A L G O N Q U I N C O L L E G E

INFORMATION SECURITY GUIDE

Employee Teleworking

Information Security Unit

Information Technology Services (ITS)

July 2013

ALGONQUIN COLLEGE

CONTENTS

1. Introduction

Many employees use College owned or personally owned computing devices while working at home, other locations or while travelling. This is often referred to as *Teleworking* or *Telecommuting*.

The College provides various technologies to support Teleworking situations. This includes laptops, tablets and mobile phones if supplied by your department. Some employees use their own home computers to access College IT resources. The College also operates and maintains the "Secure Portal for Staff" (https://secure2.algonquincollege.com/+CSCOE+/portal.html) that provides secure connections to e-mail, central storage drives, commonly used applications and personal desktop computers.

Teleworking technologies and environments often need special care and protection because they are often exposed to additional vulnerabilities, threats and risks. Therefore, it is important that staff are aware of the additional safeguards required to protect College assets and sensitive information when working remote.

This guide provides an overview of the Teleworking risks as well as the safeguards that should be implemented. Algonquin College's Information Sensitivity and Security Directive, IT-05, provides additional requirements and direction.

Questions or suggestions regarding these guidelines should be forwarded to:

Manager, Information Security
Information Technology Services (ITS)
infosec@algonquincollege.com
X6491

2. Teleworking Risks

Teleworking brings increased risks to College technology and most importantly, the sensitive information stored within. These include:

- **Loss or theft of an asset** such as a laptop, tablet, or mobile phone. There is a 30% probability that a user will lose a portable device within any given year. The average cost of a stolen laptop is $37,000 which includes loss of the asset, staff time spent investigating the incident, loss of information and breach/lawsuit related costs;
- **Unauthorized use of an asset**, due to automatic logoff not being implemented, allowing unauthorized individuals to use the asset;
- **Damage to an asset**, due to break and enter crimes, dropping, unauthorized mishandling, and spilling of liquids;
- **Unauthorized disclosure of sensitive information**, such as when unauthorized individuals oversee sensitive information on a computer/mobile phone screen at home, in a restaurant or café, in an airport, or while travelling on public transportation. This can also happen when home computers – used to access College systems – are connected to insecure wireless (Wi-Fi) home routers, or improperly disposed of;
- **Loss or theft of the sensitive information,** when an unprotected (i.e. no encryption) computer or USB drive is lost or stolen, leading to legislation (e.g. PIPEDA, FIPPA, PHIPA) breaches as well as breach notification and potential lawsuits;
- **Compromise of login credentials**, leading to system hacking, corporate network and application hacking, and identity theft. This can occur when staff use unprotected private or public networks, particularly Wi-Fi networks or use unprotected Bluetooth communications in public areas; and
- **Computer or mobile phone malware**, including viruses, worms, and Trojan horses, due to the devices being inappropriately protected.

3. Safeguards for College Owned Technology

The safest and easiest way to protect College sensitive data is to use ITS approved technology including laptops, tablets, desktops and mobile phones. In is this way, you can be assured that devices are using some of the latest ITS-approved security technologies including full disk and USB drive encryption, anti-malware protection, and have the latest security settings enabled for login, passwords, password enabled screen savers, time-enabled auto logoff and secure network login.

The following checklist will help you ensure that College security policies, best practices and a standard of due care are being followed:

1. Use College owned computers wherever possible, and enable the standard, approved set of security safeguards for encryption, anti-malware, password-enabled screen savers and auto logoff.
2. Conduct *only* College business on College owned computers.
3. Secure your home wireless (Wi-Fi) router using strong passphrases, WPA-2 encryption (do not use insecure WEP encryption) and MAC addressing if possible.
4. Conduct your computing in a private area of your home, away from prying eyes and inadvertent, unauthorized access;
5. Be conscious of individuals that might be “shoulder surfing”, such as family members or individuals in public places. While at home, use a private place to conduct your computing.
6. Do not use portable computing devices in high risk public areas such as restaurants, coffee houses and airports.
7. If you must lock a portable computing device in a car, place it in a protected, non-visible location, such as a trunk, for the minimal amount of time possible.
8. If you must secure a portable computing device while at a hotel, lock it up in the room safe or front desk safe. Never leave it unattended in a hotel room.
9. Use a ‘Kensington’ laptop lock to physically secure portable computers from theft, whenever unattended. These are available from the Technology Store. Tablet computers may not have a locking capability – if so, always secure the device when not attended.
10. Limit your use of USB drives generally due to the high risk to information that they bring. Instead, work off of your computer or a Network drive, wherever possible.
11. Never use unapproved, insecure, regular USB drives to store College information.
12. Never use unapproved, portable hard drives to store College information.
13. Never store Health related personally identifiable information (PII) on USB drives or on portable drives, without the explicit written approval of the Manager, Information Security, ITS.
14. Use approved Windows Bitlocker enabled USB drives, as setup by ITS, whenever possible. If unavailable, use ITS-approved, secure USB drives to store College

information. These are available from the Information Security Unit, ITS. Make sure to write your USB password down and store it is a secure place in case you forget it. Forgetting your password will lead to permanent loss of information.

15. Use strong passwords: Minimum 8 characters, use upper and lower case letters and include at least one number, don't include personal information, change every 120 days, and don't reuse the same password for 2 years.
16. Shred printouts of all College information in cross-cut shredders, or bring back to the office and shred, or deposit in a secure shredding bin.
17. Turn off Wi-Fi and Bluetooth networking services while not in use or while travelling on public transportation.
18. Immediately report suspicious, suspected and actual security incidents and breaches to the Manager, Information Security, ITS.

4. Safeguards for Personally Owned Technology

If you do not have access to College owned (and loaned) technology, and you must use your own, be careful of the increased risks to College information. Remember that it is highly likely College information will be stored on your own device(s). Even if you cannot "see" the information through usual means, it will exist on hard drives and can be accessed through operating system applications or other software.

The following checklist will help you ensure that College security policies, best practices and a standard of due care are being followed while using your own technology:

1. Limit the computer to only your use (i.e. do not allow family members or others to use the same device).
2. Implement full disk encryption, in case your computer is stolen or lost.
3. Implement anti-malware software that provides real-time protection as well as (minimum) full disk weekly scans.
4. Use password-enabled screensavers that activate within 30 minutes of user inactivity.
5. Ensure that your operating system and applications are receiving regular patch updates.
6. Turn off Wi-Fi and Bluetooth communications services when not being used.
7. Secure your home wireless (Wi-Fi) router using strong passphrases, WPA-2 encryption (do not use insecure WEP encryption) and MAC addressing if possible.
8. Conduct your computing in a private area of your home, away from prying eyes and inadvertent, unauthorized access.
9. Be conscious of individuals that might be "shoulder surfing", such as family members or individuals in public places.
10. Separate College and Personal work storage areas.
11. Do not use portable computing devices in high risk public areas such as restaurants, coffee houses and airports.
12. If you must lock a portable computing device in a car, place it in a protected, non-visible location, such as a trunk, for the minimal amount of time possible.
13. If you must secure a portable computing device while at a hotel, lock it up in the room safe or front desk safe. Never leave it unattended in a hotel room.
14. Use a 'Kensington' laptop lock to physically secure portable computers from theft, whenever unattended. These are available from the Technology Store. Tablet computers may not have a locking capability – if so, always secure the device when not attended;
15. Limit your use of USB drives generally due to the high risk to information that they bring. Instead, work off of your computer or a Network drive, wherever possible.
16. Never use unapproved, insecure, regular USB drives to store College information.
17. Never use unapproved, portable hard drives to store College information.

18. Never store Health related personally identifiable information (PII) on USB drives or on portable drives, without the explicit written approval of the Manager, Information Security, ITS.
19. Use ITS-approved, secure USB drives to store College information. These are available from the Information Security Unit, ITS. Make sure to write your USB password down and store it is a secure place in case you forget it. Forgetting your password will lead to permanent loss of information.
20. Use strong passwords: Minimum 8 characters, use upper and lower case letters and include at least one number, don't include personal information, change every 120 days, and don't reuse the same password for 2 years.
21. Shred printouts of all College information in cross-cut shredders, or bring back to the office and shred, or deposit in a secure shredding bin.
22. Do not leave your computer at a service facility where sensitive College data can be accessed and/or copied while not being supervised. Alternatively, bring the computer to work where an ITS client services technician can assist.
23. Turn off Wi-Fi and Bluetooth networking services when not in use or while travelling on public transportation.
24. Immediately report suspicious, suspected and actual security incidents and breaches to the Manager, Information Security, ITS.

Acronyms and Definitions

ITS – Information Technology Services
PII – Personally Identifiable Information
PHI – Personal Health Information
PHIPA – Personal Health Information Protection Act (Ontario)
FIPPA – Freedom of Information and Protection of Privacy Act (Ontario)
PIPEDA – Personal Information Protection and Electronic Documents Act (Canada)
USB – Universal Serial Bus
Wi-Fi – Wireless
WPA – Wireless Protected Access
WEP – Wired Equivalency Protocol

Information Security is everybody's business