



PROTECTING PERSONAL INFORMATION (PI)*

*Personal Information (PI) is recorded information about an identifiable individual, with the exception of the names and business contact information of employees, volunteers and service providers.



PROTECT

- **Use a strong password/passphrase.** Passwords must contain a minimum of 8 characters including upper and lower case letters, numbers, and symbols. Alternatively, use a passphrase with a minimum of 16 characters.
- **Guard your password carefully.** Do NOT share passwords or write them down. Consider using a password safe/manager.
- **Do not use UBC passwords for personal accounts.**

Refer to [Information Security Standard #02 Password and Passphrase Protection](#) and [Information Security Guideline: Password Safes](#) for more information.



SHARE

- Only share the minimum amount of PI necessary.
- Use secure storage methods such as network folders or Workspace 2.0.
- **DO NOT use email for high-risk PI.** If email has to be used, encrypt attachments with high-risk PI. High-Risk PI:

- | | |
|-----------------------------------|-------------------------------|
| ▪ Social Insurance Number | ▪ Personal Health Information |
| ▪ Official government ID card No. | ▪ Biometric data |
| ▪ Bank account information | ▪ Date of Birth |

Refer to [Information Security Standard #03 Transmission and Sharing of UBC Electronic Information](#) for more information.



DOWNLOAD

- **Download the minimum amount of PI that is required.** Reports and data extracts may contain PI that is no longer needed. Remove all unnecessary PI.
- **Store PI in secure locations such as secured network folders.** Do not store on local machines or on unencrypted devices.
- **Delete additional copies of PI that are not required.**

Refer to [Information Security Standard #03 Transmission and Sharing of UBC Electronic Information](#) for more information.



ARCHIVE

- Only retain PI for as long as it is required.
- Always securely remove PI before transferring, selling or discarding a device.

Refer to [Information Security Standard #08 Destruction of UBC Electronic Information](#) for more information.

Contact your it support representative for clarification or assistance with any of the above requirements. For more information on Information Security Standards, please visit www.cio.ubc.ca/securitystandards. Report information security breaches to security@ubc.ca or by phone to the it Service Centre at 604.822.2008.

www.privacymatters.ubc.ca

