

YOUR KEY OBLIGATIONS

When you accept the privilege of using NYU's computer and data resources, you are obligated to:

- **be aware** of and comply with all relevant school and University policies;
- **protect** the confidentiality, security, integrity, and recoverability of all computer and data resources;
- **behave** in accordance with NYU's purposes and policies and all applicable laws and regulations.

These obligations apply to you regardless of:

- the location of the computer used to access computer and data resources—in an NYU office, classroom, public space or lab, or at home or elsewhere outside the University;
- the owner of the device used to access or store the sensitive data;
- the form or manner in which sensitive data are stored or transmitted (including, but not limited to, local file, shared file, central database, fax, printer, copier, network, phone, e-mail, or voice mail).

Help & More Information

The following resources can help you fulfill your obligations concerning your use of NYU computers and data:

- *Policy on Responsible Use of NYU Computers & Data:* www.nyu.edu/its/policies/responsibleuse.html
- *Policy on Personal Identification Numbers:* www.nyu.edu/provost/policies.html
- NYU Information Technology Services Policies: www.nyu.edu/its/policies/
- ITS Top Ten Computer Security guidelines: www.nyu.edu/its/security/guidelines.html
- For technical questions, contact the ITS Client Services Center at 1-212-998-3333 or its.clientservices@nyu.edu
- Make a note of contact information for local technical assistance at your school or department here:

Please help us spread the word about Responsible Use!

Understanding Your Obligations for the Responsible Use of NYU Computers & Data

When you are authorized to use NYU's computer and data resources, including NYU-NET and NYUHome, or have access to sensitive data stored on those resources, you have an obligation to abide by the *Policy on Responsible Use of NYU Computers & Data*.

Learn about your obligations »

A publication of...



NEW YORK UNIVERSITY
Information Technology Services

© 2006 – NYU. All Rights Reserved. 5-06. ITS Pub.# 2006-04a.
<http://www.nyu.edu/its/>. Comments? Write to its.pubs@nyu.edu.

Start above, then continue inside for further details

Protect the Computers You Use

- **Install anti-virus and anti-spyware software** and keep definitions up-to-date
- **Install operating system and software patches, and set automatic updates** for computer
- **Use a locking screensaver** or other mechanism to prevent unauthorized use
- **Create separate accounts for each person** authorized to use the computer and limit their permissions, as appropriate
- **Do not install or use peer-to-peer file sharing software**, such as KaZaA or Gnutella
- Ensure that your computer is not configured to allow unauthorized access to NYU's network by other devices (e.g., no unauthorized wireless access points)
- **Comply with the University's computer disposal guidelines** (<http://www.nyu.edu/asset/>) before disposing of or redeploying hardware
- For information about computer security, see:
 - www.nyu.edu/its/security/docs.html
 - www.nyu.edu/its/pubs/pdfs/securing_windows.pdf
 - www.nyu.edu/its/pubs/pdfs/personal_firewalls.pdf

COMPUTERS

Protect Your Passwords

- **Secure all computer accounts with passwords**; password-protect all file sharing and use file sharing sparingly
- **Use strong passwords**: At least eight (8) characters; no dictionary words or readily-guessable words; at least three (3) of the following in any order: upper case letters, lower case letters, numbers, and symbols
- **Change passwords** at least once a year; avoid reusing a password for at least several change iterations
- **Do not keep passwords in plain text** in a computer file or in plain sight on paper
- **Do not send passwords** in an e-mail or provide passwords verbally by telephone
- **Do not configure programs to store passwords automatically**
- **Do not reuse your password** among different accounts
- For FAQs regarding passwords, see: www.nyu.edu/its/faq/passwords/

PASSWORDS

Protect NYU's Sensitive Data

- **Password-protect or encrypt sensitive data**, where possible
- **Do not store sensitive data unless approved to do so**. Keep sensitive data retention on desktop and laptop computers and mobile devices to a minimum; back up data regularly and keep the backup secure
- **Do not transmit sensitive data via e-mail**, unless encryption technology is used to secure the data in the e-mail message
- **Do not transmit sensitive data using instant messaging technology** (e.g., AOL Instant Messenger, Yahoo Messenger)
- **Remove sensitive data from devices before disposing of or re-deploying them**
- **Destroy sensitive data** in a manner that prevents re-creation; shred printouts
- **If you share a computer with others**, take appropriate precautions to protect sensitive data that others may not be authorized to access

SENSITIVE DATA