a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #03
Transmission and Sharing of UBC Electronic Information

Introduction

1. All UBC Electronic Information that is electronically or physically transmitted is at risk of being intercepted and copied by unauthorized parties. Users of UBC Systems have a responsibility to protect this information, according to its classification under the Security Classification of UBC Electronic Information standard.
2. This document provides standards on how to transmit or share UBC Electronic Information in a secure manner.
3. The Chief information Officer has issued this document under the authority of Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

Key Considerations when Transmitting and Sharing UBC Electronic Information

4. Only transmit the minimum amount of information required to complete a task (the principle of "least privilege"). Do not transmit any information that is not required (e.g. do not include Social Insurance Number and Date of Birth unless necessary). Where possible, do not transmit information that could be used to uniquely identify individuals.
5. When possible, do not copy, extract or download Medium, High or Very High Risk Information from Core Systems.
6. Medium, High or Very High Risk Information may be shared with other UBC employees on a 'need to know' basis, when their role at UBC requires them to have access to perform their duties.
7. Computing services based outside of Canada (such as Gmail) are not suitable for transmission or sharing of Personal Information because the British Columbia *Freedom of Information and Protection of Privacy Act* prohibits UBC from storing or allowing access to Personal Information outside of Canada. Also, these services are generally less secure than UBC-based systems.
8. Before Medium, High or Very High Risk Information is shared with Service Providers, Users must ensure the recipient is compliant with all requirements in the Outsourcing and Service Provider Access standard.

Acceptable Methods of Transmitting and Sharing UBC Electronic Information

9. The table below provides requirements for Users of UBC System on how to appropriately transmit or share UBC Electronic Information based upon the Security Classification of UBC Electronic Information standard.

Method of Transmission	**Information Security Classification**			
	Very High Risk	**High Risk**	**Medium Risk**	**Low Risk**
UBC Email Accounts (e.g. FASmail)	Acceptable only when placed in encrypted email attachments	Acceptable, although if you are sending significant amounts of this information it is best practice to put it in an encrypted attachment		Recommended
Personal Email Accounts (e.g. Gmail, Hotmail)	Not permitted			Not recommended
Approved UBC File Sharing, Collaboration & Messaging Tools[1] (e.g. Workspace, SharePoint, Network Shared Folders, Skype for Business, BlueJeans)	Recommended			

[1] Approved by the CIO or the Administrative Head of Unit as an acceptable method for transmitting and sharing all UBC Electronic Information.

Unapproved/Personal File Sharing, Collaboration & Messaging Tools (e.g. Dropbox, Google Drives / Docs / Hangouts, Skype, Slack, Facebook)	Not permitted		Not recommended
Mobile Storage Devices/ Media (e.g. USB drives, CDs/DVDs, tapes)	Encryption is required	Encryption is strongly recommended	Acceptable
Websites Hosted Within Canada	Permitted with authentication and HTTPS (encrypted) connections		HTTPS (encrypted) strongly recommended[2]
Websites Hosted Outside Canada	Not permitted	Permitted with authentication and HTTPS (encrypted) connections	HTTPS (encrypted) strongly recommended[3]
Other Internet Transmissions (e.g. SSH, FTPS, SFTP)	Permitted with authentication and encrypted connections (insecure internet transmissions e.g. Telnet, FTP are not permitted)		
Fax	Only permitted when sending/receiving fax machines are in secure locations (see Faxing guideline)		

10. Subject to section 9, if the User is using personal accounts or other information sharing tools to share UBC Electronic Information, they are responsible for ensuring that a copy of this information is stored on UBC Systems at all times.
11. For detailed information about encryption requirements, including how to encrypt documents and devices, refer to the Encryption Requirements standard.
12. For further guidance or assistance with protecting UBC Electronic Information, please contact University IT Support Staff.

Email Forwarding from UBC Email Accounts

13. Automatically forwarding or redirecting UBC email accounts to non-UBC accounts ("autoforwarding") is only acceptable for UBC faculty and staff members who have appointments at other institutions and have difficulty managing multiple work email accounts. Under these circumstances, it is acceptable to auto-forward the UBC email account to the email account at the other institution, provided that:
    a. the other institution is a public sector institution located in Canada;
    b. the other institution's email system is at least as secure as UBC's email system; and
    c. the staff or faculty member ensures that copies of emails of business value are returned to UBC Systems, so that they are managed in accordance with UBC's Records Management Policy.
14. Forwarding or redirecting UBC email accounts that are used to transmit UBC Electronic Information to a personal email account is not permitted.

[2] Major browser providers are flagging HTTP (non-encrypted) websites as insecure. All Canadian federal government websites have been mandated to be HTTPS by September 30, 2019.
[3] Major browser providers are flagging HTTP (non-encrypted) websites as insecure. All Canadian federal government websites have been mandated to be HTTPS by September 30, 2019.

Additional Requirements for Merchant Systems

15. Due to the sensitivity of Payment Card Industry (PCI) Information, it is subject to the following additional requirements:
    a. PCI Information must only be stored in approved Merchant Systems;
    b. PCI Information must never be transmitted via email or instant messaging systems. This activity is prohibited;
    c. PCI Information must never be transmitted unencrypted by any of the other above methods;
    d. media containing PCI Information must be sent by secured courier or other delivery method that can be accurately tracked; and
    e. management must approve the transfer of PCI Information from a secured area.

Case Study: Receiving Emails from Students

Students sometimes send emails to their instructors containing personal information about themselves. It is acceptable for instructors to receive and respond to these emails, as long as they only do so using their UBC email accounts. If the student wants to send or receive some extremely sensitive information, such as a medical report, the instructor should encourage the use of encryption on the document to ensure it is secure.

Receiving Information from Third Parties

16. Individuals who are not UBC employees, such as students, sometimes use insecure transmission methods, such as personal email accounts, to transmit their information to UBC. While it is acceptable to receive information in this way, we should encourage these individuals to take measures to minimize the risk of interception by unauthorized parties, such as encrypting files.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Encryption Requirements standard

Security Classification of UBC Electronic Information standard

Outsourcing and Service Provider Access standard

Faxing guideline