Policy Title: Information Technology Services – Electronic Device Security Policy

Policy Number:

Established: January 2009

Approved by:

Last Approval Date: January 2019

Revision Date: July 2019

Position Responsible for Maintaining and Administering the Policy: Executive Director, Information Technology Services

Contact: Ryan Kenney, Executive Director, IT Services, (519) 253-3000 ext. 2740

Table of Contents

Policy Statement

To establish safeguards for password protected access to confidential information on portable, fixed media and other computing hardware, including the connection of devices to the campus network.

Purpose

Electronic devices with access to confidential information that are not password protected have the potential to significantly impact the University with respect to its legal obligation to provide a secure electronic environment should said information become accessible publicly. In the event that devices are lost, stolen, or otherwise compromised, access by a third party is more difficult if the device is "power-on" or "application specific" password protected, and encrypted confidential information provides reasonable protection from access by any third party.

Electronic devices with access to confidential information may place the University at risk for maintaining its obligations inclusive of, but not limited to, the Freedom of Information and Protection of Privacy Act (FIPPA), where protection to prevent unauthorized disclosure must be upheld. It is therefore reasonable that all electronic confidential information that may be transmitted over public networks, or that is stored on machines, shall be encrypted, and accessed only using electronic devices that are "power-on" or "application specific" password protected in accordance with this Policy.

Scope

Electronic devices are inclusive of, but not limited to laptop, desktop and tablet computers; smartphones and other mobile devices, USB memory sticks and other drive storage media, used for search, storage or retrieval of confidential information.

All faculty, staff or students with access to encrypted confidential information electronically are responsible for ensuring that devices are "power-on" password protected (i.e. when the device launches the operating system) or "application specific" password protected (i.e. when an end-user application is used) for access to the information.

Responsibilities:

1. IT Services has the responsibility to:
    - Provide guidance to clients and associated services to support this Policy
2. Client area receiving the specified service has the responsibility to:
    - Comply with requirements as described in Appendix A
    - Acknowledge that any fees for service (as may be applicable) will be incurred
    - Verify (as required) that any related services have been received
    - Provide funding to cover the cost of the service, if applicable, as agreed
3. IT Steering Committee has the responsibility to:
    - Regularly review this Policy
    - Provide feedback and guidance on this Policy

Exceptions to Policy

The Executive Director, IT Services may determine that certain situations or circumstances require exceptions to this Policy in order to best serve the interests of the University. Such decisions should be communicated in writing to the Executive Director, IT Services and should include the exact nature of the exception and, if appropriate, the time period during which the exception should be granted.

Cross-References

None

Definitions

Confidential Information:
In accordance with the University of Windsor, Records Management Initiative, including life-cycle, disclosure and harm as defined therein, "confidential" includes information that for any one of a number of reasons should only be disclosed to specific people or groups and is not for general circulation. The information contained therein is typically sensitive in nature and may be:

- Recorded information about an identifiable individual ("Personal" Information); or
- Recorded information relating to the business of the university or a third party, including but not limited to, trade secrets and commercial, financial, scientific, technical or labour relations information

Information and / or records may be considered confidential if:

- The information was supplied either explicitly or implicitly in confidence; and
- Its release could result in some harm to either the University or a third party

Procedures

General
The University affirms the importance of ensuring confidential information remains reasonably secure from electronic access publicly, and that enforcement of the use of passwords for access to devices and or applications provides assurances that information will be protected more so than if no passwords were used. The University is committed to the protection of privacy and confidential information of individuals who learn, visit, research, or otherwise work at the University by the enforcement of access, encryption and other security requirements to information accessible by portable computer and other devices, including:

i) As a general rule, confidential information contained in University records accessible electronically must be secure from public access at all times, in any machine-readable form, including but not limited to whether information is in transit on a network, or stored on a device;
ii) The use of mobile electronic devices in use by those with access to confidential information have a higher risk of potential loss or misuse and therefore appropriate security measures be enforced;
iii) The collection, retention, use, disclosure and destruction of confidential information contained in University records accessible electronically shall be regulated in a manner that will protect the privacy of individuals who are the subject of that information.

Password Protection and Access

Protection
Password security shall be the sole responsibility of the user only if the user is solely responsible for the administration of the password, including establishment, maintenance, storage, recovery and destruction of the password. Notwithstanding the above, the University shall be responsible only with

respect to its *Enforcement of the Access Rights* (see below), Password Acceptable Use and Recovery, including its *Issue and Use of Passwords*, and its *Retention, Disposal and Recovery of Passwords* (see below, respectively), or as otherwise defined herein.

Password security protection requires that all persons with access to individual or application specific passwords, shall be authorized only by the University for access to confidential information in accordance with this Policy. All passwords shall be retained by individuals and machine resources, as confidential information in compliance with this Policy.

Access Rights

i) The right of use and access affirmed by this Policy should normally be implemented by providing and enforcing a password mechanism for the provision and recovery of passwords for all device users where information is accessible or stored.
ii) Where the request for password access pertains to either a device or to information, a personal verification mechanism will be made available that ensures reasonably, that individuals provided with access rights, are the password holders.

Enforcement of the Access Rights

The University grants access to the use of passwords and encryption protocols, as well as the policies and mechanisms of enforcement, that it controls, respectively. The University may, at its sole discretion, refuse access to either passwords or information that it controls, respectively, in enforcement of this Policy.

Password Acceptable Use and Recovery

Issue and Use of Passwords

The University shall issue passwords and manage a password management system that provides security for those using passwords, such that only those with authorized access to issue and manage passwords shall be granted access to the password management system.
The University shall not issue and manage passwords in its custody or under its control except:

i) for the purpose for which it was obtained or compiled for a consistent purpose;
ii) where the person to whom the information relates has identified that information in particular and has consented to its use; or
iii) to administer confidential information in its records for the purpose of its own activities.

Retention, Disposal and Recovery of Passwords

The University shall take reasonable precautions to protect the security of passwords and shall retain passwords only when necessary for recovery, and shall make reasonable arrangements for the archival, disposal or destruction of passwords when they are no longer needed by a person or machine resource.

Relationship with other University policies, guidelines and procedures

Policy and Procedure Review

The University shall develop new or revised policies, guidelines and procedures to take into account the principles and responsibilities set forth herein as needed by the University.

Existing Policies and Practices

This Policy and its guidelines and procedures are not intended to replace or restrict existing procedures and practices within the University relating to access to information that is not

confidential information, and where such procedures and practices give access equal to or greater protection than that provided in this Policy.

i) Where a separate written University policy has been adopted, its provisions, in the event of conflict, will take precedence over this Policy, provided that such conflicting provisions are also consistent with the Freedom of Information and Protection of Privacy Act.

Client Responsibilities
The Client Responsibilities section is an integral component of this policy and should be reviewed. Please refer to Appendix A.

Enforcement
The University strictly prohibits the use of any end-user device without "power-on" or "application specific" password protection used to access confidential information. The University also prohibits the access of confidential information over an unsecure public network used by those without authorization to view the information. Where password usage and or data encryption are capable on devices and are enforceable through the use of technology or by other means, it shall be enforced by the University.

Review Process for Policy

This Policy will be reviewed every five (5) years. There may be certain circumstances that may cause for the review of the Policy prior to that date: changes in legislation that affect the Policy; a specific incident triggers a review of the Policy; there is a request made by Senior Management or the Board of Governors to review the Policy,

Process for Communicating Policy

The policy will be posted on the University of Windsor's IT Services website, within two weeks of the approval of the Policy. Separate notifications may also be sent via e-mail or other means to Departments directly affected by the Policy, or in some cases, the broader campus community if deemed applicable.

Contact Information
Inquiries regarding the policy should be directed to Executive Director, IT Services or appropriate individual in the Department where the policy was developed, as per the contact information at the introduction of the Policy.

Appendices

Appendix A: Electronic Device Security Policy: Client Responsibilities

Appendix B: Electronic Device Security Policy: Summary of Considerations

Appendix C: Electronic Device Security Policy: Glossary

Appendix A: Electronic Device Security Policy: Client Responsibilities

a) No confidential information is to be accessed by, transmitted or transferred to an electronic device that is not "power-on" or "application specific" password protected.

b) All electronic devices used within the University computing environment must be properly configured and user authenticated for ensuring secure access before being used to store, transmit, receive, or in any way otherwise interact with confidential information.

c) No electronic device is considered to be a secure computing device unless University security software applicable to that device has been installed, or where an alternative security software is proposed by an individual and shall be evaluated and approved subsequently by the University for use in accordance with this Policy.

d) All electronic devices and media must use at least minimum password configurations and minimum encryption protocols (network and storage) compliant with existing North American commercial banking standards, including case-sensitivity, alphanumeric configuration and the most common encryption level standard.

e) If electronic devices are used to store, transmit, receive, or, in any way, interact with confidential information, then data must be protected in accordance with the following requirements:

    i) if these data are to be stored locally on electronic devices, they must be protected by an acceptable password and stored in an encrypted format;
    ii) for all electronic devices accessing these data, all main system functions and data must be protected by an acceptable password in accordance with University protocols for the establishment and use of passwords;
    iii) if these data are transferred via terrestrial or wireless connections over a public network, they must be transmitted in an encrypted format at least in minimum accordance with the most common North American commercial banking or other identified standards.

f) Access to confidential information from portable computing devices using internal or public terrestrial or wireless networks, requires the use of a secure network, or installation of a secure method of transmission to be enabled on the electronic device.

g) All electronic devices used in open, common, or otherwise public insecure areas must implement the following to the greatest extent possible:
    i) a theft deterrent device when the device is left unattended.
    ii) an inactivity time-out or automatic logoff mechanism.
    iii) reasonable safeguards to prevent unauthorized viewing of confidential information.

h) Any electronic device not in compliance with this Policy should not be used to store, transmit, or process confidential information, and the University discourages and prohibits their use as reasonable for access to confidential information.

i) It is the responsibility of the users to ensure that any electronic device in their possession, whether provided by the University or privately owned, is in compliance with University policies before using it to store, transmit, or process any confidential information covered under this Policy.

j) Unless the University accepts the responsibility beforehand, the assigned user of any electronic device used to store, transmit, or process any confidential information is responsible for any transaction initiated by, or transferred using the device, unless the device has been reported as lost, stolen or compromised as soon as reasonably possible to the University.

k) Assigned users shall prevent use of any electronic device access to confidential information, for which they have been assigned custody, by any other party not authorized for access to said information.

l) All other appropriate security policies applicable to desktop computers will apply to portable computing devices.

m) In the event an electronic device with access to confidential information is lost or stolen, it is the sole responsibility of the user to notify the University as soon as possible.

n) Temporary-use, replacement or loaned devices with access to confidential information shall comply with this Policy and be returned for re-use without confidential information stored or recoverable from them (including passwords), or otherwise be disposed of (see “o” below).

o) Electronic devices are to be disposed of without any confidential information stored or recoverable from them, including passwords, or otherwise shall be rendered unusable through physical destruction of the device storage media to ensure any future access and use of confidential information by any third party is not reasonably possible.

Appendix B: Electronic Device Security Policy: Summary of Considerations

The Electronic Device Security Policy protects confidential information that exists in an electronic format. The following summary considerations are important for ensuring your compliance with the Policy. Note: where there are additional interpretations required, or for more detailed information, please refer to the Electronic Device Security Policy directly, or contact the Office of the Executive Director, IT Services.

- Electronic devices covered in the Policy include computers, mobile devices, PDA's, memory sticks, external hard-drives, cell phones (if they access confidential information) and other like devices

- Password protection must be enabled on devices when they first turn on, and/or the password protection available through the application that will access confidential information must be invoked

- Password complexity and network security should be at least equivalent to North American banking standards (e.g. 4 digit alphanumeric/numeric PIN, and for use of a public network, at least 128-bit encryption must be used). Where other standards have been prescribed, these shall also be deemed as applicable.

- Confidential information stored on a device must be encrypted (so that if access to the data location is obtained, confidential information is not readily viewable)

- Security software that can be used to secure confidential information will be recommended by IT Services. If you choose to use your own, you will need to confirm with IT Services that it will provide sufficient protection in accordance with the Policy.

- Public wireless or wired networks may be insecure or have users that are not authorized to view confidential information using them. When viewing or uploading/downloading confidential information, you must be on a secure network, or when otherwise communicating from off campus, use a secure network connection (e.g. https://). If available, a Virtual Private Network (VPN) connection to access or transmit confidential information should be used.

- Devices used in open or common areas should have theft deterrents installed, inactivity time-outs set (e.g. auto-logoff), and extra viewing safeguards when accessing confidential information (e.g. hide your keystrokes when logging in with your password)

- Users are responsible to ensure that their device is compliant with the Policy for access or storage, prior to accessing or downloading confidential information

- IT Services should be notified as soon as possible about lost or stolen devices that may provide access to confidential information by any other person

- Borrowed or temporary use devices must not have any trace of confidential information when returned or left for use by another person.

- Electronic devices are to be disposed of so that any trace of confidential information

would not be reasonably recoverable or accessible. Depending on the device, this may require physical destruction of the storage media.

Specific things you should NOT do when accessing or storing confidential information.

- Do **NOT** use a device to access confidential information without any password or security protection (e.g. firewall, virus protection, etc. should be turned on)

- Do **NOT** transmit confidential information over public wireless networks, or over the UWindsor Wireless networks, without using a secure network link (e.g. https://) and or VPN software

- Do **NOT** store confidential information on a hard-drive, USB key, mobile or other device with storage media without encrypting the confidential information in a manner acceptable to IT Services

- Do **NOT** leave computers or other portable electronic devices unattended or remain "logged in" to confidential information when you are not using the device

- Do **NOT** share your password with any other person, or write it down as a reminder and store it with, or next to, the electronic device

- Do **NOT** "login" to your device for someone else to "masquerade" as you

- Do **NOT** forget to notify the University Service Desk if one of your devices is lost or stolen (e.g. phone x4440)

- Do **NOT** use formats of passwords, or manage passwords in such a way that the practices are not compliant with existing North American banking standards (e.g. 4-digit PIN and at least 128-bit encryption) or other prescribed standards

Appendix C: Electronic Device Security Policy: Glossary

128-bit encryption: 128 bits refers to the length of the software key used to encrypt information and the longer the key, the stronger the encryption. '128-bit encryption' is simplified wording for a current standard Internet security level.

Alphanumeric: contains both letters and numbers, for instance ‘uz6N94wQ'.

Application specific: a feature or mechanism controlled by the application. In this context, passwords or security systems are required by the application, not by the device or the operating system.

Authorized access: access to the device, software or data on the computer is granted only to a specific user who must have a password.

Automatic logoff: a feature that automatically “logs-out” the current user after a certain criterion is met (e.g.) after 30 minutes of inactivity or at a certain time of day.

Campus network: the UWindsor campus computer network, including the fiber networks between buildings, and the wired and wireless networks that connect computers.

Case-sensitive: often used in password systems where upper- and lower-case letters are treated differently. For instance, “Apple” is not the same as “apple”.

Computing hardware: a device or machine that assists in retrieval, storage and display of information. Examples are mobile phones, laptops, desktop computers, servers, and handheld gaming consoles.

Confidential information: information that should be accessed only by the owner or the person it was given to, and not made available to anyone else. See also the “University of Windsor Records Management Initiative”.

Configured: a collection of settings and options that control the behavior of a device or software component. For instance, you would configure your VCR to record channel 3 at 8PM.

Data: any information such as records, emails, spreadsheets, pictures, etc., that is collected and stored on computer systems.

Desktop computer: a powerful computing device consisting of a keyboard, mouse, monitor and Central Processing Unit (CPU) that is often installed permanently, for instance in an office, unlike a laptop.

Device storage media: internal capability to store data, either temporarily or permanently. In the case of computers, typically called memory, disk or storage space.

Drive storage media involves removable storage devices such as floppy disks, CD-ROMs, DVDs, USB memory sticks

Enabled: a setting or option that has been “turned on”.

Encrypted: data that no longer resembles the original, and therefore it is not in a readable form except by those authorized to view it

Encryption: the act of modifying data so that it is no longer readable in its original electronic form, typically done before sending or for storing information

Encryption level: a measure of the strength of the encryption. The higher the level, the more difficult it is to return the information to its original structure.

Encryption protocols: the collection of methods, steps and tools used to alter information so others cannot read or access it. There are several protocols that can be selected to achieve the goal of securely encrypting data.

End-user device: a piece of equipment or machinery that is used by a human in order to access, read and use information.

Enforcement: the act of ensuring that the requirements of the policy are followed. This may include technology to ensure passwords and encryption are used and to audit devices.

External hard-drive: an example of high-capacity drive storage media. Typically, can contain many gigabytes (GB) of data.

Firewall: software or hardware that monitors, permits and denies connections between devices or applications.

FIPPA: The Government of Ontario's Freedom of Information and Protection of Privacy Act is legislation that provides a right of access to information under the control of institutions, and also protects the privacy of individuals with respect to personal information.

Fixed media: synonymous with device storage media. Internal storage to a device that cannot be removed without disassembling the device.

Formats: the structure or layout of an item. In the context of passwords, a format would be to 'use alphanumeric words with varied case', such as ‘8B3hbA5z'.

Hard-drive: a high-capacity device storage media typically located inside of devices such as desktops, laptops and video cameras.

Inactivity time-out: after a certain amount of time has passed without the user performing any type of action on a device, the user will be required to re-enter their password before continuing use.

Insecure: a condition where it cannot be guaranteed that information cannot be read or intercepted by others. For instance, sending a letter that is not in a sealed envelope is an insecure way of delivery. You can have insecure locations (coffee shop) and insecure networks (the Internet) and insecure storage (unencrypted), among others.

Laptop: a computer that can be folded up and easily carried from one location to another. As powerful and high capacity as a desktop computer. Often used to access information insecurely over wireless networks.

Machine resource: a capability of a computing device, such as the operating system, its storage media or a particular software application.

Memory stick: synonymous with memory key or USB key, it is a medium-capacity form of drive storage media that can be easily moved from one machine to another.

North American commercial banking standards: the collection of protocols and requirements used by the banking system to provide end-user access to their banking information. Typically includes at least the minimum encryption level and password format.

Password: a word or phrase used as part of a process to identify a user. A password is information that only the individual should know. Banks call it a PIN when using your bank or credit card.

Password complexity: a measure of how difficult it is to guess or reproduce a password. A short password ('bus') or a sequence ('1234') has low complexity compared to a phrase ('Humpty had a little lamb') or a word that is alphanumeric with varied case sensitivity ('m5xTN3'), which have higher complexity.

Password management system: a software system for creating, changing, storing, distributing and destroying passwords.

Password mechanism: a process implemented and managed by the University in order to ensure that passwords are used where required.

Password protected access: the device, software or data cannot be used or displayed without first providing a password.

Personal verification: the process of verifying that you are the individual you claim to be. Often involves checking identification or confirming personal information (such as mother's maiden name).

Physical destruction: the process of modifying a device so that it can no longer perform its function. In the case of storage media, all data is erased, and the media can no longer be used to retrieve or restore information.

PIN: Personal Identification Number. It is the code that you are required to provide when using your bank card or a chip-enabled credit card. It is a form of a password.

Portable media: devices and objects such as USB keys, CD-ROMs and DVDs.

Power-on password: a password that must be entered after a device has been "turned on" but before any applications can be used.

Protocol: a series of methods and steps to perform a task. Computing devices and networks rely on these to perform their functions. Often referred to by their

acronym, such as TCP: Transmission Control Protocol, AES: Advanced Encryption Standard, SSL: Secure Sockets Layer.

Public insecure areas: locations where it is possible for people to be able to observe the data a user is viewing, either by reading their screen, accessing their device while the user is away, or by intercepting information while it is being transmitted.

Public network: a network that is not controlled by the University of Windsor. Examples include the Internet, the network within public libraries and the wireless networks in coffee shops.

Recoverable: a piece of data is recoverable if it is possible to reproduce it or re-issue it from the source. In the case of passwords, it means that a user can be given their password again in case it is forgotten.

Secure computing device: a device that meets the requirements of the policy for providing access to information. This typically includes password access and encryption during transport and storage.

Secure network: a network that is able to ensure that information carried can only be viewed by the authorized user.

Security software: software designed to increase or ensure the protection of a device or data.
Typical examples include firewalls, antivirus software and encryption protocols.

Storage media: any device or object that can store information. This ranges from memory to hard drives, to DVD's to floppy disks to mobile phones.

Tablet computer: a specialized laptop or portable device that provides a touchscreen to access information. They are typically used in highly mobile environments like hospitals.

Terrestrial network: a network comprised of fiber-optic cable and wiring to connect devices to each other. This is the traditional network in offices where the computer is connected by a cable to a wall jack.

Transaction: an operation performed using a computer network. An example would be requesting a web page.

Transfer: the operation of sending data from one computing device to another. Synonymous with transmission.

Transmission: the operation of sending data from one computing device to another. Synonymous with transfer.

USB: Universal Serial Bus. A way of connecting devices to one another. Typical uses include memory keys being connected to USB connectors on a desktop computer or a USB cable being used to link a mobile phone to a laptop.

USB key: synonymous with memory stick or memory key, it is a medium-capacity form of drive storage media that can be easily moved from one machine to another.

User authenticated: a requirement that in order for a device to be used, it must require a user to provide information such as a password.

Virtual Private Network: a software protocol that encrypts transmission between two computing devices. It ensures that even if the transmission is over a public network, the data is sent and received securely.

Virus protection: software that monitors a computing device to ensure that the data and software on a device are legitimate and do not pose hidden threats.

VPN: A Virtual Private Network.

Wireless connection: a link established between a computing device and a wireless network to permit transmission of data.

Wireless network: a computer network that uses radio signals instead of wires or fiber optic cables. Often less secure than a terrestrial network because radio signals are easier to intercept.