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, especially when it is Confidential or Sensitive.
2. This document provides standards on how to transmit or share 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 Confidential or Sensitive Information from Core Systems.
6. Confidential or Sensitive 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 Confidential or Sensitive 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 share UBC Electronic Information based upon the Security Classification of UBC Electronic Information standard.

<table>
<tr><th rowspan="2">Method of Transmission</th><th colspan="3">Information Security Classification</th></tr>
<tr><th>Confidential</th><th>Sensitive</th><th>Public</th></tr>
<tr><td>UBC Email Accounts
(e.g. FASmail)</td><td colspan="2">The following types of information must be placed in encrypted email attachments:
• Social Insurance Number (SIN)
• Any official government identity card No. (e.g. Passport ID, Drivers' License No., etc.)
• Bank Account Information (e.g. direct deposit details)
• Personal Health Information (PHI)
• Biometric data
• Date of Birth (DoB)

Other types of Confidential or Sensitive Information may be sent without encryption, although if you are sending significant amounts of this information it is best practice to put it in an encrypted attachment</td><td>Recommended</td></tr>
<tr><td>Personal Email Accounts
(e.g. Gmail, Hotmail)</td><td>Not permitted</td><td>Not recommended</td><td>Acceptable</td></tr>
<tr><td>UBC File Sharing Services
(e.g. Workspace, SharePoint)</td><td colspan="3">Recommended</td></tr>
</table>

Method of Transmission	Information Security Classification		
	Confidential	Sensitive	Public
Personal File Sharing Services (e.g. Dropbox, SkyDrive, Google Drive, Google Docs)	Not permitted	Not recommended	Acceptable
Mobile Storage Devices/ Media (e.g. USB drives, CDs/DVDs, tapes)	Encryption is required	Encryption is strongly recommended	Acceptable
Websites	Permitted with authentication and HTTPS (encrypted) connections		Acceptable
Other Internet Transmissions (e.g. SSH, FTP, Telnet)	Permitted with authentication and encrypted connections		Acceptable
Fax	Only permitted when sending/receiving fax machines are in secure locations (see Faxing Confidential or Sensitive Information guideline)		Acceptable

10. For instructions on how to encrypt documents and devices, refer to the Encryption Requirements standard.
11. For further guidance or assistance with protecting UBC Electronic Information, please contact University IT Support Staff.

Additional Requirements for Merchant Systems

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

Receiving Information from Third Parties

13. 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.

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.

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 Confidential or Sensitive Information guideline