Knowledgebase > Security > What is the policy that applies to laptop encryption?

What is the policy that applies to laptop encryption?

Burner EOAS - 2017-01-25 - Security

Overview

All faculty and staff are responsible for using UBC Electronic Information and Systems appropriately and maintaining their security. One of the most basic and essential elements of security is encryption. Encryption is an effective way to protect Personal Information (PI) collected by or for UBC, including but not limited to information about employees, students, and research subjects.

The Faculty of Science expects all UBC-owned laptop computers (as well as all personally-owned laptops used to store or access UBC information) to have their contents encrypted in order to safeguard any Personal Information which may be stored on these mobile devices now or in the future.

Proof of encryption includes the verbal or written declaration from the faculty member stating that the laptop is encrypted and it does not need to be visually verified.

A full-disk encryption exemption can be requested for machines that are not appropriate to encrypt, like those which are dual-boot or laptops used strictly for research.

Approval to not encrypt must be given by the IT Manager for the Department of Earth, Ocean and Atmospheric Sciences.

Additional Information

- Read Policy 104 (Acceptable Use and Security of UBC Electronic Information and Systems) to understand your obligations about information security.

- Under Policy 104, the Information Security Standards are mandatory for all Users of UBC Electronic Information Systems and failure to adhere to them may lead to disciplinary action. Please take the time to familiarize yourself with them.

- The Information and Privacy Commissioner has been clear that encryption is legally required for protecting Personal Information on a mobile device. For this reason, UBC’s Information Security Standard #05 requires all laptop computers used to store or access Personal Information to be encrypted.