a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #06
Working Remotely

Introduction

1. During the course of their employment, many UBC employees need to Work Remotely 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:
    a. the vulnerability of Laptops or other Mobile Devices to theft or loss;
    b. the risk of unauthorized persons (e.g. family members, commercial service providers) viewing information;
    c. lower standards of physical and electronic security than on UBC premises; and
    d. retention of information on mobile or remote systems without some Users being aware (e.g. cached webpages and email attachments).
2. This document defines requirements for working remotely with UBC Electronic Information on UBC and personally-owned Devices. This standard must be read in conjunction with the Securing Computing and Data Storage Devices/Media standard.
3. The Chief Information Officer has issued this document 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.

Secure Access Methods

4. Wherever possible, UBC Electronic Information should be accessed remotely on campus-based source systems rather than downloaded onto a Device, as this will significantly reduce the risk of loss or theft. The University provides the following secure processes for remote access:
    a. The preferred method is to use a Virtual Desktop Interface (VDI) and only access the information inside the VDI session. VDI is a service available through UBC Information Technology, which creates a "virtual" computer that can be accessed from home computers, Laptops, desktops, tablets and even smartphones.
    b. Alternatively, a Virtual Private Network (VPN) or SSH (secure shell) interface can be used to access information.

For access methods other than the above two, confirm with University IT Support Staff that the method is secure.

Physical Security

5. Reasonable measures must be taken to prevent or reduce the possibility of loss or theft of Devices that are used to access Medium, High or Very High Risk Information including:
    a. 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;
    b. not leaving Mobile Devices unattended in a public place, especially well-travelled areas such as airport lounges, and coffee shops; and
    c. 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.

Third Party Devices and Networks

6. 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.

7. Use caution when accessing public Wi-Fi networks, such as those in airports, coffee shops. If a ‘certificate error’ occurs when trying to connect, or if the User is otherwise uncertain about the safety of the network, then do not use that connection.

Related Documents

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

Securing Computing and Mobile Storage Devices/Media standard