a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U6
Working Remotely

1. Introduction

1.1 During the course of their employment, many UBC employees need to work remotely (including outside of Canada) with UBC Electronic Information, such as research, financial and Personal Information. UBC Electronic Information is generally more at risk of being compromised, corrupted or lost when accessed remotely than when accessed from internal systems, due to:

1.1.1 the vulnerability of laptops or other Mobile Devices to theft or loss;

1.1.2 the risk of unauthorized persons (e.g. family members, commercial service providers) viewing information;

1.1.3 lower standards of physical and electronic security than on UBC premises; and

1.1.4 retention of information on mobile or remote systems without some Users being aware (e.g. cached webpages and email attachments).

1.2 This standard defines requirements for UBC employees working remotely with UBC Electronic Information on all Devices. Working remotely includes but is not limited to:

1.2.1 working from home;

1.2.2 travelling;

1.2.3 working from a coffee shop or conference;

1.2.4 working from a location using the Eduroam wireless network; and

1.2.5 working within a health authority facility where the network is not under the control of UBC.

1.3 This standard must be read in conjunction with the Encryption Requirements and Securing Computing and Data Storage Devices/Media standards. These standards apply to all Devices used for University Business—no matter whether they are owned by the University, by the User, or by a third party.

1.4 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Secure Access Methods

2.1 Wherever possible, UBC Electronic Information should be remotely accessed through a UBC System, rather than downloaded onto a Device, as this will significantly reduce the risk of loss or theft. The following are the preferred secure methods for Remote Access:

2.1.1 The recommended methods to access information are to use a Virtual Private Network (VPN) or SSH (secure shell) interface.

2.1.2 When connecting via VPN, use remote desktop (RDP) where possible, as this presents the lowest risk for Remote Access by keeping data at the university. Important points to note:

2.1.2.1 RDP must not be used without a VPN connection;

2.1.2.2 don't map remote drives to your local Workstation; and

2.1.2.3 for information on using RDP, contact your University IT Support Staff.

2.1.3 Alternatively, a Virtual Desktop Interface (VDI) can be used, only accessing the information inside the VDI session. VDI is a service available through UBC IT, which creates a "virtual" computer that can be accessed from home computers, laptops, desktops, tablets and even smartphones.

2.1.4 Microsoft Remote Desktop Services (RDS, previously Terminal Services) is also an acceptable secure access method.

2.1.5 For access methods other than the above, confirm with University IT Support Staff that the method and configuration are secure.

2.2 Remote Access must be in compliance with the Network Protocol Requirements section of the Internet-facing Systems and Services standard.

2.3 Do not use a network connection if a 'certificate error' window or other alert appears when trying to connect to a UBC System via a secure access method (as outlined in section 2.1), or if the User is otherwise uncertain about the safety of the network.

3. Supplemental Guidance for Personally-owned Equipment

3.1 If a personally-owned desktop or laptop computer is accessing UBC Electronic Information and Systems using VPN with RDP, VDI or RDS then device-level encryption is not required, but is recommended.

3.2 Ensure personally-owned routers and home networks (including IoT Devices) are properly secured (see Securing your Home Router guideline).

4. Physical Security

4.1 Reasonable measures must be taken to prevent or reduce the possibility of loss or theft of Devices (including Multi-Factor Authentication Devices) that are used to access or protect UBC Electronic Information such as:

4.1.1 being aware of others looking over one's shoulder at the Device when working in public locations such as coffee shops, aircraft and other public transport;

4.1.2 not leaving Devices unattended in a public place, especially well-travelled areas such as airport lounges and coffee shops; and

4.1.3 keeping Devices secured when working from home, e.g. storing them in a physically secured area and ensuring UBC Electronic Information cannot be accessed by family members.

4.2 Reasonable measures must be taken to prevent or reduce the possibility of loss or theft of Multi-Factor Authentication Devices.

5. Third Party Devices and Networks

5.1 Do not access Medium, High or Very High Risk Information using third party Devices, such as kiosks in public libraries, hotels, airports, and cyber cafes, unless the Device is owned by another higher education institution or health authority in partnership with UBC (e.g. a collaborator).

5.2 When accessing public Wi-Fi networks, such as those in airports and coffee shops, do not use the connection if a 'certificate error' window or other alert appears when trying to connect to a UBC System via a secure access method (as outlined in section 2), or if the User is otherwise uncertain about the safety of the network.

6. Related Documents and Resources

Encryption Requirements standard

Securing Computing and Mobile Storage Devices/Media standard

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

UBC IT myVPN Service

Remote Desktop Protocol (RDP)

UBC IT Virtual Desktop Interface (VDI)

Internet-facing Systems and Services standard

Securing your Home Router guideline

UBC IT Guide to Working off Campus