THE UNIVERSITY OF BRITISH COLUMBIA

Faculty of Science, Office of the Dean
2178 - 2207 Main Mall
Vancouver, BC Canada V6T 1Z4

Phone 604 822 3336
Fax 604 822 5558

To: Faculty of Science (faculty, staff, graduate students, teaching postdocs)
Subject: Privacy and Information Security is everyone's responsibility

To ensure that UBC's confidential data and information systems are safe from a data breach, the university has Information Security Standards that govern the use and protection of university data and computing resources. As a reminder of your responsibilities regarding the privacy and security of data, please review the following summary of a few key UBC Security Standards. Additional details can be found by examining the full text of the standard.

NOTE: The Information Security Standards are currently being reviewed. If you have any comments about any of these standards, please take a moment to provide your feedback by sending email to privacy.matters@ubc.ca.

In addition, **Privacy & Information Security – Fundamentals** training (hxxps://privacymatters.ubc.ca/training) is now mandatory for all UBC faculty, staff and TA's. Join the 40% of Faculty of Science members who have already completed privacy and information security training, and better understand the information security measures needed to protect private and personal information, both at home and at work.

NOTE: If you have already completed the Faculty of Science information security quiz, the Fundamentals training is optional.

UBC IT Security Standard	**Key Points**
#01, Security Classification of UBC Electronic Information	Confidential Information includes Personal Information (PI) that is protected by law or industry regulation from unauthorized access, use or destruction. Examples of PI include student names, grades, or ids; personal email addresses; home addresses; health information; donor names; prospective employee names; and personal banking information. Sensitive Information is not protected by law but could cause harm to UBC if released and includes proprietary information and sensitive research data.
#04, Reporting Information Security Incidents	Users must report any suspicious incidents relating to the security of UBC Electronic Information and Systems including unauthorized access, use, alteration or destruction of data or UBC systems and theft of electronic information or the loss of a computer to their supervisor, the IT Support Staff who are assigned to their unit and to security@ubc.ca. University IT Support Staff (including both departmental IT and UBC IT staff) are responsible for handling security incidents in coordination with UBC Cybersecurity.
#05, Encryption Requirements	All faculty, staff and TA's 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. All mobile devices (e.g. laptops, phones and media such as USB sticks and portable drives) used to store Confidential Information, no matter whether they are owned by the University, by the User, or a third party, must be encrypted in order to safeguard any confidential information which may be stored on these mobile devices (now or in the future). Talk to your local IT staff for support.
#03, Transmission and Sharing of	All UBC Electronic Information must be transmitted securely to prevent it from being intercepted and copied by unauthorized parties. The *Freedom of*

UBC Electronic Information	*Information and Protection of Privacy Act* (FIPPA) requires that PI is stored only in Canada regardless of if it is encrypted. This means, you cannot use a Gmail account, Dropbox, Slack, Facebook, Google Docs or other computing services based outside of Canada for UBC business that involves PI. If, however, a student sends email from their Gmail account, containing personal information about themselves, it is acceptable for faculty and staff to respond to these emails, as long as they only do so using their UBC email accounts.
#07, Securing Computing and Mobile Storage Devices/Media	All devices used for University business, whether they are owned by the University or the user, must be protected from theft and/or unauthorized access. Lock or logout if leaving devices unattended, any Electronic Information must be backed up to a secure location, and if feasible enable features that allow devices to be located and data to be wiped remotely. Unpatched software is frequently exploited by malicious individuals to access information or resources. To mitigate this threat, vendor-provided patches for operating systems, applications, databases, etc. for devices containing UBC Confidential or Sensitive Information must be applied. If patches are not being applied to protect the system it is important to look at compensating controls, which will protect the system and reduce the risk of unauthorized access to information or resources. A possible compensating control may be to isolate the embedded system, so that it has no access to the Internet or other systems.
#02, Password and Passphrase Protection	Strong passwords and passphrases (sequences of words or other text) are important to access and protect information. Consequently, attackers attempting to access information use a variety of tools to guess or steal passwords /passphrases. To keep your password/passphrase safe and protect the information - create a strong password/passphrase; - guard it carefully (e.g. don't share it or write it down); and - avoid reusing it for other systems so that even if one is stolen, it does not allow access to your other accounts. Consider using a Password Manager, a computer application that provides a secure place to store and access passwords/passphrases. Password Managers are simple to use because they can be accessed with a single master password/passphrase.

Reference Information

- Policy 104 (Acceptable Use and Security of UBC Electronic Information and Systems) hxxps://universitycounsel.ubc.ca/files/2013/06/policy104.pdf
- The complete set of Information Security Standards - hxxps://cio.ubc.ca/information-security/policy-and-standards/
- Privacy Fact Sheets hxxps://universitycounsel.ubc.ca/access-and-privacy/privacy/
- Privacy & Information Security – Fundamentals training hxxps://privacymatters.ubc.ca/fundamentals-training
- **Please note:** *For added security, we have changed the above links to include an hxxps:// prefix. Simply copy and paste the URL into a web browser and replace hxxps:// with https://. Together we can keep our information secure.*