PRIVACY MATTERS
@ UBC

ENCRYPTION 101

A quick guide to encryption: what it is and why it's important

WHAT IS ENCRYPTION?

Encryption is the method of protecting information on your computer or mobile device. When you lock or shutdown an encrypted computer, all of the data stored on that device is scrambled. This makes it unreadable if someone tries to access the computer. After information has been encrypted, only your password will make it readable again.

WHY IS ENCRYPTION IMPORTANT?

Encrypting your computer or mobile device is the most effective way to keep your personal information and UBC's data secure. At UBC, encryption is required for all mobile devices that access UBC systems.

WILL MY COMPUTER BE DIFFERENT AFTER IT IS ENCRYPTED?

Some versions of the encryption software may require you to input your login name and passphrase, which was setup when encryption was first added to your device.

If you notice any other major differences, please contact your IT administrator or submit a ticket at it.ubc.ca/sos

IF I ENCRYPT MY DEVICE, DOES THIS MEAN THAT UBC HAS ACCESS TO MY INFORMATION?

No, UBC does not have access to your information. However, we do utilize a management tool to track and report on the total number of devices that have been encrypted at UBC. This tool also allows UBC IT to assist you in case you forget your encryption password.

IF MY ENCRYPTED LAPTOP IS LOST OR STOLEN IS MY INFORMATION SAFE?

Your computer is encrypted if it is shutdown or in sleep/hibernate mode. Encryption works best if you follow the additional guidelines to protect your information, particularly if you regularly travel or work within public areas:

- Set your screen to lock after a maximum of 15 minutes of inactivity
- Lock your screen every time you walk away from your device
- Never share your password and never write it down
- Remember that IT staff will never ask you for your password

WHAT IS A KEY ESCROW?

You may hear the term "key escrow", which refers to a system that stores the passwords needed to unlock encrypted data. This is useful in the rare circumstance that an authorized party needs to gain access to the device. Typically, this is used when a password is forgotten and information cannot be retrieved.

WHAT IF I WANT ENCRYPTION BUT I DON'T WANT TO BE LISTED IN THE KEY ESCROW?

The most important thing is that your mobile device is encrypted. If you do not want to be part of the key escrow, we can still help encrypt your device. But, it is important to note that if you make this decision, we will not be able to help you in the event that you forget your password.

IF MY HARD DRIVE IS ENCRYPTED WILL OTHERS HAVE TO DECRYPT FILES I SEND TO THEM?

No, after you have logged in, the encryption program will automatically decrypt your files as you use them. Any files that you use, send or backup will not be encrypted.

To keep files secure when sending to other people, we recommend using Workspace, TeamShare, or other UBC-supported services.

WHAT IS PRIVACY MATTERS @ UBC?

The Privacy Matters initiative aims to increase the awareness of privacy and information security at UBC. Through online training and quarterly campaigns, we hope to arm staff and faculty at UBC with the knowledge they need to protect personal information.

DIDN'T ANSWER YOUR QUESTION?

Visit **it.ubc.ca/encryption-FAQ** for more information

STILL HAVING TROUBLE?

Submit a ticket at **it.ubc.ca/sos** or contact your IT administrator

www.privacymatters.ubc.ca

THE UNIVERSITY OF BRITISH COLUMBIA