



**The College at Brockport
State University of New York**

Category:

Office of Human Resources

Responsible Office:

Office of Human Resources

Policy Title:

Maintaining the Security,
Confidentiality & Integrity of Personal
Information

Policy:

The College has an obligation to protect the information of those we employ and those we serve. Always comply with the following, and point out any lapses to your supervisor.

We control access to information stored electronically.

- Private personal data of students, alumni, faculty, professional staff or anyone employed by the College may not be stored on laptop computers or any other mobile computing device (e.g., floppy disk, CD, DVD, USB “flash” drive, PDA, etc.) under any circumstances, at any time.
- For purposes of these policies, private personal data include the Social Security Number (SSN), date of birth, driver’s license number, credit card numbers, bank account numbers, and medical information.
- Private personal data transmitted through e-mail must always be in an encrypted form using encryption technologies approved by the College’s Chief Information Officer.
- In the case that any private personal data are stored on any personal computer owned by the College and that computer is lost or stolen, the loss must be reported as soon as it is detected to:
 - University Police
 - The vice president for the division responsible for the lost or stolen computer.
- Any knowledge or suspicion that private personal data in any electronic form have been stolen or otherwise compromised (made public) must be immediately reported to the Chief Information Officer.
- To make possible the proper reporting of theft of private personal information, responsible users should note each College computer on which private personal data is stored.
- When computers containing private personal data are retired from service, attention should be paid to removing the data and to making it impossible to recover the data from the computer’s hard drive(s).

- Workstations are password protected and not accessible to the public unless reviewing an individual's own records.
- We minimize screens not in use, to prevent inadvertent breeches.
- Employees are encouraged to logout or lock their workstations when not in use. However:
 - Tellers may not lock their workstations except for short breaks
 - Management covering the front line must have access to workstations
 - Tellers are encouraged to close their sessions and email when not in use.
- We use strong passwords
 - Network and email access (at least eight characters, alphanumeric, special character)
 - Mainframe access (at least eight characters, alphanumeric)
- We change passwords periodically.
- We do not post our passwords near or on our computers.

We protect personal information.

- We respond to requests for personal information in accordance with FERPA.
- We refer to the appropriate security policies as needed to ensure our compliance.
- We report any fraudulent attempts to obtain personal information to management, who then reports the attempt to the appropriate law enforcement agencies.

We control access to rooms and file cabinets where paper records are kept.

- We lock doors to our offices areas during non-business hours.
- Work areas where personal information is processed are separate from public areas.
- Guests are escorted in areas where personal information is being processed.
- Guests are restricted to areas that do not have personal information in plain view.
- File cabinets used to store personal information are locked or are secured in locked areas.
- The fireproof cabinets used to store promissory notes are locked during non-business hours.

Documents no longer needed are disposed of in designated recycling/shredding containers.