes • The email server for a school which is required to deliver email messages to students in the event of an emergency
Low Criticality	Servers that store only *Confidential* or *Public Data* OR servers that have privileged access to systems that store *Protected Data* OR servers that host *Standard Availability* applications OR personal workstations	• All personal workstations • All IT systems that are not classified as *Medium* or *High Criticality* • Workgroup servers that do not store *Protected* or *Restricted Data*

Related Policies:
- *Policy on Responsible Use of NYU Computers and Data*
- *University Data Management Policy*
- *Data and Computer Security Policy*
- *Measures for Data and System Security*

DRAFT

- *Security Guidelines for Desktop and Laptop Computers*
- *Security Guidelines for System Administrators*
- *Policy on Personally Identifiable Information*

Send questions or comments to: security@nyu.edu

DRAFT