a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #01
Security Classification of UBC Electronic Information

Introduction

1. UBC Electronic Information used by Users, has varying degrees of sensitivity which have corresponding levels of risk and protection requirements; therefore, it is necessary to classify this information to ensure it has the appropriate level of protection.
2. This standard explains how UBC Electronic Information is classified using UBC's three-level Information Security Classification Model.
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.

Information Security Classification Model

4. UBC Electronic Information is classified as follows:

	Confidential	Sensitive	Public
Definition	UBC Electronic Information that must be protected by law or industry regulation from unauthorized access, use or destruction	UBC Electronic Information that is not protected by law or industry regulation from unauthorized access, use or destruction, but could cause harm to UBC or others if released to unauthorized individuals	UBC Electronic Information that may be freely released to the public

Examples	• Personal Information, which must be protected under the *Freedom of Information and Protection of Privacy Act.* Examples:
	  • Official government identity card No. (e.g. Social Insurance No., Drivers' License No.)
	  • Bank Account Information
	  • Personal Health Information (PHI)
	  • Biometric data
	  • Full face photographic images
	  • Date of Birth (DoB)
	  • Student name
	  • Student or Employee ID
	  • Student grades
	  • Home address
	• Payment Card Industry (PCI) Information, which must be protected under the Payment Card Industry – Data Security Standard (PCI-DSS). (e.g. credit card numbers, names, expiry dates, or PINs)
		• Proprietary information received from a third party under a non-disclosure agreement
		• Restricted circulation library journals
		• Research information of a non-personal nature
		• Financial information and records
		• Information that could allow somebody to harm the security of individuals, systems or facilities
		• Any information that is not Confidential and is not generally made available to the public
			• Names and work contact information of UBC faculty and staff members
			• Information that is posted on our public website

Potential Impact of Loss	High (e.g. significant harm to one or more individuals, identity theft, severe impact to University reputation or operations, financial loss, such as fines of up to $500,000, increased credit card transaction fees)	Moderate (e.g. reputational and financial impact, loss of priority of publication, loss of access to journals and other copyrighted materials)	Low (e.g. minor embarrassment, minor operational disruptions)

Responsibility for Classifying Information

5. The Administrative Head of Unit is responsible for creating an inventory of all UBC Electronic Information under his/her control and determining its information security classification. This responsibility may be delegated to the Information Steward/Owner.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #02
Password and Passphrase Protection

Introduction

1. This document defines standards for the creation and use of passwords and passphrases to protect the UBC Electronic Information that Users handle.
2. Passwords (words or strings of characters) and passphrases (sequences of words or other text) are common and important ways to access and protect digital information on or off the Internet through almost any type of device. Consequently, attackers attempting to access information use a variety of tools to guess or steal passwords/passphrases.
3. In summary, the top three ways to keep a password/passphrase safe and protect the information are:
    a. create a strong password/passphrase;
    b. guard it carefully (e.g. don't share it or write it down); and
    c. avoid reusing it for other systems.
4. 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.

Creating a Password/Passphrase

5. Passwords must contain a minimum of 8 characters including upper and lower case letters, numbers and symbols. Alternatively, use a passphrase with a minimum of 16 characters. Guidelines for consideration:
    a. To create a complex short password, consider using the first letter of each word in a phrase. For example, "I ride my bike to school at 7 AM!" becomes "Irmbtsa7AM!".
    b. To create a passphrase, consider using a sentence or part of a sentence, or a phrase of disconnected words (e.g. "plug in sunshine thimbles" or "stingers sing paint").
    c. Avoid using a password/passphrase that replaces a letter with a number, such as "Br0adcast!" where the "O" is replaced with a zero. Password guessing programs can easily crack these.
    d. Password generation and storage programs should be used to create and manage passwords/passphrases.
    e. Name, username, address, or date of birth should not be used to create a password/passphrase. These items are too easily guessed by attackers. Also, any term that can be guessed by someone that Users know well should not be used.

Bad (Easy to Guess)	Good (Hard to Guess)
password	Pass turtle phrase
123456	the sky sings gold
12345678	One plus two beach
abc123	ABC is not like 123
qwerty	Quietly walks trees.
monkey	Monkey Pats Dog
dragon	Dragon singes cat!
111111	1 pickle flies badly
letmein	let me cloud in

Changing a Password/Passphrase

6. Passwords/passphrases for all university user accounts must be changed annually. When changing a password/passphrase:
    a. do not use the 10 most recent passwords/passphrases that have been used on the same system;
    b. do not use the same passwords/passphrases for personal accounts and university accounts; and
    c. it is recommended to use unique passwords/passphrases for different accounts, so that even if one is stolen, it does not allow access to other accounts owned by the same User; however, it is acceptable to use the same password/passphrase across university accounts.

Protecting a Password/Passphrase

7. If a password/passphrase is written down, it must be locked away in a secure, inaccessible location such as a safe.
8. Best practices state that passwords should not be shared for any reason - even with trusted individuals such as supervisors.
9. University IT Support Staff will never ask for Users' passwords.
10. Do not respond to Emails or phone calls requesting passwords/passphrases, even if they appear to be from a trusted source. These requests are often attempts to steal Users' credentials.

Case Study: Why You Shouldn't Share Your Password

A single user ID and password was shared amongst a research lab's personnel. One of these individuals maliciously destroyed some of the data in the account. Since this was a shared account, it was challenging to identify the responsible party.

11. Passwords/passphrases must be immediately changed if there are suspicions that they could have been compromised and the incident must be reported to UBC Information Security (see the Reporting Information Security Incidents standard).
12. If a password safe (an application for securely storing multiple passwords) is to be used, refer to the Password Safe guideline.

Passwords/Passphrases for Mobile Devices

13. Laptops and Mobile Computing Devices must be configured with passwords. Due to Mobile Computing Devices (smartphones and tablets) having touch-screen interfaces, it is not practical to use a strong password to lock the device. Instead, a password/PIN lock that is at least 5 characters long can be used.
14. See the Securing Computing and Mobile Storage Devices/Media standard for further requirements regarding mobile device security.

Choosing your PIN

A simple PIN option is to think of a 5 or 6 letter word and spell it out using the letters on the numeric key pad. Example: HOUSE becomes "46873".

Additional Requirements for University IT Support Staff

15. For University IT Support Staff, there are additional requirements around the storage of passwords/passphrases. These requirements are detailed in the User Account Management standard.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Securing Computing and Mobile Storage Devices/Media standard

Reporting Information Security Incidents standard

User Account Management standard

Password Safe guideline

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

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #04
Reporting Information Security Incidents

Introduction

1. Compromises in security can potentially occur at every level of computing from an individual's desktop computer to the largest and best-protected systems on campus. Incidents can be accidental or deliberate attempts to break into systems; purpose or consequence can be from benign to malicious. Regardless, each incident requires a careful response, at a level commensurate with its potential to cause harm to an individual and the University, as a whole, as defined in the UBC Incident Response Plan.
2. This document defines standards for Users to report any suspicious incidents relating to the security of UBC Electronic Information and Systems. University IT Support Staff (including both departmental IT and UBC IT staff) are responsible for handling security incidents in coordination with UBC IT Information Security.
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 security@ubc.ca.

Incidents which Must be Reported

4. Users must report the following information security incidents (if there is uncertainty whether a violation has occurred, Users must err on the side of caution and report the incident anyway):
    a. all violations of Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems; examples include but are not limited to:
        i. use of UBC computing facilities to commit illegal acts;
        ii. unsolicited or spam email originating from UBC sources;
        iii. unauthorized access, use, alteration or destruction of UBC Electronic Information or UBC Systems, including but not limited to: software, computing equipment, Merchant Systems, network equipment and services; and
        iv. theft of any UBC Electronic Information whether it be via electronic means or physical theft of any Device containing this information.
    b. unauthorized wireless access points discovered in either merchant areas or areas accessing, transmitting or storing UBC Electronic Information; and
    c. use of Malicious Code, which may show up as unexplained behavior on desktops, laptops or servers such as webpages opening by themselves, new files or folders appearing on the local hard drive, and lockouts of user accounts.

How to Report Incidents

5. Users must immediately report all suspected information security incidents as follows:
    a. to Information Security at security@ubc.ca or via phone to the IT Service Centre at 604-822-6141. Information Security will coordinate the incident as required in accordance with the UBC Incident Response Plan;
    b. to their supervisor and University IT Support Staff who are assigned to their unit; and
    c. where the incident involves physical security issues on a UBC campus, in addition to information security issues, to Campus Security.

It is essential to report incidents immediately, as time is of the essence when dealing with information security breaches and other potentially damaging incidents arising from malicious code.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

UBC Incident Response Plan

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #05
Encryption Requirements

Introduction

1. Encryption is the process of making information unreadable, to protect it from unauthorized access. After information has been encrypted, a secret key or password is needed to unencrypt it and make it readable again. This document defines standards that Users must comply with for encrypting Devices and files to safeguard Confidential Information. This standard does not apply to Sensitive or Public Information. This standard may also be used to protect the User's own personal data, e.g. personal banking information.
2. This standard incorporates the legal requirement to encrypt Personal Information (a type of Confidential Information) stored on a laptop or a mobile Device, which has been affirmed by the British Columbia Information and Privacy Commissioner in her interpretation of the *Freedom of Information and Protection of Privacy Act*.
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.

Password Protection and Zipping

4. Password protecting a Device or file merely creates a barrier that can be easily bypassed by a technically knowledgeable individual. By contrast, encrypting a Device or file protects information by "scrambling" it to make it unreadable. It is virtually impossible to bypass encryption that complies with UBC standards.
5. Also, Zipping files does not automatically encrypt them; a Zip file is simply a way to compress data into an easy-to-transport package. Most Zip programs contain the ability to protect the compressed file with strong encryption, but this feature is not turned on by default.

Device-Level Encryption Requirements

6. Wherever possible, encryption should be implemented at the Device level, as follows:

Device	Encryption Requirements for Confidential Information[1]	Recommended Encryption Toolset
Servers	Encryption is not required if server is located in a datacentre that complies with the Physical Security of UBC Datacentres standard. Otherwise, full disk encryption is recommended	UBC IT Encryption Service
Desktop computers	Full disk encryption is recommended	UBC IT Encryption Service
Laptop computers	Full disk encryption is required	UBC IT Encryption Service
Mobile Computing Devices (e.g. smartphones, tablet computers)	Device-level encryption is required	iOS Devices connecting to FASmail using ActiveSync are automatically encrypted; for other Devices refer to Encrypting Mobile Devices guideline
Mobile Storage Devices/Media (e.g. USB keys, CDs, DVDs, tapes, portable hard drives)	Device/media-level encryption is required	Refer to How to Encrypt USB Sticks and Other Removable Media guideline

[1] Additional requirements for these types of Devices are set out in the standards on Working Remotely and Securing Computing and Mobile Storage Devices/Media

7. Using Mobile Devices to store Confidential Information is not recommended. However, there may be situations where this is necessary. For example, USB sticks are commonly used to transport large amounts of information. Also, if a Mobile Device is used to access email, these emails (including emails containing Confidential Information) may be backed up automatically on the Device. In both of these situations, encryption would be required.
8. If Users are travelling abroad with a laptop that has an encrypted drive or that contains encrypted information, authorities of that country may require them to unencrypt the information or hand over the encryption keys (see Security Considerations for International Travel with Mobile Devices guideline).
9. If a Device is lost or stolen, it is essential for the University to be able to accurately report on its encryption status; to that end, Users must either:
    a. ensure that encrypted UBC-owned Devices automatically report their encryption status (whenever connected to the UBC network) to validate that encryption was active at the time of loss or theft (UBC's Encryption Service offers this functionality); or
    b. provide a written confirmation of the encryption status at the time of loss or theft.

File-Level Encryption Requirements

10. When it is not feasible to apply encryption controls at the Device level, it is recommended that any files that contain Confidential Information be encrypted.
11. For instructions on encrypting Word, Excel and other general files, refer to the How to Encrypt Files Using Common Applications guideline.
12. For requirements on emailing Confidential Information, refer to the Transmission and Sharing of UBC Electronic Information standard.

Password Requirements

13. Strong passwords must be used for encryption in compliance with the Password and Passphrase Protection standard.
14. If the password (also called a "key") is forgotten or lost, the data may be unrecoverable. Therefore, it is essential to have a key recovery strategy. Users can use the University's reliable Key Escrow service, or simply write down the password and store it in a secure location such as a safe. Further information about key recovery, can be found in the Cryptographic Controls standard.

Technical Requirements

15. UBC's minimum encryption standard is AES-128 bit encryption or equivalent; AES-256 bit encryption is recommended. Further technical requirements can be found in the Cryptographic Controls standard. University IT Support Staff, including staff in the IT Service Centre, are available to assist Users to implement these requirements where necessary.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Cryptographic Controls standard

Password and Passphrase Protection standard

Securing Computing and Mobile Storage Devices/Media standard

Transmission and Sharing of UBC Electronic Information standard

Working Remotely standard

Encrypting Mobile Devices guideline

How to Encrypt Files Using Common Applications guideline

How to Encrypt USB Sticks and Other Removable Media guideline

Security Considerations for International Travel with Mobile Devices guideline

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 Confidential or Sensitive 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 104, 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 UBC Electronic 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 Confidential or Sensitive UBC Electronic Information using third party Devices, such as kiosks in public libraries, hotels, airports, and cyber cafes.
7. Use caution when accessing UBC Electronic Information via 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 104, Acceptable Use and Security of UBC Electronic Information and Systems

Securing Computing and Mobile Storage Devices/Media standard

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #07
Securing Computing and Mobile Storage Devices/Media

Introduction

1. All Devices used for University Business – no matter whether they are owned by the University, by the User, or by a third party – need to be protected from theft and/or unauthorized access. This standard specifies the minimum security requirements that Users must comply with to protect these Devices. University IT Support Staff, including staff in the IT Service Centre, are available to assist Users in implementing these requirements where necessary.
2. Two broad categories of Devices are covered by this standard:
    a. Computing Devices, e.g. servers, desktop and laptop computers, tablets and smartphones; and
    b. Mobile Storage Devices/Media, e.g. external hard drives, DVDs, and USB keys.
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.

Electronic Security

4. Computing Devices used for University Business must comply with the following electronic security requirements. Users with IT-related responsibilities should also see the Vulnerability Management standard.

<table>
<tr><th></th><th>Servers</th><th>Desktops & Laptops</th><th>Tablets & Smartphones</th></tr>
<tr><td>Password Control</td><td colspan="3">All Devices must be password-protected in accordance with the Password and Passphrase Protection standard. Always lock Devices or log out before leaving them unattended.</td></tr>
<tr><td>Screensaver Locks</td><td>Automatically activate after no more than 5 minutes of inactivity</td><td colspan="2">Automatically activate after no more than 30 minutes of inactivity (5 minutes is recommended for devices storing Confidential or Sensitive Information)</td></tr>
<tr><td>Device Location</td><td colspan="2">n/a</td><td>Enable any features that will allow the Device to be remotely located in the event of loss or theft</td></tr>
<tr><td>Data Destruction</td><td colspan="2">n/a</td><td>Enable the feature that automatically erases data if 10 consecutive incorrect passwords are entered</td></tr>
<tr><td>Remote Wiping</td><td colspan="2">n/a</td><td>Enable any features that will allow data stored on the Device to be erased in the event of loss or theft</td></tr>
<tr><td>Antivirus & Spyware</td><td colspan="3">Install up-to-date antivirus and spyware cleaning software and configure it to update at least once per day (except for tablets and smartphones that do not offer this feature). See the Antivirus Protection Guideline.</td></tr>
<tr><td>Firewalls</td><td colspan="3">Install and configure firewalls (except for tablets and smartphones hat do not offer this feature). See the Firewalls Guideline.</td></tr>
</table>

	Servers	Desktops & Laptops	Tablets & Smartphones
Operating System	The Device must run a version of its operating system for which security updates continue to be produced and are available. If this is not possible, see the Vulnerability Management standard for compensating controls. If the Device is University-owned, software updates must not be impeded, and no unauthorized changes may be made to the Device.		
Data Availability	Any UBC Electronic Information stored on the Device must be regularly backed up to a secure location and checked periodically (preferably quarterly) to ensure the integrity and availability of the information such that it can be restored. See the Backup Guideline.		
Encryption	Refer to the Encryption Requirements standard.		

5. Mobile Storage Devices/Media used to store Confidential Information must be encrypted as explained in the Encryption Requirements standard.

Physical Security

6. For their protection, unattended Devices must be located in one or more of the following areas:
    a. a room or other enclosed area that is locked or otherwise access-controlled; and/or
    b. a locked cabinet or other fixed container such as a locked server cabinet/cage.
7. Servers containing significant quantities of Confidential Information must be hosted in UBC Datacentres that are compliant with the Physical Security of UBC Datacentres standard, because these provide the highest level of security. To get access to server space in a UBC Datacentre, Users can rent space or use the virtual server service.
8. Keys or swipe cards giving access to Devices must be limited to authorized individuals.
9. Measures should be taken to ensure Devices cannot be viewed from outside the secure area, e.g. by drawing curtains or blinds.
10. Cable locks are recommended as a supplementary security measure for Computing Devices, but they do not provide sufficient protection by themselves. It is safer to lock portable Devices, such as laptops, in a cabinet out of sight rather than relying on a cable lock.
11. The use of alarms is highly recommended, especially to protect Devices used to store Confidential or Sensitive Information.

Use of Non-University-Owned Devices

12. UBC recognizes that it is often convenient for Users to use their personally-owned Devices for work purposes and such use is permitted provided that they manage their Devices in accordance with this standard.
13. Some Users may also use Devices supplied by third parties in connection with University Business. Users, in consultation with University IT Support Staff, are responsible for determining whether these Devices meet the minimum security requirements in this standard; for example, Health Authorities have good information security measures in place, and it is acceptable to use their computers for University Business.

Special Requirements for Servers

14. Servers (especially Web and FTP servers) are attacked on a continual basis. To avoid creating security weaknesses, servers must not be used for general web browsing or email.

15. Users must not run server applications on desktops or laptops (e.g. web or FTP servers) that are Internet-Facing. Exceptions may be approved by the Administrative Head of Unit, in consultation with University IT Support Staff, provided that compensating controls are put in place to control security risks.

Inventory of UBC-owned Laptops and Desktops

16. Central UBC IT support staff must maintain an inventory of UBC-owned laptops and desktops that they have deployed, including which Users these devices are assigned to. All other University IT Support staff are recommended to maintain such inventories.

Return of Devices and Information upon Termination

17. Upon termination of their employment, Users must return all of the UBC-owned Devices in their possession to an authorized employee of UBC, and must return and delete any UBC Electronic Information stored on their personally-owned Devices.

Loss Reporting Requirement

18. Users who lose a Device used for University Business (no matter who owns the Device) or suspect that there could have been an unauthorized disclosure of UBC Electronic Information must report the loss/disclosure in accordance with the Reporting Information Security Incidents standard.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Encryption Requirements standard

Password and Passphrase Protection standard

Physical Security of UBC Datacentres standard

Reporting Information Security Incidents standard

Vulnerability Management standard

Antivirus Protection guideline

Backup guideline

Firewalls guideline

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #08
Destruction of UBC Electronic Information

Introduction

1. A large proportion of UBC Electronic Information is Confidential or Sensitive, such as student records, personnel records, financial data, and protected health or research information. If this information is not properly removed when no longer required and before the equipment is disposed of, unauthorized access may occur resulting in harm to an individual and/or the University.
2. This document defines standards for Users on the destruction and/or sanitization of UBC Electronic Information (data destruction).
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.

Responsibilities of Users

4. Users should only retain information as long as required.
5. Users are responsible for ensuring that UBC Electronic Information is always removed from a Device before it is transferred to another individual, sold, or discarded. The information needs to be removed even if it does not appear to be Confidential or Sensitive. Users should contact University IT Support Staff or the IT Service Centre if they require data destruction assistance.

Responsibilities of Service Providers

6. Where a third party Service Provider has received copies of UBC Electronic Information for the purpose of UBC work, the Service Provider must destroy all of the information in its possession within seven days of the completion of the project or termination of the agreement, whichever first occurs, using destruction methods compliant with this standard and give the Administrative Head of Unit a signed confirmation of destruction in a format consistent with the Data Destruction Confirmation procedure.
7. Where data destruction is not feasible, Administrative Head of Unit may consult with UBC Information Security to determine appropriate alternate controls.

Acceptable Data Destruction Methods

8. Any of the following are acceptable methods of data destruction:
    a. using a software utility, such as "Secure Erase", that erases, overwrites or encrypts the data;
    b. magnetically erasing (degaussing) the data;
    c. formatting a Device after encrypting it; or
    d. using a machine that physically deforms or destroys the Device to prevent the data from being recovered.
9. Using the “Empty Recycle Bin/Trash”, “Delete”, “Remove”, and “Format” operating system commands do **not** destroy data and therefore are **not** acceptable methods for preparing media for transfer or disposal.
10. Data destruction methods must comply with the minimum standards set out in the Clearing and Declassifying Electronic Data Storage Devices (ITSG-06) guideline issued by the Government of Canada.
11. Wherever encryption is used before formatting a device, it must be AES-128/256 bit encryption with strong passwords or passphrases; it is recommended that this be supplemented with other data destruction methods whenever possible.

Special Cases

12. To reuse flash memory devices (e.g. SD memory cards, USB drives) containing UBC Electronic Information, the User can encrypt the whole device according to the Encryption Requirements standard. After encryption, the User can format the device and reuse it safely.
13. Smartphones must have all data removed (factory reset) prior to being transferred to another person or being turned in for recycling; note that some smartphones have removable memory cards that need to be treated the same as flash memory devices and securely sanitized separate from a phone factory reset. Users can contact their cellular service provider if they are uncertain of how to perform a factory reset.
14. Other imaging devices with a hard drive (e.g. photocopiers, printers, fax machines, etc.) are also subject to the data destruction requirements; additionally, where possible, these devices should have image overwriting enabled. This is a function where scanned or electronic images of a document are immediately overwritten using a data destruction technique. This function is known by various names, e.g. “Immediate Image Overwrite” (Xerox), “Hard Disk Drive Erase Feature” (Canon), “Hard Disk Overwrite Feature” (HP).

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Encryption Requirements standard

Data Destruction Confirmation form

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #09
Outsourcing and Service Provider Access

Introduction

1. Service Providers (vendors, contractors, consultants and other non-UBC employees who provide services to UBC) may access, process, store or transmit UBC Electronic Information and Systems in order to deliver agreed-upon services. The increased security risk when access is extended outside of the organization needs to be managed appropriately.
2. This standard explains the information security requirements applicable to all Service Providers. The Administrative Head of Unit who engages a Service Provider is responsible for ensuring compliance with all of these requirements.
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.

Security and Privacy Risk Assessment

4. Before Service Providers are granted access to UBC Electronic Information and Systems, information security risks must be assessed and managed using the Service Provider Security Risk Assessment Checklist.

Compliance with Policies and Standards

5. Before access is granted to UBC Electronic Information and Systems, the Service Provider must be made aware that it will be subject to Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems, and its accompanying standards.

Contractual Requirements

6. Service Providers must sign a Security and Confidentiality Agreement (SACA) prior to being granted access to Confidential or Sensitive Information. The Administrative Head of Unit may request the Office of the University Counsel to grant a waiver of the requirement for a SACA where the primary contract with the Service Provider contains equivalent privacy and security language. Doctors, lawyers, accountants, auditors, psychologists and other professionals who are bound by a duty of confidentiality do not need to sign a SACA.

Storage and Transmission of Information

7. Service Providers must store UBC Electronic Information in a separate system or database, ensuring that the information is not mixed with information belonging to or accessed by other parties. If this is not possible, Service Providers may use alternative controls, with the written approval of the Administrative Head of Unit, to ensure that the data is secure and can be destroyed after the project is completed.
8. Service Providers must not access or store Personal Information (PI) outside Canada, as that would violate the Freedom of Information and Protection of Privacy Act (FIPPA). It should be noted that UBC classifies PI as Confidential Information. As an exception, temporary access or storage outside of Canada is allowed, provided that this is:
    a. necessary for installing, implementing, maintaining, repairing, trouble-shooting or upgrading an electronic system or recovering data from such a system; and
    b. limited to the minimum amount of time necessary for that purpose.
9. Service Providers must ensure that they transmit UBC Electronic Information in accordance with the Transmission and Sharing of UBC Electronic Information standard.

Access Controls

10. All Service Provider access to UBC Electronic Information and Systems must be granted as follows:
    a. access must be authenticated and role based;
    b. access must be granted on a principle of 'least privilege' (only the minimum level of access that is required to perform their duties); and
    c. wherever possible, access to UBC Systems containing Confidential Information should be logged.

Ongoing Monitoring

11. The work of Service Providers must be monitored and reviewed to ensure that privacy, confidentiality and information security requirements are being satisfied.

End of Services and Data Destruction

12. Immediately upon completion of the project or termination of the agreement, whichever first occurs, the following must take place:
    a. the Administrative Head of Unit must ensure that the Service Provider's access to UBC Electronic Information and Systems is revoked; and
    b. the Service Provider must stop accessing UBC Electronic Information and Systems.
13. Within seven days of the completion of the project or termination of the agreement, whichever first occurs, the following must take place:
    a. the Service Provider must return all UBC assets (including access control cards and keys), equipment, and UBC Electronic Information in their possession; and
    b. the Service Provider must destroy all UBC Electronic Information and hard copies of this information in its possession in compliance with the Destruction of UBC Electronic Information standard.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Destruction of UBC Electronic Information standard

Transmission and Sharing of Electronic Information standard

Security and Confidentiality Agreement

Service Provider Security Risk Assessment Checklist

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #10
Accessing Electronic Accounts and Records

Introduction

1. This document defines standards that Users must comply with to gain access to electronic accounts and records on UBC Systems, such as email accounts, Student Information System accounts, voicemail accounts, internet usage records, and telephone logs. This standard does not apply to system administrators or other technical personnel who, in the course of carrying out their duties, require access for technical purposes, such as installation, maintenance, repair, troubleshooting, or upgrading.
2. The purpose of this standard is to protect the personal information of individual account holders while continuing to allow access to information required for University purposes.
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.

Access with Consent

4. Policy #104 authorizes reasonable personal use of UBC Systems. For privacy reasons, it is preferable to get the consent of Users before accessing electronic accounts and records.
5. Consent must be in writing, but does not need to be signed (an email is acceptable). The following language is recommended for a consent statement:

   I, [NAME], authorize UBC to access [ACCOUNTS/RECORDS] for the following purpose: [PURPOSE]. This authorization is effective until [DATE].

6. If the consent of the User has been secured, authorization of the Administrative Head of Unit or the Office of the University Counsel is not required to access the account or records in question.

Access without Consent

7. It is occasionally necessary to gain access to an electronic account or record without the User's consent. To ensure that the University's Business requirements are balanced against the User's privacy interests, access without consent requires the authorization of the Administrative Head of Unit and the Office of the University Counsel. This authorization will depend on the type of information intended to be accessed and how the information will be used after it has been accessed.

Criteria for Access to UBC Electronic Information without Consent

8. If UBC Electronic Information only needs to be viewed, then the Administrative Head of Unit and the Office of the University Counsel will authorize access the electronic accounts/records provided that:
   a. there is a pressing reason to view this information for University Business purposes, and
   b. consent of the User cannot be secured despite making reasonable attempts to do so, e.g. the User is incapacitated, has gone on vacation without leaving contact information, or has been terminated and is unwilling or unavailable to provide consent.
9. When accessing accounts or records to view UBC Electronic Information, reasonable efforts must be made to avoid viewing the User's Personal Use Records. If Personal Use Records have been inadvertently viewed, then these records must not be copied, altered, deleted, used or disclosed unless they provide evidence of a violation of law, in which case the matter must be referred to the Office of the University Counsel, which will determine the appropriate action.

Example

An employee has been incapacitated in a motor vehicle accident. Her supervisor needs to access the employee's work email account to check for any time-sensitive work-related messages, but the employee is unable to consent to this access. Under these circumstances, access would normally be authorized. However, the supervisor should not read the employee's personal messages.

10. In addition to Personal Use Records, accounts may also contain other sensitive information, such as teaching materials or research information. The confidentiality of this information must be respected as its unauthorized use and disclosure may harm the interests of the User and the University as a whole.

Criteria for Access to Personal Use Records without Consent

11. If Personal Use Records need to be viewed, then the Administrative Head of Unit and the Office of the University Counsel will only authorize access to electronic accounts/records if the University is legally required to do so, or if securing consent would compromise:
    a. the health or safety of an individual or a group of people,
    b. the availability or accuracy of the information, or
    c. an investigation or a proceeding related to a breach of law or policy or the employment of the User.

Procedure for Access

12. To access accounts and records, the Request to Access Electronic Accounts and Records form must be completed and submitted to the administrator who controls access to the account. If the User's consent is not obtained, the Administrative Head of Unit and the Office of the University Counsel must be requested to sign the access form to authorize access. The administrator will grant access to the account/records only for the period of time specified in the access form.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Request to Access Electronic Accounts and Records form

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #11
User Account Management

Introduction

1. User Accounts control access to UBC Electronic Information and Systems. This document defines standards that Information Stewards/Owners must comply with when managing these accounts throughout their lifecycle to ensure individual accountability exists and access is restricted on a 'need to know' basis. In addition to this standard, Privileged Accounts must also comply with the Privileged Account Management standard.
2. 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.

Creating User Accounts

3. Applications for User Accounts must be reviewed and approved and a record must be kept of all Users being granted these accounts and who provided authorization. This record must be retained for at least one year.
4. Service Providers applying for User Accounts must comply with the Outsourcing and Service Provider Access standard.
5. All User Accounts must be uniquely identifiable to a specific User.
6. Users must be granted the minimum level of access for their defined job function (i.e. the principle of "least privilege").
7. User Accounts must not be shared. Accounts must be traceable back to the individuals using them. This requirement does not apply to test accounts, which may be shared during the pre-production phase.
8. Where possible, User Accounts should be linked to sources of record that can accurately capture User status (e.g. HRMS, SIS).

Examples of User Accounts

- FASmail
- Student email
- Student Information System (SIS)
- Financial Management System (FMS)
- Workspace
- Home network drive
- Login account (Active Directory or equivalent)

Changing User Account Access Rights

9. When Users' roles and responsibilities change, their access rights should be updated in a timely manner to ensure they remain aligned with the "least privilege" principle.
10. Changes to User Accounts should be documented, approved and retained by Information Stewards/Owners in the same manner as User account requests.

Disabling User Accounts

11. All User Accounts must be disabled (i.e. access is revoked) in a timely manner, especially when the User has been terminated or the User has a Privileged Account. Accounts may be disabled by either closing the account to all Users or changing the password to restrict access by specific Users.
12. On Merchant Systems, User accounts must be automatically disabled if not used for 90 days.
13. The information stored in disabled accounts, as well as the username, logs and other metadata for these accounts, must be retained for one year, except for the following accounts:

Account	Retention
Student Email	TBD, currently indefinite
Student Email Alias	TBD, currently indefinite
Home Drive	90 days

14. In cases where accounts are migrated from one authentication system to another, the original account does not need to be retained, provided all of the information in the account has been migrated to the new system.
15. At any time before the expiration of the relevant retention period, the account can be reinstated to the account holder where appropriate.
16. After the expiration of the relevant retention period, the account and the information stored within it must be securely deleted.

Reviewing User Accounts

17. Users' access rights must be reviewed at regular intervals to ensure they remain aligned with current roles and responsibilities. The frequency of the review must be risk based (e.g. access rights to Confidential Information such as personal health information should be reviewed more frequently than access rights to Sensitive Information that may not do as much harm if exposed to unauthorized individuals).

Security of User Accounts and Authentication Systems

18. University IT Support Staff must protect User Accounts in compliance with Securing User Accounts standard.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Outsourcing and Service Provider Access standard

Privileged Account Management standard

Securing User Accounts standard

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #12
Privileged Account Management

Introduction

1. Privileged Accounts provide a very high degree of access to UBC Electronic Information and Systems and therefore pose a significant risk if used in an unauthorized manner.
2. This standard establishes requirements for the management and use of Privileged Accounts. Unless otherwise stated, Privileged Accounts are subject to the same requirements as User Accounts, as set out in the User Account Management standard. The purpose of this standard is to highlight the different or enhanced security controls that must be in place to protect Privileged Accounts.
3. The Information Steward/Owner is responsible for compliance with this standard.
4. 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.

Types of Privileged Accounts

5. Privileged Accounts are usually categorized into the following types:

Privileged Account Type	Description
Privileged Personal Accounts	Privileged Accounts assigned to individual Users (usually University IT Support Staff). Examples include the following privileged groups which Users are added to in order to elevate their privileges to the associated group access levels: DBA user, Exchange Admins, Domain Admins.
Generic/Shared Administrative Accounts	Privileged Accounts that exist in virtually every device or software application; these accounts hold "super user" privileges and are often shared among University IT Support Staff. These accounts may be used by multiple Users. Examples: Windows Administrator, UNIX root, Oracle SYS, SA.
Emergency Accounts	Generic Privileged Accounts used by the enterprise when elevated privileges are required for business continuity, disaster recovery, or to fix urgent problems. These accounts may be used by multiple Users. Also called: break-glass accounts, fire-call IDs.
Service Accounts	Privileged Accounts that provide a security context to a running service, daemon or process, such as a file server, web server, e-mail server, etc., or are used by applications to access databases and other applications; these accounts typically have broad access to underlying business information in databases. Also called: app2app accounts, as they are used by one application to sign into another.

Creating Privileged Accounts

6. Privileged Accounts may be shared between multiple Users (except for Privileged Personal Accounts, which must be assigned to unique individuals). However, for all account types, a single individual must be assigned with accountability for the security of the account.
7. Approval procedures for granting access to Privileged Accounts are set out in Authorization for Privileged Account Access procedure.

Protecting Privileged Account Passwords

8. Service Accounts must not be shared between applications or services, i.e. a separate account must be created for each application/service.
9. Passwords for Privileged Personal Accounts must be changed regularly, in compliance with the Password and Passphrase Protection standard, or at an interval stipulated by the Information Steward/Owner.
10. Passwords for Generic/Shared Administrative Accounts and Emergency Accounts should be machine generated and held in a secure place, available to system administrators in the case of an emergency through a Break Glass Procedure created by the Information Steward/Owner.

11. A Break Glass Procedure (which draws its name from breaking the glass to pull a fire alarm) refers to a quick means for a person who does not have access to a Privileged Account to gain access in an emergency. When a Break Glass Procedure is used, access to the Privileged Account must be:
    a. limited to the minimum amount of time necessary;
    b. associated to a change, problem or incident number/ticket;
    c. recorded by the specific database, system, or application; and
    d. logged in an auditable record (which identifies the individual User who 'broke the glass') for later review.
12. After a Break Glass Procedure has been completed, the password for the Privileged Account must be changed.

Logging Privileged Accounts

13. There are special requirements for logging Privileged Account activity, which are set out in the Logging and Monitoring of UBC Systems standard.

Reviewing Privileged Accounts

14. Access to Privileged Accounts must be reviewed at an interval stipulated by the Information Steward/Owner, or at a minimum annually, to validate that they remain restricted to authorized personnel. Discrepancies must be reported in a in a timely manner to the Information Steward/Owner for resolution.

Responsibilities of Users with Access to Privileged Accounts

15. As Privileged Accounts provide a significant level of control over UBC Electronic Information and Systems, individuals with access to these accounts are expected to exercise a higher degree of caution than for User Accounts.
16. All Users with access to Privileged Accounts must maintain the confidentiality of any information that they have access to both during, and after, their employment with UBC.
17. All Users with access to Privileged Accounts:
    a. must not use Privileged Accounts for day-to-day activities, such as email and web browsing;
    b. wherever possible, must not use Privileged Accounts (except Service Accounts) to run daemons, services or applications.
18. University IT Support Staff with access to Privileged Accounts must also comply with the System Administrators' Code of Ethics.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Logging and Monitoring of UBC Systems standard

Password and Passphrase Protection standard

User Account Management standard

Authorization for Privileged Account Access procedure

System Administrators' Code of Ethics

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #13
Securing User Accounts

Introduction

1. User Accounts control access to UBC Electronic Information and Systems and as such they must be effectively protected against unauthorized access. This standard is closely tied to the User Account Management standard.
2. This document defines standards that University IT Support Staff must comply with when securing these accounts.
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.

Password Protection Requirements

4. All User Accounts must be password protected in accordance with the Password and Passphrase Protection standard. Where possible, systems should enforce password complexity rules in accordance with that standard.
5. Users who receive new accounts or who require a replacement password must be provided with a temporary password, which is forced to change upon first login. Temporary passwords must be given to Users in a secure manner.
6. Procedures must be established to verify the identity of a User prior to providing a new, replacement or temporary password for an account. It is recommended that identification procedures follow the standard practice of validating the answers to three questions that were previously created by the User during account creation (this procedure is mandatory for CWL password changes).
7. Default vendor passwords must be changed following the installation of systems or software.

Authentication System Requirements

8. Where possible, all User Accounts should be centrally controlled in the UBC Enterprise Active Directory, Enterprise LDAP, or Campus-Wide Login.
9. Authentication systems for User Accounts must be adequately protected from password cracking using at least one of the following methods:
    a. the account is locked for a period of time if an incorrect number of passwords/passphrases is entered over a specified time period (for example, if an incorrect password/passphrase is entered 10 times within a 30 minute window, the account will be locked for 30 minutes); and/or
    b. each time an incorrect password/passphrase is entered, the system introduces a delay before providing the failure response; this delay increases as the failed login attempts continue but will reset once the User successfully logs in (for example, the delay period could begin at 100 milliseconds, and double after each subsequent failed login).
10. Authentication systems must not store account passwords in clear text. Where possible, passwords should be stored using a strong cryptographic hash and salted; for further guidance see Salted Password Hashing - Doing it Right.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Password and Passphrase Protection standard

User Account Management standard

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #14
Vulnerability Management

Introduction

1. This document defines standards for protecting UBC Systems through vulnerability management, which is a security practice designed to proactively reduce the chance of exploitation of IT vulnerabilities, which could cause considerable reputational damage, cost and disruption. Effective vulnerability management includes patch management, vulnerability scanning, anti-virus, and secure configuration of systems, particularly firewalls. Unless otherwise stated in this standard, vulnerability management is the responsibility of University IT Support Staff.
2. This standard applies to UBC Systems containing Confidential or Sensitive Information and may also be applied to other systems where appropriate.
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.

Patch Management

4. University IT Support Staff are responsible for subscribing to the Appropriate Notification Services to ensure they are aware of new vulnerabilities and corresponding patches as soon as they are available.
5. Unpatched software is frequently exploited by malicious individuals to access information or resources. To mitigate this threat, vendor provided patches for UBC Systems (e.g. operating systems, applications, databases, etc.) must be applied as follows:
    a. High-Severity Vulnerabilities (as defined in the Severity Ratings for Vulnerabilities (CVSS v2.0)) must be patched as soon as possible, preferably within 3 days of the patch release; and
    b. Medium-Severity Vulnerabilities (as defined in the CVSS v2) must be addressed (i.e. patched) as soon as possible, once all high-severity vulnerabilities have been resolved.
6. Patch management procedures must prioritize patches based on the severity of the vulnerability being patched, the sensitivity of the data in the system, and the criticality of the system to University Business. A back-out or roll-back procedure should also be in place so that the patch can easily be removed in the event of a serious problem.
7. Backups should be completed before applying any significant patches, in case of unexpected problems.
8. Operating system and application updates/patches must be installed as follows:
    a. to the extent possible, desktops, laptops and servers must be configured to install these updates and patches automatically;
    b. where automatic installation is not feasible, all security-related updates and patches must be manually installed at the earliest opportunity, in accordance with their severity, as outlined in section 4 above;
    c. where security-related updates and patches are not installed, the risks must be mitigated with compensating controls; and
    d. where the system is at end of life and security-related updates and patches are no longer available from the vendor, then you must either upgrade the system or implement compensating controls.
9. Embedded instrument systems that run **Windows 95/98/XP/Vista/7 Embedded Operating System** or any other embedded operating system that can only be patched by the hardware vendor, frequently will have vulnerabilities for which there are no patches to protect the system. In this case, it is important to look at compensating controls, which will protect the system and reduce the risk of unauthorized access to information or resources. A possible compensating control may be to isolate the embedded system, so that it has no access to the internet or other systems, with the exception of a “proxy” system. The proxy system will be able to access other computers and the internet and through a dedicated interface, it can communicate with the embedded system. Provided the proxy system can be well patched and secured, the risk of access to the unpatched embedded system is reduced to a reasonable level by this control.

Vulnerability Scanning

10. UBC IT is responsible for ensuring that all operational UBC Systems attached to the UBC network are scanned with a network vulnerability scanning tool (e.g. Nessus) at least every quarter.
11. All new or substantially modified Internet-facing servers attached to the UBC network should be scanned for vulnerabilities prior to going into production. Any detected vulnerabilities must be resolved in accordance with their severity, as outlined in section 5 above; rescans are required until passing results are obtained.

Penetration Testing

12. It is highly recommended that Penetration Testing be conducted for high-risk UBC Systems, such as Merchant Systems and systems containing personal health information. To find a qualified penetration testing service, contact information.security@ubc.ca.

Antivirus and Hardening

13. Anti-virus protects against malicious code and is another layer of defense to help protect against exploitation of vulnerabilities.
14. Desktops, laptops and servers connected to UBC's network or other networked resources must have anti-virus software installed and configured, so that the virus definition files are updated daily. The anti-virus software must be actively running on these devices and kept up to date.
15. Unused services on servers should be disabled, and operating systems and applications should be hardened against external threats, see the UBC Systems and Applications Hardening Guides for recommended configurations.

Firewall Configuration

16. Firewalls provide an effective compensating control for many types of vulnerabilities for which patches are not readily available; these are known as zero-day vulnerabilities. UBC Systems storing Confidential or Sensitive Information must be protected by a firewall.
17. Firewalls are only as effective as their Access Control List (ACL) rule set, which determines how traffic is blocked or passed. Firewall ACL rule sets must be configured as follows:
    a. a "Deny by Default" policy must be implemented on all firewalls;
    b. services that are not explicitly permitted must be denied;
    c. firewalls must use ingress filtering at a minimum and must use egress filtering if it is used to protect Confidential Information;
    d. ACLs must restrict traffic to the minimum necessary to conduct University Business; and
    e. rule sets must be reviewed annually for optimization and validation of effective rules.
18. Network-based firewalls configured to control access to different zones must be dedicated firewalls. Firewalls should never be used for multiple purposes beyond access control and monitoring. Next Generation firewalls, Unified Threat Management (UTM) and virtual firewalls are still considered to be dedicated.
19. Where high availability is required, standby firewalls should be configured to take over the services of primary firewalls in the event that the primary fails. This also implies that standby firewalls must be kept up to date with changes made to the primary firewall to properly support this capability.
20. If a firewall becomes a single point of failure, it must fail in a closed state and not allow passage of data traffic through it.
21. The firewalls must be capable of "stateful packet inspection" and this capability must be turned on.
22. All firewall critical alarms must generate an automatic notification to the firewall administrator.
23. Host based firewalls should be used if available, in addition to network firewalls; this facilitates defense in depth.
24. All firewall logs should be sent to a separate machine solely dedicated to the collection of logs at an appropriate level.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems
Appropriate Notification Services guideline
Severity Ratings for Vulnerabilities (CVSS v2.0) guideline
UBC Systems and Applications Hardening Guides

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #15
Wireless Networks

Introduction

1. UBC has a large and complex wireless network that plays an integral role in the operations of the University. Consequently, intruders and hackers may consider the wireless network an attractive target to breach the security of UBC Electronic Information and Systems.
2. This standard defines requirements to ensure that wireless devices, such as Wireless Access Points (WAPs), which allow wireless devices to connect to a wired network, are deployed in a secure, controlled and centrally managed way to reduce the likelihood of a security breach. Unless otherwise indicated, the UBC IT Infrastructure Team (the "Infrastructure Team") is responsible for ensuring compliance with this standard.
3. In addition to this standard, UBC IT wireless networks provisioned by UBC IT are governed by Policy 130, Management of the Wireless Network. In particular, all new WAPs must be authorized under the terms of that policy.
4. 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.

Physical Protection

5. WAP hardware must be protected to ensure physical security mechanisms (e.g. locked cabinet, high ceiling mount, etc.) are in place to prevent theft, alteration, or misuse.

Secure Configuration

6. All WAPs should be secured using Wi-Fi Protected Access (WPA2) with a minimum of AES 128-bit encryption.
7. Wired Equivalent Privacy (WEP) is prohibited for wireless network security, as it is insecure.
8. It is recommended that Users connecting to WAPs, providing access to the UBC LAN, be configured to use the "autoconnect" ubcsecure automated client configuration tool. This will help prevent connecting to rogue WAPs, which have been setup with the same name (spoofing) to steal credentials.
9. Console access must be password protected in compliance with the Password and Passphrase Protection standard.
10. WAP and wireless controller management must be handled as follows:
    a. utilize secure protocols such as HTTPS, SSH, and CAPWAP;
    b. management must only be over the LAN interface;
    c. if SNMP is used in the management environment, all default SNMP community strings must be changed, otherwise it must be disabled;
    d. vendor defaults such as encryption keys, and administrative passwords must be changed.
11. The use of Telnet or other insecure protocols is prohibited.

Security Updates

12. The operating system or software code on WAP and wireless controllers should be patched and kept current to ensure proper protection from the latest security vulnerabilities.

Additional Wireless Requirements for Payment Card Industry (PCI) Information

13. Users responsible for Merchant Systems must:
    a. ensure that a perimeter firewall is in place between any wireless network and Merchant Systems processing Payment Card Industry (PCI) Information. These firewalls must be configured to deny or control any traffic from the wireless environment to Merchant Systems;

b. test for the presence of unauthorized WAPs on a quarterly basis. Note: Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control NAC), or wireless IDS/IPS; and
c. Report any unauthorized WAPs as a security incident, in compliance with the Reporting Information Security Incidents standard.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Policy 130, Management of the Wireless Network

Password and Passphrase Protection standard

Reporting Information Security Incidents standard

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #16
Cryptographic Controls

Introduction

1. This document defines standards for the implementation and use of encryption technologies within UBC to maintain the confidentiality and integrity of Confidential Information. For standards on when encryption is required, see the Encryption Requirements standard.
2. Cryptographic controls provide an enhanced level of protection for UBC Electronic Information in the event of theft, loss or interception by rendering information unreadable by unauthorized individuals. Unless otherwise stated, University IT Support Staff are responsible for ensuring compliance with this standard.
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.

Cryptographic Requirements

4. Encryption usage must be risk based and must take into account the sensitivity of information as per the Encryption Requirements standard.
5. Encryption strength must be AES-128 bit or equivalent, at a minimum; AES-256 bit encryption is preferred as it provides greater protection.
6. Cryptographic hash functions must be strong: SHA256, SHA512, RipeMD-160, WHIRLPOOL or equivalent.
7. Whenever a password or passphrase is used as an encryption key ("Key"), it must follow the standards defined in the Password and Passphrase Protection standard, which details strong password/passphrase construction. Keys that are compromised (e.g. lost or stolen) must be reported immediately in accordance with the Reporting Information Security Incidents standard. The Key must be revoked or destroyed and a new key generated. Key re-assignments require re-encryption of the data.
8. Digital signatures should be supported by certificates issued by a trusted third party Certificate Authority (CA); if the signatures are intended for legal signing then they must be supported third party CA certificates. The minimum acceptable hash algorithm is SHA2; SHA0 and SHA1 cannot be used as they are insecure.
9. The following requirements apply to X.509 certificates:
    a. X.509 certificates used for the securing of Sensitive or Confidential Information during User transmission must be issued by a trusted third party CA, as part of a Public-Key Infrastructure (PKI);
    b. server-to-server transmissions should be encrypted and should use a trusted third party certificate;
    c. servers must be configured to use TLS version 1.0 at a minimum; TLS version 1.1 is preferred;
    d. newly purchased or renewed X.509 certificates must be a minimum of 2048-bits; and
    e. X.509 certificates may be purchased under the University's Enterprise account, via security@ubc.ca.

Full Disk Encryption (FDE)

10. In order to help Users to comply with the above requirements, the University provides a secure and effective FDE solution to protect laptop and desktop computers.

Key Management

11. For encryption to be effective, encryption Keys must be protected against unauthorized disclosure, misuse, alteration or loss. In order to reduce the risk of loss or exposure of Keys, it is recommended that all Key management processes be performed with automated software. A Key management plan must also be in place that covers the following process areas:

Process Area	Process Description	Process Requirements
Key Generation	Secure creation of keys (symmetric encryption) or key pairs (asymmetric encryption).	• Keys must be created using cryptographically strong algorithms (see Cryptographic Requirements above).
Key Distribution	Secure distribution of keys using manual transport methods (e.g. file transfer, key loaders), automated methods (e.g. Key transport and/or Key agreement protocols), or a combination thereof.	• Keys must be encrypted when transmitted over communication lines. • The exchange of keys must employ encryption using an algorithm that is at least as strong as the one that is used to encrypt the data protected by the keys, and access must be strictly limited to those who have a need-to-know.
Key Storage and Protection	Protect all cryptographic keys against modification, loss and destruction.	• Keys and their associated software products must be securely maintained for the life of the archived data that was encrypted with that product. • Keys must be protected using the same or superior level of security as the information that they are protecting, and access must be strictly limited to those who have a need-to-know. • In public-private key encryption, private keys need protection against unauthorized disclosure. • Keys must not be stored on the same storage media as the encrypted data. • Equipment used to generate, store and archive keys must be physically protected.
Key Recovery	To prevent data loss, establish processes to ensure Keys can be recovered if they are forgotten.	• Strategies must be implemented to enable Key recovery. • UBC's central Key Escrow service is recommended for this purpose because it is reliable and secure. See the Key Escrow guideline for more information. • Alternatively, the Key may be recorded on a piece of paper and locked in a secure location such as a safe. • The recovery process must be documented to assure it will be effective when required.
Key Change	Revoke and publish new keys when they are suspected of compromise or unauthorized disclosure, they reach the end of their lifetime, and/or the key owner or delegated individual leaves the employ of UBC.	• Key lifespan must be documented along with processes and rules for making changes to keys. • Clear authorization process for key changes. • Specific responses to suspected compromised keys.

Additional Requirements for Merchant Systems

12. Users must not store authentication data collected in Merchant Systems after authorization (even if this data is encrypted); authentication data includes:
    a. the full contents of any track from the magnetic stripe or chip;
    b. the card-verification code or value (three or four-digit number printed on the back/front of a payment card); and
    c. the personal identifier number (PIN) or the encrypted PIN block.
13. Users must ensure that the credit card number is masked (the first six and last four digits are the maximum that can be displayed) whenever displayed (e.g. electronically, hard-copy, etc.).

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems
Encryption Requirements standard
Password and Passphrase Protection standard
Reporting Information Security Incidents standard
Key Escrow guideline

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #17
Logging and Monitoring of UBC Systems

Introduction

1. Effective logging and monitoring procedures (i.e. continual monitoring and/or periodic reviews) provide ongoing assurance that UBC Systems and the UBC Electronic Information, which they hold, are secure and that confidentiality and integrity are effectively being ensured. In the event of a security breach, audit logs are relied upon to determine whether or not information has been accessed or modified without authority.
2. The nature and frequency of logging and monitoring procedures must be based upon the sensitivity of the information stored in the system and the potential impact of a security breach upon the University and affected individuals. It is only necessary to implement logging and monitoring at a level that will reasonably identify unauthorized access to UBC Systems and UBC Electronic Information in a timely manner. Logging and monitoring should be considered at the operating system, database and/or application level.
3. This standard defines requirements for effective logging and monitoring of UBC systems and UBC Electronic Information for security purposes. Unless otherwise stated in this document, University IT Support Staff are responsible for ensuring compliance with these standards. In addition, Information Stewards/Owners are responsible for ensuring that logging and monitoring procedures are adequate for securing the information they are responsible for. Core Systems, Merchant Systems and EMRs must be compliant with this standard; it is recommended that all other UBC Systems comply with this standard.
4. 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.

Logging and Monitoring Requirements

5. The following key activities must be logged:
    a. User login, logout and access to a resource;
    b. action performed by the User and the time it was performed; and
    c. where feasible, any access to, or modification of, records.
6. Logs should be configured to record system faults that are potential indicators for detecting attacks against UBC Systems or other unauthorized activity.
7. Logs provide valuable information that can be used to validate the integrity and confidentiality of UBC Electronic Information; to be effective, logs must be:
    a. retained for at least 90 days and regularly backed up whenever possible, preferably to offsite secure storage;
    b. retrievable in a timely manner if they are required for analysis; and
    c. protected against unauthorized access and modification, preferably by locating them on a separate server outside the Demilitarized Zone (DMZ), such as a Database Server protected by a firewall, and restricting access as necessary; no-one should be able to change or delete log information.
8. Logs should be monitored to determine the use of system resources and to detect information security events (e.g. failed logons, simultaneous logins from different geographic locations, escalation of privilege, attacks against systems, etc.). Monitoring software should be configured to send an alert to responsible University IT Support Staff when appropriate.
9. Accurate logs are dependent on accurate time. Systems containing or processing Confidential Information must be set to synchronize their clocks with a reliable source. UBC's DNS servers act as the University's (Time synchronization) NTP servers. These are synchronized to an external time source, ntp.org; all Users and University IT Support Staff should use these or an equivalent service as a time synchronization source. More details on this service can be found on the myDNS Overview page.

Additional Requirements for Privileged Accounts

10. University IT Support Staff must ensure that logs are kept of the usage of all Privileged Accounts. Key activity to be logged must include the following:
    a. login, logout and the identity of the User, if known;
    b. action performed and the time it was performed;
    c. where feasible, any access to, or modification of, UBC Electronic Information; and
    d. any other information that the Information Stewards/Owners decide should be captured in order to protect high risk files.
11. Logs of Privileged Account activity must be reviewed on a regular basis to detect information security events and determine if further investigation is required; where feasible this should be automated. Investigations should be reported to the Information Steward/Owner as required.
12. Where appropriate, Privileged Account logging systems must automatically transmit alerts of significant activities to the technology owner (typically a manager of a University IT Support Staff team). The following activities must always trigger an alert:
    a. escalation of privilege; and/or
    b. usage of the Break Glass Procedure as described in the Privileged Account Management standard.

Additional Requirements for Merchant Systems

13. For all Merchant Systems processing PCI Information, there is a requirement that logs be maintained for the following events:
    a. which particular record was accessed;
    b. which User accessed the record; and
    c. the time the User accessed the record.
14. Logs of access to PCI Information should be retained for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).

Use and Disclosure of Logs

15. Logs are generally intended to be used for maintenance and troubleshooting, as well as detecting and investigating information security events. Access for other purposes must be approved using one of the following methods:
    a. internally, within UBC, in accordance with the Accessing Electronic Accounts and Records standard;
    b. externally to law enforcement via Campus Security; or
    c. externally to other entities via authorization from the Office of the University Counsel.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Accessing Electronic Accounts and Records standard

Privileged Account Management standard

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #18
Physical Security of UBC Datacentres

Introduction

1. Effective security measures require physical security controls. While electronic controls alone are important, they may become useless if the device is physically accessed or removed by an unauthorized party.
2. This document defines standards for the physical security of UBC Datacentres. These Datacentres are intended to provide a secure location for operations, controlled access to equipment and data, protection against environmental threats, and support for the availability requirements of UBC Electronic Information and Systems. University IT Support Staff are responsible for ensuring that the requirements of this document are complied with.
3. The University has a responsibility to protect Confidential Information from unauthorized viewing and use. In particular, the *Freedom of Information and Protection of Privacy Act* (FIPPA))[1] and Records Management Policy[2] require public bodies to implement reasonable and appropriate security arrangements for the protection of Personal Information (in both electronic and paper format). Therefore, servers containing significant quantities of Confidential Information must be hosted in UBC Datacentres, which provide the highest level of security. Sensitive and Public Information may also be hosted in UBC Datacentres where appropriate.
4. 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.

Physical Security Controls

5. The table below outlines the minimum set of physical security controls required for UBC Datacentres, based upon the Security Classification of UBC Electronic Information standard.

Control Area	Information Security Classification		
	Confidential	Sensitive	Public
Rooms	Datacentre must be located in a fully enclosed room. Walls must meet the following criteria: • Must extend from floor to ceiling slab. • Should preferably be constructed from a solid, resistant material such as concrete or brick. If they are not solid (e.g. drywall), then they must be reinforced with wire mesh.		Equipment can be located in open areas if other protective measures are in place, e.g. locked cages.
Doors and Locks	• Datacentre doors must be locked when room is not in use. • Good practice is to install automatic closing mechanisms. • Security grade door fastening hardware must be used in conjunction with a metal door and frame. • Acceptable locking mechanisms include electronic proximity access cards/fobs, keypad type entry locks, and biometric locks.		Datacentre doors must be locked when room is not in use. Either electronic or mechanical locks are acceptable.

[1] FIPPA, section 30
[2] Policy 117, section 2.4

Control Area	Information Security Classification		
	Confidential	**Sensitive**	**Public**
Glazing	All exterior glass in doors and accessible windows must be reinforced. Consider installing high grade security film (minimum standard should be Profilon AXA1-15Mil or equivalent) to resist forced entry.		Windows must be able to securely lock from the inside.
Visibility of Equipment	Window coverings (blinds/shades) or reflective/tinted film should be installed on glazed windows or doors in order to reduce direct sightlines to valuables inside the facility.		
Cabling	Power and network cabling carrying data or supporting information services should be protected from interception or damage outside of the Datacentre.		
Managing Access	• The public must not have direct access to the Datacentre perimeter. An outer security perimeter should be established with access controls sufficient to prevent direct public access. • Use signage to clearly delineate publicly accessible space from Authorized Personnel-Only areas. Signage should not indicate the presence of UBC Electronic Systems. • Individual(s) must be assigned the authority to grant access to the Datacentre and someone must be appointed to formally manage the physical access process including revocation of access (fob/card, keypad access). • Individuals who are not authorized to access the Datacentre must be escorted at all times by an authorized individual. • Access must be logged electronically or in a logbook in the case of keypad entry doors that do not uniquely identify an individual.		
Alarms and Remote Monitoring	Alarms (monitored 24/7) must be installed that trigger on unauthorized access.	Good practice is to install and monitor an alarm system to detect intruders.	
	CCTV has been debated as an effective deterrent to crime, but if employed with adequate resolution and proper camera placement, its forensic effectiveness is undisputed. All CCTV installations must be approved by the Access and Privacy Manager.		
Power Supply	• Redundant power should be supplied to the Datacentre where possible. • Servers should all be connected through a UPS in order to remain running in the event of short power outages.		N/A
Environmental Controls	• Sufficient Heating, Ventilation and Air Conditioning (HVAC) systems must be in place to effectively maintain all UBC Electronic systems within the manufacturers' required temperature and humidity operating ranges. • Measures must be in place to monitor and detect variation in temperature and humidity • Where possible, water and drainage plumbing should not run across the ceiling of a Datacentre. • The floor of the Datacentre should be raised above the subfloor to reduce the risk of flood damage.		Comply with Building Code requirements.
Fire Protection	Fire detection and suppression devices, such as fire		Comply with Building Code

Control Area	Information Security Classification		
	Confidential	Sensitive	Public
	extinguishers and pre-action or dry pipe sprinkler systems, must be in place.		requirements.
Data Backups	If information is backed up onto electronic media, the same physical security requirements are to be applied to that media unless the information is encrypted (see the Encryption Requirements standard).		

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Encryption Requirements standard

Security Classification of UBC Electronic Information standard

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #19
Internet-Facing Systems and Services

Introduction

1. UBC Systems and services that are Internet-facing (i.e. visible or accessible from the Internet) are prime targets for exploitation. Without adequate security, these systems and services provide an avenue for malicious activity such as theft of UBC Electronic Information or the denial of service to UBC resources.
2. This document defines minimum standards to be followed by University IT Support Staff for the security architecture, protected network protocols, hardening/patching and monitoring/logging of UBC's Internet-facing systems and services to ensure they are adequately protected. This standard focusses on Web Servers because these are primary targets for exploitation and therefore pose the highest risk to the University. Servers that are not internet-facing, such as intranet servers, should also follow this standard, wherever feasible.
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.

Security Architecture Requirements

4. Ideally, web, application and database functions should be hosted on separate servers; however, it is acceptable to host all of these functions on the same server in the following circumstances:
    a. Confidential Information is not being processed through these servers; and/or
    b. hosting the functions on separate servers would not be technically feasible or would cause unreasonable business disruption (e.g. render the application unusable or unsupportable).
5. If functions are hosted on the same server, compensating controls must be implemented to commensurate with the risk, such as:
    a. web application (layer 7) firewall;
    b. file integrity monitoring;
    c. Intrusion Detection Systems/Intrusion Prevention Systems; and
    d. log monitoring (e.g. SIEM).
6. When web, application and database functions are hosted on separate servers, Web Servers are permitted to communicate with Application Servers but not with Database Servers.
7. All Internet-facing servers must be placed in a Demilitarized Zone (DMZ) configured as follows:
    a. the DMZ must contain all Web Servers;
    b. the DMZ may only contain Application Servers if they are combined with Web Servers;
    c. the DMZ must not contain Database Servers that store or process Confidential Information;
    d. a firewall must be in place between the DMZ and the Internet as well as between the DMZ and the UBC internal network;
    e. wherever possible the DMZ should be protected from the Internet by web application firewalls, as they are better equipped to protect web applications from threats;
    f. firewalls must use ingress filtering at a minimum, and must also use egress filtering if the firewall is used to protect Confidential Information; and
    g. firewalls must use access rules that restrict traffic to only the minimum necessary to conduct University Business; access rules must not be wide-open allowing any source to connect to any destination, as this defeats the security of the firewall.
8. Access to all Confidential and Sensitive Information on servers must be authorized and limited based on the User's role, following the principle of least privilege.

Network Protocol Requirements for Confidential or Sensitive Information

9. Secure transmission of Confidential or Sensitive Information must comply with the following requirements:

a. any form, application or service that requires some type of authentication, or that is used to collect or transmit information from User to server or between servers, must be encrypted using HTTPS with TLS version 1.0 at a minimum, TLS version 1.1 is preferred (or the equivalent, for non-web-based applications; and
b. information transmitted via SSH must be encrypted using a minimum of AES-256 bit encryption with mutual authentication between the server and User.

10. Users frequently access desktops, laptops and servers remotely. Remote access covers a broad range of technologies, protocols and solutions (e.g. RDP, SSH, VNC, VDI, terminal services, etc.). Remote access transmissions must comply with the following requirements:
    a. remote access servers (e.g. terminal server, VDI, Remote Access Gateways, etc.) must be located in the DMZ and use strong encryption for server-to-User transmissions, e.g. RDP with Network Level Authentication, SSH with AES-256 bit encryption, etc.;
    b. host desktops, laptops or servers not located in the DMZ should only be remotely accessed via a Remote Access Gateway, VPN or SSH; and
    c. VPN connections must be encrypted and restricted at both ends to the minimum number of systems necessary; split tunneling must not be enabled.
11. Servers running other internet-facing protocols (e.g. Telnet, FTP, etc.) must be located in the DMZ and must encrypt transmissions of Confidential or Sensitive Information.

Additional Requirements for Merchant Systems

12. University IT Support staff must configure remote access technologies, used in Merchant Systems, to automatically disconnect User sessions after a specific period of inactivity. 30 minutes is recommended.

Hardening and Patching Requirements

13. Servers must be hardened, patched and scanned in accordance with the Vulnerability Management standard.

Logging and Monitoring Requirements

14. Servers must be logged and monitored in accordance with the Logging and Monitoring of UBC Systems standard.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Logging and Monitoring of UBC Systems standard

Vulnerability Management standard

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #20
Development and Modification of Software Applications

Introduction

1. A Software Application is a piece of software designed to perform a task for end users, such as accounting, human resource management, and student information management. When purchasing, designing or substantially modifying these Applications, it is important that security requirements are understood, documented and implemented at the earliest appropriate stage of the project. This is substantially cheaper and more effective than trying to apply security controls retroactively.
2. Information Stewards/Owners are responsible for ensuring this standard is complied with whether the project is undertaken internally or by a Service Provider.
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.

Assessing Security Requirements for Projects Involving Confidential Information

4. All new or substantially modified Applications that store or access Confidential Information must undergo a Security Risk Assessment of the new Application's security controls, using the Software Application Security Risk Assessment checklist.

Examples of "Substantially Modified":

- granting access privileges to Confidential Information to new categories or groups of individuals
- outsourcing management, storage or security of Confidential Information to an external service provider
- changing how Confidential Information is collected, used or displayed

Assessing Privacy Requirement for Projects Involving Personal Information

5. In addition to the requirement to undergo a Security Risk Assessment, all new or substantially modified Applications that store or access Personal Information must undergo a privacy impact assessment (PIA), as set out in the Privacy Impact Assessment Requirements.

Pre-Production Development and Test Environments

6. Development and test environments must be logically and/or physically isolated from any production environments.
7. Where possible, testing of new Applications should be done with fabricated data that mimics the characteristics of the real data, or on copies of real data with any Confidential or Sensitive Information appropriately sanitized. Testing should not be done on live data due to the threat to its confidentiality and/or integrity. Testing that requires the use of live data or Confidential Information must have appropriate security controls employed.

Application Development Requirements

8. Applications must validate input properly and restrictively, allowing only those types of input that are known to be correct (e.g. cross-site scripting, buffer overflow errors, SQL injection flaws, etc.).
9. Applications must execute proper error handling so that errors will not provide detailed system information, deny service, impair security mechanisms, or crash the system. See the Open Web Application Security Project for more information.
10. Where possible, code-level security reviews must be conducted with professionally trained peers for all new or significantly modified Applications, particularly, those that affect the collection, use, and/or display of Confidential Information.
11. All new or substantially modified Applications connected to the UBC network must be scanned for vulnerabilities in accordance with the Vulnerability Management standard.

Change Management

12. A change management process must be implemented and maintained for changes to existing Applications; substantial modifications may trigger a new assessment of security and privacy risks, as explained above.

System Documentation

13. University IT Support Staff must securely store system documentation and ensure that it is only available to authorized Users.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Vulnerability Management standard

Software Applications Security Risk Assessment checklist

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #21
Requesting Variances from Information Security Standards

Introduction

1. In order to protect University information assets, the Chief Information Officer (CIO) has issued binding Information Security Standards. Academic and administrative units that wish to deviate from these Information Security Standards are required to request a variance from the CIO.
2. This document establishes the procedure for Administrative Heads of Unit to request such a variance.
3. The CIO 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.

Variance Request Procedure

4. Initial Request - the Administrative Head of Unit must submit the following information to information.security@ubc.ca:
    a. contact information;
    b. description of the requested variance and expected duration;
    c. explanation of why the variance is warranted;
    d. analysis of risk associated with granting the variance, and what controls will be in place to manage this risk; and
    e. analysis of cost and resource implications of granting the variance.
5. When considering the request for a variance, the CIO may seek the input of the Information Security Governance Committee (which is the Advisory Committee defined in Policy 104) if he or she considers this appropriate.
6. The CIO may authorize a variance from the Information Security Standards in any of the following circumstances:
    a. the Administrative Head of Unit is temporarily unable to meet the compliance standard;
    b. compliance is not achievable for technical or financial reasons;
    c. an alternate method of compliance is available that offers equivalent or better security; or
    d. the variance is otherwise reasonable and is consistent with the Information Security Standards.
7. If the CIO approves a deviation, he or she will set out the terms of the variance, including any applicable mitigation requirements or other conditions.
8. If the CIO denies the requested deviation, he or she will provide an explanation and, if possible, a suggestion of alternatives.

Resolution of Disagreements

9. If a disagreement arises and cannot be resolved in a timely manner between the CIO and the Administrative Head of Unit with respect to the requested deviation, then either party may refer the disagreement to the Responsible Executive specified under Policy 104, who will decide the matter. This Responsible Executive may consult with the Information Security Governance Committee and/or the other Responsible Executive if he or she determines it would be appropriate to do so.
10. The Responsible Executive's decision is final.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems