Policy on Responsible Use of NYU Computers and Data

PURPOSE OF THIS POLICY

New York University is a not-for-profit research university, and its facilities, including *computer and data resources*, are to be used in furtherance of its not-for-profit, educational, research, and service purposes. More and more university activities are conducted using computers and electronic communications, with increased convenience and accessibility from and to all parts of the world. At the same time, today's inter-connected environment intensifies the risks and threats of unauthorized access to computers, inadvertent disclosures of *sensitive data*, and unexpected destruction of essential information, resulting in potentially serious consequences to individuals and to institutions. *Members of the University community* and *affiliates* interact with a wide spectrum of *sensitive data* for numerous reasons. Evolving federal and state regulations require organizations and individuals to safeguard sensitive data. With computing so widely distributed throughout NYU, the responsibility to safeguard computers and data resources extends to all *members of the University community* and *affiliates*.

SCOPE OF THIS POLICY

This policy applies to *members of the University community* and *affiliates* who use NYU's *computer and data resources* and/or who have access to *sensitive data* sent, transmitted, viewed, received, or stored on these resources.

POLICY DEFINITIONS

1. *Affiliates* refers to individuals who have contractual or other relationships with the University and who are not employees, faculty, or students.

2. *Authorization* in this context means to grant permission to an identified individual to use a *computer or data resource.* Acceptance of *authorization* to use NYU *computer and data resources* establishes an obligation on the part of the individual to use those resources responsibly.

3. *Computer and data resources* include computers and computing devices, both wired and wireless; computing, application, and database access (including passwords); software, hardware, computer, and email services; and associated computing accounts. Computers and computing devices include, but are not limited to, desktops or laptop computers, smartphones and cellphones, USB flash memory drives, or similar devices, and all other mobile devices on which High Risk Data may be sent, transmitted, viewed, received or stored.

4. *Members of the University community* refers to full- and part-time employees, faculty, and students.

5. *Sensitive data* include, but are not limited to, information about prospective, current, and former students, patients and clients of medical and dental facilities and services, and users of legal and other services, employees and donors; also information concerning research and University business, finance and operations, and passwords. Federal and state laws and regulations, as well as University policies and office procedures, regulate the handling and reporting of many different kinds of *sensitive data*. Refer to the University's *Electronic Data and System Risk Classification Policy*. International, federal and state laws and regulations, as well as University policies and office procedures, regulate the handling and reporting of many different kinds of data. Check with the NYU IT Global Office of Information Security if you are unsure of the classification of particular data.

UNIVERSITY POLICY

New York University expects *members of the University community* and *affiliates* to employ reasonable and appropriate administrative, technical, and physical safeguards to protect the *computer and data resources* that they use and the *sensitive data* stored on these resources. Access to *computer and data resources* (including software, hardware,

computer, and email services) are privileges extended to *members of the University community* and *affiliates*, and must be exercised in conformity with all applicable NYU policies and procedures and all applicable federal and state laws. Access to NYU *computer and data resources* is limited to authorized persons and is for approved purposes only. Approved purposes are those consistent with both the broad instructional and research goals of the University and the person's relationship with the University. *Authorization* to use these resources is granted by designated individuals at the University entrusted with overall responsibility and management of data and related systems. Acceptance of *authorization* to use NYU *computer and data resources* establishes an obligation on the part of the individual to use these resources responsibly as defined in the Policy Requirements and Specifications below.

This policy does not form a contract of any kind, including, among others, an employment contract. The University reserves the right to modify this policy without notice and at its discretion. The current version of this policy is posted on the NYU IT website (www.nyu.edu/it/policies). All terms noted in *italics* are defined at the beginning of this policy.

POLICY REQUIREMENTS

A. Acceptance of *authorization* to use NYU *computer and data resources* establishes an obligation to:

1. behave in accordance with NYU's educational, research, and service purposes and in a manner compliant with this and other applicable NYU policies and procedures and all applicable laws and regulations;

2. not use your account for any commercial purposes;

3. behave with civil regard for other members of the NYU community and of the wider community on the Internet;

4. take reasonable steps to ensure that any computer used to access NYU resources, whether it is located on an NYU campus or elsewhere, is secure, virus-free, and otherwise not compromised;

5. protect the confidentiality, security, integrity, and recoverability of all *computer and data resources* and take reasonable and appropriate steps to guard these resources from improper or unauthorized use, including such use by third parties;

6. use applications that conform to NYU's privacy and security policies and guidelines;

7. refrain from activities that interfere with the ability of others to use *computer and data resources*; and

8. be aware of and comply with other relevant school and University policies, procedures, and business rules and applicable local laws and regulations; in all cases the more stringent standard should be followed.

B. This obligation applies regardless of:

1. where the computer used to access *computer and data resources* is located in an NYU office, classroom, public space, or lab, or at home or elsewhere outside the University;

2. who owns the device used to access or store the *sensitive data*; or

3. the form or manner in which *sensitive data* are stored or transmitted, including, but not limited to, local file, shared file, file on removable media such as CD-ROM disk and jump drive, central database, fax, printer, copier, network, phone, email, or voice mail.

C. Access and use, or causing or allowing access and use, of *computer and data resources*, including email services, by anyone other than as permitted by NYU is strictly prohibited by NYU and by state and federal laws and may subject the violator to criminal and civil penalties as well as NYU-initiated disciplinary proceedings.

D. Use of some NYU *computer and data resources* may be governed by additional University, college, school, or departmental policies and procedures. Anyone authorized to use these resources is responsible to become familiar with and abide by such policies and procedures.

E. In order to safeguard the security and efficiency of *computer and data resources*, NYU computer systems and NYU-NET are routinely monitored and recorded for integrity and operation of the system by authorized University staff. *Computer and data resources* provided by NYU are the property of NYU and not the personal property of the individual.

F. Designated individuals at the University entrusted with overall responsibility and management of *computer and data resources* and *sensitive data* and related systems have decision-making authority for authorizing access to and use of those resources and systems.

1. These individuals at the University include, but are not limited to, University-wide administrators, such as the Registrar, Deans, and other School administrators, and the Vice Provost for Research on data-intensive research projects.
2. These individuals at the University have responsibility for the development, implementation, and maintenance of policies and procedures related to authorizing access to the shared stores of the various categories of *sensitive data* in use in electronic form at NYU and for handling that data appropriately wherever it resides. Such individuals may delegate responsibilities as they deem appropriate in specific functional areas.
3. These individuals at the University may have more stringent standards for the use, storage, and transmittal of the data they manage than those set forth in this policy; the more stringent standard should be followed. Individuals authorized to use the data are expected to be aware of relevant current policies and to abide by them.
4. Access to *sensitive data* will be granted only on an "as needed/minimum necessary" basis.

G. New York University's Vice President, Information Technology & Global University Chief Information Officer is responsible for periodic reviews of the University's security policies and procedures relating to *computer and data resources* and *sensitive data*, which will be

revised as necessary and any updates publicized. Current versions of the University's policies relating to *computer and data resources* and *sensitive data* are maintained on the NYU IT website (www.nyu.edu/it/policies). Questions for clarification and suggestions about these policies can be sent to cio.policies@nyu.edu.

H. Violators of this policy may be subject to disciplinary action, up to and including the termination of employment or contract with the University, or, in the case of students, suspension or expulsion from the University. Anyone who knows or has reason to believe that another person has violated this policy shall report the matter promptly to his or her supervisor, in the case of students to the Division of Student Affairs, Director of Judicial Affairs, or to cio.policies@nyu.edu, as appropriate. Any attempt to retaliate against a person for reporting a violation will itself be considered a violation of the policy and may result in disciplinary action up to and including the termination of employment or contract with the University. The appropriate office or entity, including the Office of the Vice President, Information Technology & Global University Chief Information Officer, the Office of General Counsel, and other University officials as required, will lead the investigation into all alleged violations or reports of violations of this policy and, where appropriate, will take steps to remedy the situation.

SPECIFICATIONS

A. NYU Computer Security

Computer security controls are based on the construct that the data on an individual machine/device influences the classification of that machine/device and, in turn, the multi-layer security strategy for defense against unauthorized access. See the *Data and System Security Policy* at www.nyu.edu/it/policies.

1. Safeguarding Computers for Individual Use

This section describes measures to safeguard computers typically used by individuals in NYU-related activities and for accessing other University resources, such as NYU-NET. As used in these operational specifications, "computers" include but are not limited to

desktops or laptop computers, smartphones and cellphones, USB flash memory drives, or similar devices.

a. Physical Security

i. Do not give physical access to computers to unauthorized persons.

ii. Take appropriate precautions to prevent theft and damage.

iii. Where possible, position monitors to prevent casual viewing by visitors or passersby.

b. System Security

i. Install anti-virus software and keep virus definitions up to date.

ii. Install operating system and software patches and take other recommended steps to mitigate known vulnerabilities of the computer in a timely manner.

iii. Use only NYU-approved software; do not download unauthorized software.

iv. Use a locking screensaver or other mechanism to prevent unauthorized use of the computer.

v. Do not leave your computer unattended without locking it or logging off.

vi. Do not install or use Peer-to-Peer file sharing software; these programs typically enable unauthorized remote access without any password to the contents of the computer.

vii. Do not install or run software that requires a license without that license. Respect license agreements and do not infringe on the copyright of others. (See section A.5)

viii. Respond promptly to notices from authorized University staff that vulnerabilities have been detected in your computer's system.

ix. Take particular care to secure your NYU-access information (e.g., log-ins, passwords) on home computers from unauthorized use by others.

x. Do not install unsecured third-party applications that may deliver malware to a personal device on which you may have High Risk Data, thereby putting NYU at breach risk.

c. Passwords

i. Where possible, secure all computer accounts with passwords, and use passwords to protect all file sharing.

ii. Use strong passwords. Strong passwords consist of at least eight (8) characters. They should not be dictionary words or readily guessable. They should include at least three (3) of the following four (4) characteristics in any order: upper case letters, lower case letters, numbers, and symbols.

iii. Change passwords periodically. Avoid reusing a password for at least several change iterations. If you have multiple accounts, avoid using the same password for those accounts. Additional information about passwords may be found in the ServiceLink knowledge base.

iv. Do not keep passwords in plain text in a computer file or in plain sight on paper. Passwords should neither be sent in an email nor provided verbally by telephone. If you must communicate account access information in order to ensure business continuity, you should communicate it in a secure manner. Supervisors and managers should make certain that offices have plans for access to files and data for business continuity.

v. Keep a well-secured copy of your passwords available for emergency access. Encrypt any computer file containing passwords. Keep any written file of passwords in a physically secure location, preferably separate from the computer or application they secure.

vi. Passwords for sensitive websites or email accounts should not be saved on the computer.

vii. Where possible, do not configure programs to automatically store passwords.

viii. Shut down web browsers, email programs, or other applications that might store passwords temporarily when they are not in use.

d. Remote Access

i. Any remote computer used to access NYU resources must conform to these Specifications and may be subject to further resource-specific restrictions.

ii. If you do not maintain or control the remote computer, do not use it for access to, or transmission of, *sensitive data*. Access to non-*sensitive* data may be permissible. Check with the responsible department or a supervisor for guidance.

iii. Use remote access software and services with caution. Pay special attention to the configuration of remote access software, hardware, and services to ensure that they do not present a security risk to your computer or to NYU. Consult with the NYU IT Global Office of Information Security (security@nyu.edu) for guidance on how to choose, set up,

and operate remote access technologies.

iv. Obtain prior *authorization* from both your senior management and the NYU IT Global Office of Information Security (security@nyu.edu) before using a modem with a computer connected to the University network. Modems present a significant security risk because they enable unmonitored and uncontrolled remote access to NYU's network and data.

v. Ensure that your computer is not configured to allow unauthorized access to NYU's network by other devices. Special access arrangements, such as wireless access, RAS (Remote Access Server) services access, and sharing network connections, must be authorized by the NYU IT Associate Vice President, Global Infrastructure and Operations (GIO).

2. Safeguarding Computers Used by Multiple Individuals

The section covers additional measures for safeguarding computers used by multiple individuals. All the operational specifications set forth above apply, as well as the following additional measures to safeguard such computers.

a. Secure all computer accounts with passwords.

b. Give accounts to authorized persons only; provide individual log-ins. If you share a computer with others, take appropriate precautions to safeguard *sensitive data* that others may not be authorized to access and, where possible, create separate accounts for each person who is authorized to use the computer, setting appropriate permissions.

c. Where possible, enforce use of strong passwords and periodic password changes.

d. Make every effort to maintain computer logs and review them on a regular basis.

e. Stay familiar with best practices for administering the particular computer and use them.

3. Business Continuity

Take reasonable steps to ensure that, in case of emergency, another authorized person is able to access the NYU computer you use in order to provide continuity of NYU functions performed on and through it. The University's business interests should be balanced with data safeguards and privacy. There are numerous methods available of ensuring shared responsibility for data and systems rather than sharing passwords. For assistance, contact the NYU IT Global Office of Information Security (security@nyu.edu).

<u>4. Purchasing</u>

Discuss adherence to applicable NYU policies and procedures as part of the purchasing process. Computers and software acquired for use with NYU *computer and data resources* should conform to these specifications.

<u>5. Software Licensing</u>

Software users shall use and install only properly licensed software on NYU computers and the NYU network.

a. *Unauthorized* duplicating, distributing, downloading, sharing, selling, or installing software and related documentation or using unlicensed software and related documentation constitutes a violation of the software license agreement and of University policy.

b. Each School, department, or other unit is responsible for ensuring that software used on their computers is properly licensed, for adhering to the terms and conditions of those software licenses, and for maintaining appropriate documentation of those software licenses.

c. Upon separation from NYU, all University-owned software, including all NYU-licensed software, must be removed from non-NYU owned computers. This includes mobile devices, laptops, and home computers. If you have software on your office computer that permits you to install a second copy on your home computer, remove that second copy.

<u>6. Equipment Disposal or Redeployment</u>

a. Before disposing of or re-deploying hardware, comply with University computer disposal guidelines, which can be found at www.nyu.edu/asset. See also Computer Disposal Guidelines.

b. Disposing of or re-deploying personal devices which stored High Risk Data should be accomplished thoroughly, expunging all High Risk Data. See the *Standard for Destruction and Disposal of Electronic Equipment and Data*.

B. NYU Data Security

How you handle non-public data depends on its data classification. The more restrictive the data is, the better it should be secured. Consult the *Data Handling Security Measures* section of the *Data and System Security Policy* for specific requirements; the following are more general requirements.

1. Protecting *Sensitive Data* on Computers

a. Follow *NYU Computer Security Specifications* set forth above.

b. Know what data are stored on your computer, the sensitivity of that data, and what policies apply.

c. Keep local data retention to a minimum. Rely on unit, school, or University storage where you can.

d. Where possible, password protect or encrypt *sensitive data*.

e. Back up local data on a regular basis and keep the backup secure. Protect backups with the same level of security as the original data. Test backup recovery periodically to verify that it works.

f. If you use a computer shared with others, take appropriate precautions to safeguard *sensitive data* that others may not be *authorized* to access. Where possible, create separate accounts for each person who uses the computer, setting appropriate permissions.

2. Storing or Transmitting Sensitive Data

a. Do not redistribute *sensitive data* to others within or without the University, unless you are an authoritative source for and an authorized distributor of that data and the recipient is authorized to receive that data.

b. Do not allow *sensitive data* to be stored on computers or servers outside NYU, unless such storage is authorized.

c. Whenever possible, *sensitive data* should be transferred in encrypted form, e.g., using SSL (Secure Socket Layer) or SSH (Secure Shell).

d. Remember that email typically is not a secure form of communication. Care should be taken to be certain that the recipient is authorized to receive that data and the address is accurate.

e. *Sensitive data*, including electronic protected health information (EPHI), Social Security numbers, or credit card information, should not be sent unencrypted via email. If use of email is necessary, use encryption technology to protect the transmission of *sensitive data* in email. This may include the use of VPN (Virtual Private Network), SSL, or encryption of the message itself using software such as PGP (Pretty Good Privacy).

f. Do not transmit *sensitive data* using instant messaging technology such as Slack, WhatsApp, and Facebook Messenger, which use servers outside of NYU. These services may allow *sensitive data* to be accessed by or stored by unauthorized parties. It is recommended that you consult with NYU IT Global Office of Information Security (security@nyu.edu) for guidance.

g. Take special care when sending *sensitive data* by fax to make sure that it is clearly marked as confidential. Every effort should be made to ensure that only the intended recipient has access to the faxed information.

h. Keep fax machines, printers, and copiers used for sensitive data in secure areas. Faxes, printouts, and copies of *sensitive data* should be picked up promptly and handled appropriately.

3. Disposing of Sensitive Data

a. *Sensitive data* should be destroyed in a manner that prevents re-creation.

b. Reformat or physically destroy any removable storage media (such as floppy disks, zip disks, tapes, or compact disks (CD)) that contained *sensitive data* before disposing of them.

c. Shred printouts of *sensitive data*.

d. Ensure that *sensitive data* are removed from devices you use, including remote printers, before you dispose of or re-deploy those devices.

4. Responding to Requests for Information

a. Do not share *sensitive data* with representatives of the press (radio, television, print, or electronic media), other individuals, or in public forums, such as mailing lists or web bulletin boards, without appropriate *authorization*.

b. Refer subpoenas and similar requests or demands for the release of *sensitive data* to the Office of General Counsel.

Notes

1. **Dates of Official Enactment and Amendments:**

   a. Adopted by the Office of the Chief Information Technology Officer (CITO) on February 6, 2006.

   b. Included a section on Software Licensing (Section A.5), January 14, 2009.

   c. Added a sentence regarding commercial purposes (Policy Requirements, Section A), December 12, 2011.

   d. Updated NYU Information Technology Services (ITS) references and links to new organizational name: NYU Information Technology (NYU IT), October 26, 2015.

   e. Revisions made throughout to reflect updated technological terminology, June 2, 2016.

   f. Changed title designation from Vice President, Information Technology and Chief Information Technology Officer to Vice President, Information Technology and Chief Information Officer; and revised office designation from NYU IT Technology Security Services to NYU IT Office of Information Security, October 3, 2016.

   g. Updated the cito.policies@nyu.edu email address to cio.policies@nyu.edu, February 23, 2018.

   h. Updated the Data Classification Table title and link to point to the new Electronic Data and System Risk Classification Policy, December 4, 2018.

   i. Changed title designation from Vice President, Information Technology and Chief Information Officer to Vice President, Information Technology & Global University Chief Information Officer, and the revised office designation from NYU IT Office of Information Security to NYU IT Global Office of Information Security, March 9, 2020.

2. **Cross References:**

   a. NYU Guidelines for compliance with the Family Educational Rights and Privacy Act (FERPA)

b. [NYU Information Technology Policies](#)

c. [NYU HIPAA Information Security Policies](#)

d. Guidelines on equipment disposal or redeployment: [Asset Management](#) and [Standard for Destruction and Disposal of Electronic Equipment and Data](#).

e. Email address for computer security assistance and advice: security@nyu.edu

f. Email address for policy clarifications and suggestions: cio.policies@nyu.edu

g. Email address to report policy violations: cio.policies@nyu.edu

---

Notes

1. Dates of official enactment and amendments: Feb 6, 2006

2. History: Last Review: November 2, 2021. Last Revision: March 9, 2020.

3. Cross References: See above

About This Policy

Effective Date

Feb 6, 2006

Supersedes

N/A

Issuing Authority

Executive Vice President

Responsible Officer

Vice President, Information Technology and Global University Chief Information Officer

---

+ Definitions

+ Related Policies