Brock University
Freedom of Information and Privacy Office

Best Practices for Security Measures for Protecting Personal Information

Brock University is subject to the *Freedom of Information and Protection of Privacy Act* (FIPPA) and follows the legislation's requirements regarding the collection, use, retention, disclosure and disposal of personal information in the University's custody or control. These best practices reflect Brock's commitment to protect personal information.

The following are some best practices for security measures to ensure that any personal information accessible to employees remains confidential and protected.

Best Practices of physical security measures:

1. Lock doors and filing equipment when the office is vacant.
2. Locate FAX machines and printers in a secure area, and retrieve sensitive documents immediately.
3. Ensure that sensitive and confidential information is not visible to the public.
4. Label filing cabinets, drawers, boxes and other storage containers in a manner that maintains the anonymity of items in storage.
5. Keep open filing equipment or mail boxes behind a counter or other physical barriers to the public.
6. Where possible, modify office layout to protect confidential information from inappropriate exposure.
7. When transporting confidential information (e.g. student assignments or exams home for marking) ensure secure transportation and that confidentiality is maintained.
8. Ensure records that are the property of the university, in particular student assignments and exams, are not removed from university control when an employment contract is terminated. (i.e. return all student assignments)
9. Ensure confidential destruction of paper records by using a cross-cut shredder or by placing the records in one of the University's locked boxes designated for cross-cut shredding.

Best Practices of procedural security measures:

1. Control distribution and return of keys, and make regular changes to combinations or codes to prevent inappropriate room entry.
2. Ensure that when a Computer Account Application form is completed, the request for access is only for information that the employee will need to do their job.
3. Notify Information Technology Services if there is a change in an employee's employment status.
4. Do not disclose passwords or PINs, to ensure only authorized users can gain access.
5. Report any lost or stolen records to your immediate supervisor.
6. Train new staff and periodically hold refresher training when security changes are made.
7. Encourage a clean desk policy to reduce the risk of exposing confidential information to others.
8. Use a file checkout procedure, to record the file's temporary location/borrower's name, and date borrowed, to easily locate files.
9. Phone the intended recipient to confirm receipt of a FAX containing sensitive information.
10. Know how long to retain personal information, and securely destroy it as per the appropriate retention period.
11. Complete a Confidentiality and Privacy Agreement with a third party when outsourcing services that involve the storage or access to personal information under the custody or control of the University. Contact the Freedom of Information and Privacy Coordinator for a copy of the Agreement, by calling 905-688-5550, ext. 5380.

Best Practices of technical security measures:

1. Ensure confidential electronic records are destroyed either by erasure, or some other means, in accordance with the appropriate retention period(s).
2. All CD's (and floppy disks or charge cards) scheduled for destruction, should be securely shredded using a cross-cut shredder.
3. For more technical security measures, please visit the ITS website: www.brocku.ca/its/security.

Best Practices of mobile workplace security measures:
This section is referring to personally identifiable information contained on a laptop, USB, PDA, cell phone or other mobile devices.

1. When removing laptops, and any other mobile workplace devices from the University, ensure that all confidential material remains secure and is password protected.
2. Remove as few records containing personal information as possible as required to do your job.
3. Consider alternatives to storing personal information on mobile devices. For example, use a secure website (e.g. Brock DB) or a Virtual Private Network (VPN).
4. Use a lockable briefcase or laptop case that does not bear any visible Brock logos. Place an "if found, return by calling [phone number"] card inside the briefcase, with no other identifying information.
5. Do not leave devices containing personal information or other confidential information in a vehicle. (If it absolutely cannot be avoided, lock them in the trunk before starting the trip.)
6. Do not use public computers or networks – or work on confidential material in public places.
7. If possible, remove personal information from the mobile device(s) as soon as practical, but understand that deleting data files from the screen of a mobile device won't necessarily delete the data completely.

The Information Privacy Commissioner has some additional solutions to secure mobile workplace devices at the following link: http://www.ipc.on.ca/images/Resources/up-mobilewkplace.pdf

Protect Personal Privacy:
Do not collect or use personal information that is not needed to do your job.

Unauthorized access occurs when employees or members of the public get access to personal information and records where they do not need to see or handle it in the course of their employment or other duties. Unauthorized disclosure of personal information violates an individual's privacy. Following the above security measures can help prevent a breach of privacy. When a privacy breach occurs, both the individual(s) affected by the breach and the University are potentially vulnerable to adverse consequences. If you feel there is a breach of personal information, please inform your immediate supervisor.

Related Policies and Procedures:

- Brock University's Access to Information and Protection of Privacy Policy
- Brock University's Access To Student Records And Disclosure Of Information Policy
- Brock University's Procedure: Handling Personal Information
- Brock University's Procedure: Posting Grades and Returning Student Exams and Assignments

For more information, please see Brock University's Freedom of Information and Protection of Privacy website at www.brocku.ca/accessandprivacy or contact the Freedom of Information and Privacy Coordinator at 905-688-5550, ext. 5380, or by emailing mhansen@brocku.ca.

Revised: January 17, 2008