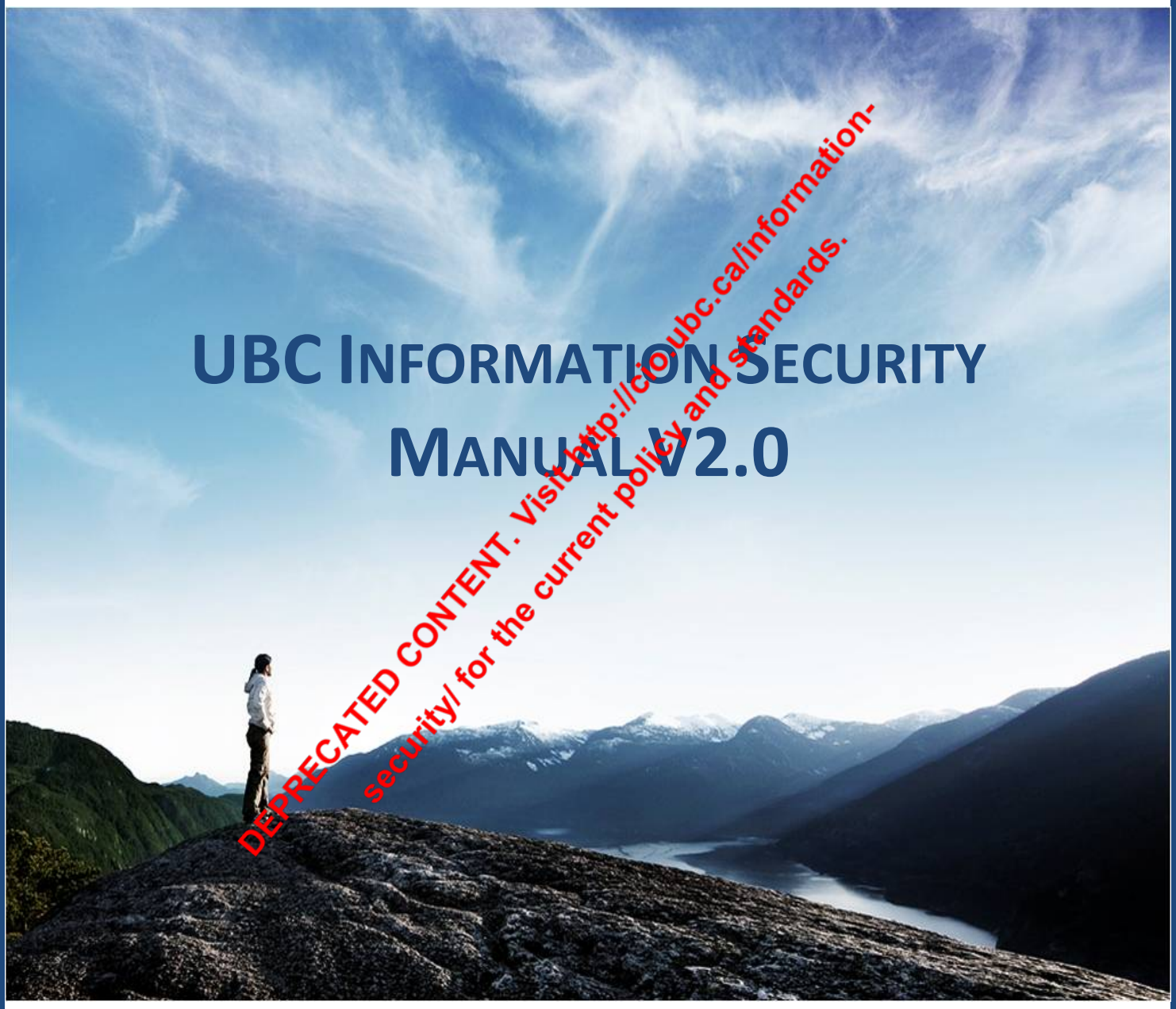
a place of mind

THE UNIVERSITY OF BRITISH COLUMBIA



UBC INFORMATION SECURITY MANUAL V2.0

Approved: June 2010
Revised: March 2012

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

UBC Information Security Manual

Table of Contents

Introduction

The UBC Information Security Manual provides guidance, in the form of institutional standards, on relevant information security best practices, as well as applicable regulatory compliance issues. This manual is designed to be a living document and, as such, it will be regularly updated to reflect the changing information technology environment of the University of British Columbia. It is expected that all personnel working with administrative, academic or research systems and/or data on behalf of the university will adhere to this manual. This manual is created under the authority of UBC Policy #106 "Access to and Security of Administrative Information".

The ultimate backbone of higher education is information: the university gathers, stores, analyses, retrieves and secures the information necessary for the proper functioning of all aspects of our mission. Without continued and uninterrupted access to that information, as well as assurances that the information is secure and reliable, we would be unable to fulfill our educational, research and service objectives.

Protecting our information, against the backdrop of this institutional mandate, are the various laws, regulations, contractual requirements, security policies, procedures, standards and controls, which are part of the fabric of every institution. As part of our risk management efforts these compliance objectives act as controls that help enhance our university's reputation and minimise risk and other negative consequences, by ensuring compliance with the legal requirements and university policies.

The University strongly values intellectual property. This manual is not intended to limit the academic freedom or the intellectual property interests of University employees and faculty members.

1 Asset Management

Overview

An asset is defined as "anything that has value to the organisation" (source: International Organization for Standardization 27000). Asset management is based on the idea that it is important to identify, track, classify and assign ownership, for the most important assets, to ensure they are adequately protected. Tracking inventory of some kind is the simplest example of asset management. Knowing what we have, where it lives, how important it is and who's responsible for it are all important pieces of the puzzle. Similarly, an Information Asset is a collection of data needed to conduct University business (administrative, academic or research). The same concepts of general asset management apply to the management of information assets. To be effective, an overall asset management approach should include information assets, software assets and information technology equipment. In addition, the people employed by the university, as well as the university's reputation, are also important assets not to be overlooked in our asset management objectives.

Important elements to consider are:

- Asset responsibility/ownership (do we know who is responsible for each asset?)
- Asset inventory (do we know what assets we have & where they are?)
- Asset classification (do we know how important each asset is in relation to other assets?)
- Asset protection (is each asset adequately protected according to how important it is?)

1.1 Responsibility for Assets

Objective: *To ensure adequate protection of University resources, all information assets should be accounted for and each asset should have a designated responsible party.*

Inventory of Assets

1.1.1 As part of the information asset inventory, which includes administrative, academic and research assets, the University should have a good understanding of what personal information exists on University systems and where those assets are located.

Guidance 1.1.1: The University needs to maintain an information asset inventory in order to better understand what information it has in its custody and how it is being protected. With an inventory of information assets that is properly maintained the University will be better empowered to identify and assist with systemic risks throughout the University; however, the only way to know about such systemic issues is to create an asset inventory. Directions for creating and maintaining the information asset inventory will be provided by the Information Security Office. While information assets comprise both hard copy and electronic data, the University will commence with an inventory of electronic assets, as an initial phase, because electronic data has a higher risk of exposure to multiple parties than hard copy assets.

While information may consist of many different types of data, personal information has a mandatory requirement for effective protection under B.C. legislation and as such, at a minimum, the University should understand what personal information exists on University systems and where they are physically stored within Canada.

Note: This does not refer to "Records Management", which is covered under UBC Policy 117; the information asset inventory covers the security and protection of records; specifically, maintaining the confidentiality, availability and integrity of those records.

Ownership of Assets

1.1.2 Unit heads are responsible for declaring the functional stewards/owners of information assets within each of their units; these are the functional person(s) responsible for determining how the data in an asset is used and who can access the data.

Guidance 1.1.2: Information assets contain information that is valuable to the University. This varies from unit to unit and can include intellectual property, information protected under legislation/regulation and information needed for the University to conduct its mission activities, to name just a few of the types of information that exist. In all cases it is important to have a clear understanding of who is responsible for the management and protection of that information. All functional stewards/owners should self-identify information assets they are responsible for to the head of their unit or the head's designate; any undeclared information assets will have a functional steward/owner identified by the unit head.

While all administrative data is owned by the University, a functional steward/owner should be identified for each information asset regardless of whether it is used for administrative, academic or

research purposes. The functional steward/owner may consist of one or more persons, as is identified for each asset, where the functional steward/owner consists of the person(s) who determines:

a) How the data in an asset is used and;

b) Who is authorised to access the data.

Acceptable Use of Assets

1.1.3 Acceptable use of assets is covered in UBC Policy 104 Sections 1.2, 1.3, 1.6, 2.3 and 7.1.

Guidance 1.1.3: Specifically assets shall be used in a manner that is consistent with the intended purpose for which it was provisioned. i.e. a student computer lab used for teaching and learning shall be used in a manner consistent with its intended purpose; likewise research computing lab facilities shall be used in a manner that is consistent with the intended research activities of the lab.

Users must not misrepresent their identity as senders of messages. Spoofing email or phone systems to send messages, using an identity other than your own, is prohibited.

The list of unacceptable uses, identified in section 7.1 of UBC Policy 104, is not meant to be an exhaustive list; it is provided in order to facilitate a better understanding of what is unacceptable to the University.

1.2 Information Security Classification

Objective: *To appropriately protect various kinds of information, an information security classification scheme is required that states the relative importance of each type of information to the University, as well as an appropriate level and method of protection for each one.*

1.2.1 The Information Security Office must communicate the UBC information security classification schedule to all Departments.

UBC Information Security Classification Schedule

	Confidential ***Highest level of sensitivity***	**Sensitive** ***Moderate level of sensitivity***	**Public** ***Very low, but still requiring some protection***
Legal Requirements	Protection of data where it is required by law (e.g. Freedom of Information and Protection of Privacy Act [FIPPA] legislation, which includes Personally Identifiable Information [PII] and Protected Health Information [PHI]) or by industry regulation (e.g. Payment Card Industry – Data Security Standard [PCI-DSS] for protection of credit card data) or by University of British Columbia policy	The institution has a contractual obligation to protect the data (e.g. Bibliographic citation data, bulk licensed software)	None
Reputation Risk	High	Medium	Low
Other Institutional Risks	Information that facilitates/provides access to resources/infrastructure, physical or virtual	Smaller subsets of Confidential data from a Faculty, large part of a Faculty, or Department	Data that is generally available to the public
Potential Impact of Loss	• Long-term loss of research funding from granting agencies • Long-term loss of reputation • Legal costs • Individuals put at risk for identity theft • Unauthorized tampering of research data • Increased regulatory requirements • Long-term loss of critical campus or departmental service	• Short-term loss of reputation • Short-term loss of research funding • Short-term loss of critical departmental service • Unauthorized tampering of research data • Individuals put at risk for identity theft	• Loss of use of individual workstation or laptop • Public embarrassment

Guidance 1.2.1: To appropriately classify information assets, identify the highest sensitivity classification (Confidential, Sensitive or Public) of any single data point within that asset. That highest point determines the appropriate level of classification for all data in that asset. If there is ambiguity as to what information is contained within the asset and a definitive classification of the information cannot be made, then the information asset must be classified as Confidential until such time that it can be definitively identified as a lower level of classification.
Once classified, apply the appropriate handling controls from the Information Security Handling Schedule. If an information asset that is classified as Sensitive or Confidential eventually becomes released to the public then it may be reasonable to declassify it to Public.

Examples 1.2.1: include but are not limited to

	Confidential	Sensitive	Public

Data Examples	• Personally Identifiable Information (PII) (protected under FIPPA)
	  • Student or Prospective Student
	  • Name
	  • Student ID number
	  • Email address, if it can identify an individual
	  • User account name, if it can identify an individual. E.g. CWL ID
	  • Courses taken if linked to the identity of an individual
	  • Enrolment status of a student. E.g. we cannot inform a student's parents/guardians if the student is enrolled at UBC, unless we have the written consent of the student
	  • Employee incl. faculty, staff & volunteers
	  • Office email (not the email address)
	  • Office network/home drive, which is used solely by the employee
	  • Home: address, phone, cell & email, if it can identify an individual
	  • Dependents
	  • Emergency contact details
	  • Donor or Prospect
	  • Name
	  • Contact details
	• Protected Health Information (PHI): Patient/medical/health including Electronic Medical Records
	  • Name
	  • Patient ID number
	  • HealthCare number
	  • Address, phone, email
	  • Emergency contact details
	  • Personally identifiable patient data
	  • Human subject
	  • Name
	  • Contact details
	• Credit card numbers (PAN data)
	• Financial
	• Contracts
	• Certain management information
	• Physical plant detail
		• Research data that does not contain confidential data and has not been released publically
		• Anonymised or de-identified human subject data (e.g. health/medical or human subject study information) used in research
		• Library journals
		• Library transactions (e.g. catalogue, circulation, acquisitions) and Journals
		• Information resources with access to Confidential data
		• Directory service systems used, to authenticate users, for access to confidential data, which do not contain confidential data itself. E.g. an Active Directory or LDAP, which contains no student names or any other confidential information, and is used to access a student system containing confidential information
		• Any information that is not confidential and is not generally made available to the public
		• Financial transactions that do not include Confidential data (e.g. telephone billing)
		• Very small subsets of Confidential data
			• Employee
			  • Name
			  • Work: address, phone, cell & email
			  • Title
			  • Salary
			• Campus Maps
			• Processed anonymous data
			• Census data
			• Anonymised statistical information about the University. E.g. UBC PAIR data that is published publically

1.2.2 The Information Security Office must communicate the UBC information security handling schedule to all Departments.

UBC Information Security Handling Schedule

	Confidential ***Highest level of sensitivity***	**Sensitive** ***Moderate level of sensitivity***	**Public** ***Very low, but still requiring some protection***
Access Protocol	Access is limited to those personnel permitted under law, regulation and University of British Columbia policies, and those with a need to know.	Access limited to those personnel with a need to know.	Open
Transmission	• It is strongly recommended that Confidential information transmitted through a network should use approved encryption. • Third party email services are not appropriate for transmitting Confidential information. • Confidential data may be masked instead of encrypted.	• Approved encryption is recommended when transmitting information through a network. • Third party email services are discouraged for transmitting Sensitive information.	Open
Storage	• Location of Confidential information should be clearly identified and reported via the Prioritisation Tool. • Approved encryption or masking is strongly recommended and may be required on computing equipment depending upon law or regulation.	• Approved encryption of Sensitive information is recommended. • Level of required protection of Sensitive information is either pursuant to UBC policy or at the discretion of the owner or custodian of the information. If appropriate level of protection is not known, check before storing Sensitive information unencrypted.	Encryption is not required.
Protection Controls	In accordance with law, regulation and University of British Columbia policies, procedures & standards.	In accordance with University of British Columbia policies, procedures & standards.	In accordance with University of British Columbia policies, procedures & standards.

Access Protocol 1.2.2: Defines how access to the information is approved.

- Confidential data is limited to those personnel who are permitted under the FIPPA, PCI-DSS or any other applicable law or regulation, as well as those permitted under UBC policy, in addition to personnel with a need to know. E.g. personnel who need to access confidential research data in order to conduct their research would be granted access to it; whereas other personnel who do not have a need know would not be granted access.

- Access to confidential data should be granted using role based access control models where permissions are set on a per role basis and individuals are assigned to a role that carries access permissions such as read, write, modify, etc. Permissions should be set following the principle of least privilege. e.g. if a role does not need administrative access to the data and only needs to view it, then that role should only be granted read or view access.
- Sensitive data is limited to those personnel with a need to know in order to carry out their operational duties for the University.
- Public data is open to everyone and requires no control around access to the information.

Transmission 1.2.2: Describes how information should be transmitted.

- Encryption is recommended in situations where confidentiality of information is required, in order to mitigate eavesdropping by unauthorised individuals.
- Confidential information:
    - It is strongly recommended that Confidential information transmitted via the web should be encrypted using HTTPS with TLS version 1.0 at a minimum, TLS version 1.1 is preferred;
    - It is strongly recommended that Confidential information transmitted via SSH should be encrypted using AES-256 bit encryption with mutual authentication between the server and user.
    - If data masking is used effectively on Confidential information, prior to transmission, then encryption may not be required.
    - Third party email services are not appropriate for the transmission or storage of Confidential information; **Confidential information must be stored in Canada** and only in UBC owned or authorised environments. Specifically, email accounts used by University personnel, handling Confidential information, must not be on third party services such as Gmail, Hotmail, Yahoo, etc.
- Sensitive information:
    - It is recommended that Sensitive information should be encrypted using TLS version 1.0 at a minimum, TLS version 1.1 is preferred;
    - Sensitive information transmitted via SSH should be encrypted using AES-256 bit encryption with mutual authentication between the server and user.
    - The University discourages the use of third party email services in the transmission of sensitive information.
- Public information is open and does not require encryption or data masking
- TLS certificates may be purchased under the University's Enterprise account, via the Information Security Office, by contacting security@ubc.ca.

Storage 1.2.2: Identifies recommended storage practices for information in order to secure data at rest.

- Encryption is recommended in situations where theft of data (both physical & electronic) may result in data exposure to unauthorised individuals. Provided strong encryption is used and the keys are effectively managed separately from the data, then the risk of unauthorised disclosure is greatly reduced.
- It is strongly recommended that Confidential information should be stored encrypted using a minimum of AES-256 bit encryption.
    - Information stored in a database should use the vendor's database-level encryption functionality, at minimum, preferably Transparent Data Encryption (TDE), which forms a strong encryption level for information in the database.

  - If data masking is used effectively on Confidential information, prior to storage, then encryption may not be required.
  - The physical location of where Confidential information is stored should be identified in the UBC Information Security Prioritisation Tool.
- It is recommended that Sensitive information be encrypted following the same standards as Confidential information.
- **Data Destruction:** When information is no longer required it should be cleansed (deleted, sanitised or destroyed). Media that has been used to store university information must be cleansed of information prior to decommissioning following the standards below. Information stored with a hosted vendor must be cleansed once it is no longer needed – typically at the end of the contract. Information no longer required to be stored under regulatory, legal or contractual requirements and also not needed for University operations must also be cleansed.
  - Confidential Information must be sanitised using secure methods that reasonably limit the ability of an unauthorised person from recovering the information. Acceptable methods are described here by the RCMP and CSEC for the Canadian Government; any of the following methods are considered acceptable for the sanitisation of Confidential information at UBC:
    - CSEC ITSG-06
    - RCMP TSSIT OPS-II
    - DoD 5220.22-M
    - Center for Magnetic Recording Research (CMRR) "Secure Erase"
    - Vendors, delivering a hosted solution, which manages Confidential information on behalf of UBC, must have data destruction terms written into the contract. Clauses are available from the Information Security Office website on the Policies page.
  - Sensitive information should be sanitised following the same standards applied to Confidential information.
  - Public information has no information sanitisation requirements.

Protection Controls 1.2.2: In general terms these are described in applicable legislation (FIPPA), regulations (PCI-DSS) and policies of the University.

- Public data only requires sufficient protection controls in order to protect the integrity of the information; this safeguards the institution from having unauthorised individuals changing public information to something other than what was intended.

2 Human Resources Security

Overview

Employees who handle personal information in the university need to receive appropriate awareness training and regular updates in an effort to safeguard the information entrusted to them. Appropriate roles and responsibilities assigned for each job description need to be defined and documented in alignment with the university's security policies, procedures and standards. The institution's data must be protected from unauthorised access, disclosure, modification, destruction or interference. The management of human resources security and privacy risks is necessary during all phases of employment association with the university. Training to enhance awareness is intended to educate individuals to prevent data disclosure, recognize information security problems and incidents, and respond according to the needs of their work role.

Safeguards depending upon roles may include the following:

- Job descriptions and screening,
- User awareness and training,
- A disciplinary process, and
- An orderly exit process must exist to equip employees to operate securely and use information appropriately, and ensure that access privileges change when a user's relationship with the university changes.

The objective of Human Resources Security is to ensure that all employees (including contractors and any user of confidential or sensitive data) are qualified for and understand their roles and responsibilities of their job duties and that access is removed once employment is terminated. While there are three areas of Human Resources Security, the current focus is on:

- **During Employment:** Employees with access to confidential or sensitive information in the university should receive periodic reminders of their responsibilities and receive ongoing, updated security awareness training, to ensure their understanding of current threats and corresponding security procedures to mitigate such threats.

2.1 During Employment

Objective: *To ensure that employees are aware of and understand their roles and responsibilities; to ensure that they understand information security threats and; to ensure they have the necessary knowledge to mitigate those threats.*

2.1.1 The Information Security Office must make information security awareness, education and training available to employees via the University Learning Management System.

Guidance 2.1.1: The University, via the Information Security Office, must make information security awareness training and education, available to all employees of the University, as well as to all graduate students. This will be done via the university's official Learning Management System. The training must be appropriate for the general culture of the University and is recommended for employees and graduate students.

3 Communications and Operations Management

Overview

To be effective in reducing security risks and ensuring correct computing operations, a security programme needs to include operational procedures, controls and well-defined responsibilities. Additional formal policies, procedures and standards are needed to protect the exchange of data and information through any type of communication media or technology. Operational and communication exchange procedures and controls address:

- **Protection Against Malicious and Mobile Code** such as computer viruses, network worms, Trojan horses and logic bombs. System managers are responsible for implementing controls to prevent, detect and remove malicious code. Procedures need to be created to make aware of and train personnel on the dangers of malicious code.

- System **Back-up** procedures and policy and its timely restoration in case of a disaster or media failure.

3.1 Protection Against Malicious and Mobile Code

Objective: *To protect the confidentiality, integrity, and availability of University information technology resources and data.*

3.1.1 University IT personnel should ensure that administrative, academic and research systems run up-to-date anti-virus to protect against malware and vulnerabilities.

Guidance 3.1.1: Viruses can drop payloads that include Trojans, key-loggers and root-kits, which can be used to steal credentials that are needed to access confidential and sensitive information, potentially resulting in a data breach. University servers and workstations (incl. laptops) should run anti-virus/anti-malware that is updated on a daily basis. New threats emerge daily that can impact the operations of the University, as a result it is critical that updated definitions/signatures for viruses and other malicious software be installed as soon as they are made available by the vendor. UBC has licensed Sophos Anti-Virus for all University owned systems, as well as for home systems of employees and students.

There may be instances where systems used to conduct certain types of activities, typically research, cannot be protected by anti-virus that is updated daily due to potential impact on long-term computational processes (e.g. a two week statistical analysis of data, a simulation that takes days/weeks to setup, etc.). In these cases it is important to look at compensating controls, which will protect the system and reduce the risk of unauthorised access to data 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 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.

3.1.2 University IT personnel should ensure that all email servers are protected against phishing/spam/malware.

Guidance 3.1.2: All University email servers should be protected against phishing/spam and malware. While spam is generally considered the most prevalent problem it is in fact an annoyance that clutters up mailboxes; whereas phishing on the other hand, is very dangerous. Phishing can be used to steal usernames and passwords to access University information without authorisation. The University has licensed Sophos PureMessage for the protection of UBC email servers.

3.2 Back-up

Objective: *To ensure the integrity and availability of information processed and stored within information processing facilities.*

3.2.1 University IT personnel should ensure that backups of Personal Information are secured via password protection and encryption.

Guidance 3.2.1: Any personal information that is protected under FIPPA should be regularly backed-up; if the back-ups are portable (tape, DVD, portable hard drive, USB stick, etc.) then they should be secured using password protection and encryption. In the event that the backups are lost or stolen, properly encrypted and protected backups present minimal risk of unauthorised data exposure. Encryption strength should be at a minimum AES-256 bit or equivalent. It is recommended that backups should be performed daily.

3.2.2 University IT personnel should ensure that test restores of data from backup media are performed periodically to ensure data remains available

Guidance 3.2.2: Test restores of backups should be done a periodic basis, typically quarterly, to ensure that data can be recovered and that the backups were effective.

4 Access Control

Overview

A basic element of any institution's information security programme is the protection of information resources that support the critical operations of the institution from unauthorised access, modification or disclosure. Access control is the use of administrative, physical or technical security features to manage how users and systems can access or modify university information assets.

In its essence, access is the flow of information between an entity requesting access to a resource or data and the resource. The entity can be a device, process or a user. Access control is any mechanism by which a system grants or revokes the right to access some data or perform some action. Normally, an entity must first login to the resource using some authentication system. Next, the Access Control mechanism controls what operations the entity may or may not make by comparing the credentials provided to an access control list.

Examples of access control:

- When a user is prompted to provide a username and password to be able to access UBC resources (e.g. our Learning Management System).
- Upon logging in, the user attempts to Edit a resource (e.g. a course in the LMS) and the user is denied based on the fact that the individual is not on a list of users that have the right to edit courses in the LMS.
- Since the user was denied access, the user submits a request to be granted the authority to edit the resource. Upon verification that the user teaches the course in question and establishing the business need, the user is added to the list of users that have the right to edit courses.

4.1 User Responsibilities

Objective: *Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.*

Password Use

4.1.1 All accounts used to access administrative systems and directory services must have their password changed at least one (1) time per year.

4.1.2 Passwords cannot be changed to the same password that is currently being used.

4.1.3 If an incorrect password is entered ten (10) times within a thirty (30) minute window then the account must be locked for at least thirty (30) minutes.

4.1.4 Passwords must adhere to the following criteria:

a) Passwords must not contain all or part of the user's account name.

b) Passwords must not be the user's name, address, date of birth, username, nickname, or any term that could easily be guessed by someone who is familiar with that person.

c) Exception - Mobile devices must be:

- ***Protected with a password of at least five characters, unless limited by the device OS***
- ***Configured to lock the screen automatically, after no more than 30 minutes of inactivity, with password protection***
- ***Encrypted via device level encryption, if available***
- ***Configured such that they can be remotely wiped in the event of loss or theft***

Guidance 4.1.4: Passwords are used to authenticate an individual for access to applications, services, systems and data. More generally, passwords are the entry point to University IT resources.

Protecting access to University resources is critical in ensuring that systems remain secure. Users must be diligent in guarding access to those resources and protecting them from threats both inside and outside the organisation.

Mobile devices, by their very nature, are highly portable and can easily be lost or stolen. If these devices store University email that is used for administrative, academic or research purposes, then the device contains personal or confidential information. Under FIPPA we must take steps to protect personal information and since we know that information is being stored and transmitted in email, it is necessary to secure these devices with a password, regardless of whether they are University owned or not, as the data being accessed is University data and UBC is responsible for the effective stewardship of this information under FIPPA.

4.1.5 Responsible use and protection of passwords is covered in UBC Policy 104 Section 1.5.

Guidance 4.1.5: Users must not share the passwords to any accounts that they have access to.

a) Users in a lab should not use a "common" or "shared" account for use of systems in the lab, as this removes all accountability; in the event that an incident were to occur in that lab, it would be very difficult to understand who is responsible for which actions, if all personnel use the same account.

b) A supervisor must not request usernames and passwords for the accounts of members of their unit (common reasons given for this request include: illness, vacation or any unexpected absence). Instead they should look at delegation of authority or access options, where they are

granted access to perform duties that are needed under their own account – this also applies to email where individuals can be delegated access without sharing any passwords.

4.1.6 Passwords are subject to the following guidelines:

a) No passwords must be spoken, written, e-mailed, hinted at, shared, or in any way known to anyone other than the user involved. This includes supervisors and administrative assistants.

b) No passwords must be shared to allow access to systems while an employee is out of the office. Alternative temporary accounts will be established to resolve this if there are resources you need to access while an individual is away.

c) Passwords must not be displayed or concealed within the workspace. E.g. writing passwords on a post-it note and putting it under the keyboard would be unacceptable.

Guidance 4.1.6: Recommended Guidelines on creating secure passwords:

a) Create a passphrase instead of a password; typically these are longer than passwords and provide effective protection, while still remaining easy to remember; this can be done by using a sentence or part of a sentence, a phrase (e.g. "Vancouver is green!").

b) A good way to create a complex short password is by using the first letter of each word in a phrase. E.g. "I ride my bike to school at 7 AM" = Irmbtsa7AM.

c) Something that is no longer considered strong would be "Br0adcast!" where the "O" has been replaced with a zero. This used to be considered safe but hackers now check for dictionary words with numbers replacing common letters.

Privilege Management

4.1.7 Usage of Root, Administrator, SA, Sysman, and other Superuser accounts by University IT personnel is privileged and should follow these practices:

a) The account should be used only when no other alternative exists.

b) The account must not be used as a generic system account to run daemons, services or applications.

c) The password should be machine generated and held in a secured place, available to system administrators in the case of an emergency, at which time the "Break Glass" procedures will apply.

4.1.8 University IT personnel should archive systems logs to offsite storage and be kept for one year.

4.1.9 University IT personnel should ensure that logs facilitate ease of searching and the ability to alert on known or set parameters.

"Break Glass" Procedures

4.1.10 Based on group membership, DBAs, System Administrators and System support staff should be able to access the appropriate passwords/accounts for the database, systems and applications that they support.

4.1.11 Group membership should limit systems access to only the personnel that directly support them; through this process personnel can access the account/password when needed but only the specified personnel.

4.1.12 System administrators should document any actual emergency access to elevated accounts (Root, Administrator, SA, Sysman, and other Superuser accounts) for later audit and review. Typically, a special audit trail is created to monitor such access.

4.1.13 If the password for the account is machine generated, the system should issue a new password once the activity is complete.

4.1.14 Access to elevated accounts/passwords should be:

- **a) Time limited.**
- **b) Associated to a change, problem, or incident number/ticket.**
- **c) Logged in an auditable record.**
- **d) Recorded by the specific database, system, or application and logs should associate the generic Superuser account access/changes with the identifiable user that "broke-the-glass" to receive access to the account.**

5 Information Systems Acquisition, Development and Maintenance

Overview

Security can be incorporated into information systems acquisition, development and maintenance by implementing effective security practices. A key part of those practices is that software needs to be monitored and patched for **technical vulnerabilities**. Procedures for applying patches should include evaluating the patches to determine their appropriateness and whether or not they can be successfully removed in case of a negative impact.

5.1 Technical Vulnerability Management

Objective: *To ensure that procedures are implemented to mitigate and/or patch technical vulnerabilities in systems and applications.*

5.1.1 University IT personnel should patch/update software (operating systems and applications) in a timely (and auditable) manner; software that cannot be patched (embedded instrument systems) should have compensating controls in place to protect them

Guidance 5.1.1: Malicious individuals who wish to have unauthorised access to information or resources frequently will take advantage of unpatched software that can be exploited. In order to mitigate this threat, vendor provided patches for operating systems and applications should be applied in

a timely manner; it is recommended that critical patches (used to address "High" severity vulnerabilities, as classified in CVSS v2) be applied as soon as possible, preferably within days of their release.

Currently there is a strong shift towards mobile devices in higher education, which has also resulted in a shift towards attacking mobile devices. Mobile devices, including tablets and smartphones, should also be kept up-to-date with vendor provided software updates/patches.

Procedures for applying patches should evaluate the patch to determine its criticality, its impact and whether or not it can easily be removed in the event of a serious problem. Backups should be completed before applying any significant patches, in case of unexpected problems.

Embedded instrument systems that run **Windows 95/98/XP/Vista/7 Embedded** OS or any other embedded operating system can only be patched by the vendor of the hardware; as such it is likely that vulnerabilities will exist 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 unauthorised access to data 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 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 for this control.

5.1.2 University IT personnel should complete regular vulnerability assessments on all systems (servers and workstations) that store Personal Information

Guidance 5.1.2: Systems that store personal information should be hardened and kept current on vendor supplied software updates; however, in order to be sure that configuration changes and patches have effectively been applied the systems should have quarterly vulnerability assessments using software such as Nessus, Nexpose, etc.

- A vulnerability assessment will identify any "apparent" vulnerabilities in the system, once those vulnerabilities are identified they need to be investigated to determine whether they are valid or a false-positive.
- **Systems containing personal information should pass four (4) quarterly vulnerability assessments** with no unresolved "High" severity vulnerabilities, as classified in CVSS v2; the assessments must be repeated each year for each quarter. i.e. if there are High vulnerabilities then they either need to be addressed or documented as a false-positive in such a way that an independent 3rd party can verify the findings.
- Vulnerability assessments must not be hampered or blocked by network firewalls or intrusion detection/prevention systems.

Electronic Medical Record systems **must also complete an annual penetration test**, in addition to passing the four (4) quarterly vulnerability assessments each year.

- *The goal of penetration testing is to determine whether unauthorised access to confidential systems and data can be reasonably achieved. If access is achieved, the vulnerability should be rectified and the penetration test repeated until the tester no longer achieves unauthorised access.*
- *Penetration testing may be performed by either qualified internal University IT personnel or a qualified third party. If internal personnel are used to perform penetration testing, then the personnel must be experienced penetration testers; additionally, the penetration testers should be organisationally separate from the personnel managing the security of the system(s) being tested.*
- *The penetration test methodology, the results and any corrective action, taken as a result of the test, should be documented and retained. The documentation and retention provides evidence of policy compliance and of the strategy used for validating the security of the systems being tested.*
- *Penetration testing is not infallible. Although one tester could not gain access using the methods at their disposal, another tester or a malicious attack could still break through a vulnerable system. A successful passing mark on a penetration test is not a guarantee of security; it is an indicator that the system had reasonable security for the tests applied against it.*

6 Information Security Incident Management

Overview

Software complexity, near universal worldwide internet connectivity and the criminals determined to profit from these factors, make information security incidents inevitable. Our information security incident management strategy focuses on driving the impact of the incidents down, while processing incidents as efficiently as possible. Handled effectively, good incident management will also help with the prevention of future incidents.

The university's information security programme includes important aspects of detecting, reporting, and responding to adverse security events, as well as weaknesses which may lead to events, if they are not appropriately addressed.

Effective, appropriate communication at all levels of the university is essential for limiting the impact of security events, using formal detection and reporting processes. In addition, technical controls should be implemented for the automated detection of security events, coupled with as near to real-time reporting as possible, to investigate and initiate immediate responses to problems. For new IT systems, often the best time to develop automated detection of security events is when the preventive security controls are being architected.

Confirmation of an adverse security event is an inevitable outcome in any organisation. A formal management procedure for incident response, including roles and responsibilities for each aspect of the response is essential to the effective management of these events.

6.1 Reporting Information Security Events and Weaknesses

Objective: *To provide clear direction to all University personnel (faculty, staff, students, contractors and volunteers) for handling information security incidents in accordance with the UBC Incident Response Plan located at http://www.it.ubc.ca/security/securitypolicies.html.*

6.1.1 Users are asked to use good judgment when reporting what may appear to be an information security incident, as opposed to a user or other simple system error; however, if the incident appears to be a security issue, please report it immediately, as time is of the essence when dealing with information security breaches and other potentially damaging incidents arising from virus and malware infections.

Guidance 6.1.1: Information security incidents include but are not limited to:

a) Any unexplainable erratic and persistent system behaviour on desktops, servers or the UBC network.

b) Unexplained lock out of user accounts.

c) Any detected attempt at unauthorised access to UBC information assets for any purpose whatsoever.

d) Any identified rogue wireless access points discovered in either merchant areas or areas accessing or holding confidential data; examples include but are not limited to:

- *Areas that contain confidential data regulated under the PCI-DSS in Canada; such as, UBC merchants or UBC's e-commerce payment applications including UBC E-Payment (formerly referred to as the Consolidated Billing Module or CBM).*
- *Areas that contain confidential data regulated under the Freedom of Information and Protection of Privacy Act in British Columbia (FIPPA); these include the Student Information Systems (SIS), the Human Resources Management System (HRMS) and Personal Information (PI) of any kind which includes students, prospective students, employees and patients.*
- *Areas that contain sensitive data that could be damaging to the University if accessed by unauthorized individuals; these include the Financial Management System (FMS) and Intellectual Property (IP).*

e) Any other information technology-related activities that seem to be abnormal.

6.1.2 All UBC employees have a responsibility to report incidents affecting information security in a timely manner as specified in the UBC Incident Response Plan located at http://www.it.ubc.ca/security/securitypolicies.html.

6.1.3 All information security incidents are to be immediately reported to UBC IT via the IT Service Centre (ITSC) at 604-822-2008.

7 Compliance

Overview

The University highly values the information assets used to carry out the mission objectives of the institution, regardless of whether those assets consist of publically available data, intellectual property or highly confidential information. In all cases there may be legislation, regulations, contracts or policies that govern how that data and/or its systems must be handled; whenever this is the case, the University is obligated to be maintain compliance with the relevant laws, regulations, contracts and policies. Functional stewards/owners are responsible for maintaining compliance, on behalf of the institution, wherever required.

In order to maintain effective compliance, system audits must be conducted on a regular basis. There should be controls to safeguard operational systems and audit tools during information systems audits; these controls help to maximise the effectiveness of the audit, while simultaneously minimising interference with the information systems audit process itself. Systems audits need to be conducted with a clear understanding of expectations, with respect to compliance with institutional controls.

Important elements include the following:

- Awareness of relevant regulations/legislation (do you know what you need to follow?)
- Approach to complying with each item (do you know what the University is doing to follow the law?)
- Approach to self-audits (do you know what you can do to assess your level of compliance with institutional policies and legal requirements?)
- Approach to handling audits, whether internal or external, including grant audits (if a granting agency audits you, do you have a set of standards that you're already compliant with, which are established by the University?)

7.1 Compliance with Legal Requirements

Objective: *"Compliance" under this section has a broad meaning over several disciplines. Under this first section the term "Compliance" is about complying with the legal, contractual and records requirements that the University faces to avoid legal or contractual breaches and is specifically limited to the security of electronic information.*

7.1.1 Compliance with legal requirements is covered in UBC Policy 104 Sections 1.8, 4.1 and 5.1.

Identification of Applicable Legislation

The following legislative and regulatory compliance areas do not form an exhaustive list of all applicable legislation to the University

FIPPA Compliance

7.1.2 All users, who handle personal information, are required to maintain compliance with the B.C. Freedom of Information and Protection of Privacy Act; this is covered in UBC Policy 104 Section 1.8.

Guidance 7.1.2: under the UBC Information Security Classification (Section 1.2.1 of this manual) several examples are provided for what is personal information.

PCI-DSS Compliance

7.1.3 The University conducts a large number of payment card transactions on an ongoing basis. With the acceptance of payment card transactions comes the responsibility for managing sensitive data. Security measures must be current and complete to minimise risk.

7.1.4 The payment card industry's fines for non-compliance are costly and affect the entire campus community. A single UBC merchant in breach of compliance can incur fines of up to $500,000.00 per incident. The penalty for a breach can also result in increased costs for the entire University and mandated third-party oversight of all of the University's credit card processing systems.

7.1.5 All merchants within UBC that conduct payment card transactions must comply with the PCI-DSS requirements in order to securely process payment card information.

7.1.6 All UBC merchant systems components that store, process or transmit payment card data must comply with the PCI-DSS Requirements.

PCI-DSS Requirements

7.1.7 Each UBC merchant is responsible for conducting an annual risk assessment that identifies threats and vulnerabilities to merchant system components that store, process or transmit payment card data, as well as updating that risk assessment when their payment card processing environment changes.

7.1.8 The following 12 requirements are a general outline of the detailed PCI-DSS. UBC merchants are responsible for fully complying with all of the detailed requirements of the PCI-DSS, as described online at https://www.pcisecuritystandards.org/.

a) **Install and maintain a network firewall to protect cardholder data.**

Guidance 7.1.8.a: Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Network firewalls are a key protection mechanism for any computer network. All systems must be protected against unauthorised access from the Internet; this includes but is not limited to:

- *Entering the system from the Internet for e-commerce.*
- *Merchant personnel's Internet-based access through desktop browsers.*
- *Merchant personnel's e-mail access.*

b) Do not use vendor-supplied defaults for system passwords and other security parameters.

Guidance 7.1.8.b: Hackers (external and internal to an organisation) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

c) Protect stored cardholder data.

Guidance 7.1.8.c: Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data without the proper cryptographic keys, the data is unreadable and unusable to that person. Other

effective methods of protecting stored data should be considered as potential risk mitigation opportunities, such as not storing cardholder data unless absolutely necessary and truncating cardholder data if the full PAN is not needed.

d) **Encrypt transmission of cardholder data across open, public networks.**

Guidance 7.1.8.d: Cardholder information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify and divert the data while in transit.
WEP is prohibited for wireless security as it is insecure.
Never send unencrypted PANs via end-user messaging technologies (e.g. e-mail, instant messaging/chat)

e) Use and regularly update anti-virus software.

Guidance 7.1.8.e: Many vulnerabilities and malicious viruses enter the network via merchant personnel's e-mail and web browsing activities. Anti-virus software must be used on all merchant systems commonly affected by viruses to protect the systems from malicious software.

f) **Develop and maintain secure merchant systems and applications.**

Guidance 7.1.8.f: Unscrupulous individuals use security vulnerabilities to gain privileged access to merchant systems. Many of these vulnerabilities are fixed by vendor-provided security patches or updates. All merchant systems must have the most recently released appropriate software patches to protect against exploitation by merchant personnel, external hackers and viruses.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations or software. Custom developed web applications handling e-commerce payments shall follow the OWASP practices and guidelines for secure coding. All web applications require a formal code review and signoff by another independent developer.

g) **Restrict access to cardholder data by organisational need-to-know.**

Guidance 7.1.8.g: This requirement ensures critical data can only be accessed by authorised merchant personnel.

h) **Assign a unique ID to merchant personnel with computer access.**

Guidance 7.1.8.h: Assigning a unique ID to merchant personnel with access ensures that actions taken on critical data and merchant systems are performed by, and can be traced to, known and authorised users.

i) **Restrict physical access to cardholder data.**

Guidance 7.1.8.i: Any physical access to data or merchant systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove merchant systems components or hardcopies and should be appropriately restricted.

j) **Log all access to network resources and cardholder data within the merchant system environment.**

Guidance 7.1.8.j: Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows tracking and analysis in case something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

k) **Regularly test security systems and processes.**

Guidance 7.1.8.k: Vulnerabilities are continually being discovered by hackers and researchers, in addition to being introduced by new software. Merchant systems, processes and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.

l) Maintain a policy that addresses information security for merchant personnel, including contractors.

Guidance 7.1.8.l: A strong security policy sets the security tone for the whole organisation and informs merchant personnel what is expected of them. All merchant personnel must be made aware of the policy and the sensitivity of data, along with their responsibilities for protecting it.

Intellectual Property Rights

7.1.9 Intellectual property rights are covered in UBC Policy 104 Sections 3.1, 3.2 and 6.1.

Guidance 7.1.9: the University strongly values intellectual property, whether it is property created under research at UBC or property copyrighted by others. The University has a site dedicated to copyright materials and their usage: "Copyright at UBC".

Data Protection and Privacy of Personal Information

7.1.10 Data protection and privacy of personal information is covered in UBC Policy 104 Sections 1.4, 2.1, 2.2, 2.4 and 2.5.

Guidance 7.1.10: the University respects the privacy of personal information and as such, system administrators will not access personal information (see examples in section 1.2.1 of this manual) without proper authorisation. Specifically, that authorisation must come from the administrative Head of the unit, Human Resources and University Counsel; this is done to ensure that there is good justification for accessing the information. The "Authorization to Access Electronic Accounts & Records" form can be found on the UBC IT website.

7.2 Information Systems Audit Considerations

Objective: *Audits of institutional systems shall be planned and agreed upon, in order to minimize the risk of disruptions to University operations.*

7.2.1 The Information Security Office must publish clear audit controls, for self-audits by functional stewards/owners of information assets, as a framework for use in regular audits

Guidance 7.2.1: The University, via the Information Security Office, has a responsibility to publish self-audit controls, which can be used by functional stewards/owners, to better understand how effectively they have implemented security controls on a particular information asset. At a minimum, it is recommended that self-audits should be performed on the highest priority information asset in each department at least once a year.

7.2.2 Departments should know what their responsibilities are with respect to self-audits

Guidance 7.2.2: It is the functional data stewards/owners responsibility to perform self-audits. There should be a designated information technology resource within each department who can implement the self-audit on behalf of the data steward/owner; however, it is the steward/owner's responsibility to see that it is completed.

Appendix A - Glossary

A1 **AES:** Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. It supersedes DES. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

A2 **Administrative Systems:** are all administrative and academic computer facilities, electronic media, communications networks, software programs, systems, and hardware of all types that are owned by the University and/or used, wholly or in part, for administrative functions. This includes, but is not limited to, application software, operating system software, operating support software, security software, and computer communications equipment and associated equipment, transmission media of all types, gateways, and networks.

A3 **Administrative Data:** are the information and data used by the University to fulfill administrative functions.

A4 **Anonymised Data:** the act of permanently and completely removing personal identifiers from data, such as converting personally identifiable information into aggregated data. Anonymised data is data that can no longer be associated with an individual in any manner. Once this data is stripped of personally identifying elements, those elements can never be re-associated with the data or the underlying individual (source: Educause).

A5 **Anti-virus:** is used to prevent, detect and remove malware, including but not limited to, computer viruses, computer worms, trojan horses, spyware and adware. UBC has licensed Sophos Anti-Virus for all University owned systems, as well as for home systems of employees and students.

A5.1 **Email Server Security:** The University has licensed Sophos PureMessage for the protection of UBC email servers from phishing, spam and other malware.

A6 **Asset:** anything that has value to the organisation (source: International Organization for Standardization 27000).

A7 **Backup:** the process of backing up refers to making copies of data, so that these additional copies may be used to restore the original after a data loss event.

A8 **Breach:** What occurs when one or more persons obtain unauthorised access to data in an asset.

A9 **Break Glass**: break glass (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 privileges to certain information, to gain access when it is necessary.

A10 **CVSS v2:** Common Vulnerability Scoring System (CVSS) version 2 is an industry standard for assessing the severity of computer system security vulnerabilities. It attempts to establish a measure of how much concern a vulnerability warrants, compared to other vulnerabilities,

so efforts can be prioritised. The score is based on a series of measurements (called metrics) based on expert assessment (source: Wikipedia). The CVSS v2 is used by the National Institute of Standards and Technology (NIST) and the National Vulnerability Database (NVD) in North America.

A10.1 **High Severity Vulnerability:** vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

A10.2 **Medium Severity Vulnerability:** vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9

A10.3 **Low Severity Vulnerability:** vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9

A11 **Data Masking:** is the process of obscuring (masking) specific data elements within data stores. It ensures that sensitive data is replaced with realistic but not real data. The goal is that sensitive customer information is not available outside of the authorized environment. Data masking is typically done while provisioning non-production environments so that copies created to support test and development processes are not exposing sensitive information and thus avoiding risks of leaking.

A12 **De-identified Data:** de-identification involves the removal of personally identifying information in order to protect personal privacy. De-identified data is not anonymised data; this means that the personally identifying information may be able to be re-associated with the data at a later time.

A13 **Electronic Medical Record:** the Electronic Medical Record (EMR) generally refers to an electronic version of the traditional paper-based patient record used within a medical practice setting. The EMR is a comprehensive record of health information compiled during a direct patient-provider relationship and is under the stewardship of the physician providing primary care (source: B.C. Office of the Information Privacy Commissioner).

A14 **FIPPA:** the Freedom of Information and Protection of Privacy Act in British Columbia. The Act governs how PII must be collected, used and protected, in addition to describing how an individual can access their own PII under that act.

A15 **Firewall:** Firewalls can be implemented in both hardware and software, or a combination of both. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria for the organisation. Firewalls are frequently used to prevent unauthorised Internet users from accessing private networks connected to the Internet.

A15.1 **Network Firewall:** protects networks of connected computers, printers and other devices from the internet or other networks. Firewalls control computer traffic allowed into and out of an organisation's network, as well as traffic into more sensitive areas within an organisation's internal network.

A15.2 **Host-based Firewall:** is a piece of software running on a single host that can restrict incoming and outgoing network activity for that host only. They can prevent a host from becoming infected and stop an infected host from spreading malware to other hosts.

A16 **Functional Steward/Owner:** the functional person(s) responsible for determining how the data in an asset is used and who can access the data.

A17 **HTTPS:** Hypertext Transfer Protocol Secure (HTTPS) is a combination of Hypertext Transfer Protocol (HTTP) with SSL/TLS protocol. It provides encrypted communication and secure identification of a network web server. HTTPS connections are often used for payment transactions on the World Wide Web and for sensitive transactions in corporate information systems (source: Wikipedia).

A18 **ID**: stands for identification.

A19 **Information Asset:** a collection of data needed to conduct University business (administrative, academic or research).

A20 **Learning Management System (LMS):** UBC supports a single Learning Management System, operated by UBC IT. The system is currently using the WebCT Vista product and by 2014 will be transitioned to be using the Blackboard Learn product.

A21 **Merchant**: any university entity that accepts payment cards bearing the logos of any of the five members of the PCI-DSS (American Express, Discover, JCB, MasterCard or VISA).

A22 **Merchant Personnel**: for the purposes of PCI-DSS compliance, "merchant personnel" refers to full-time and part-time employees, temporary employees and personnel, volunteers, and contractors and consultants who are "resident" on the university's site.

A23 **Merchant System components**: any network component, server or application that possesses cardholder or authentication data.

A23.1 **Applications**: include all purchased and custom applications, including internal and external (Internet) applications.

A23.2 **Network components**: include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances and other security appliances.

A23.3 **Server types**: include but are not limited to web, database, authentication, email, proxy, network time protocol (NTP) and domain name server (DNS).

A24 **Mobile Devices**: any portable hand-held electronic device used for accessing other systems or data. Examples include, but are not limited to: smartphones (Android, BlackBerry, iPhone, Windows Mobile, etc.) tablets and PDAs.

A25 **Network firewalls**: See firewalls.

A26 **OS**: an Operating System is the software that runs on specific hardware to allow user programs to run. Windows, Mac OS and BlackBerry OS are all examples of operating systems.

A27 **OWASP**: Open Web Application Security Project http://www.owasp.org/index.php/Main_Page.

A28 **PAN**: Primary Account Number is a definition used in the PCI-DSS.

A29 **Personal Information:** means recorded information about an identifiable individual other than contact information (source: B.C. FIPPA).

A30 **PCI-DSS**: Payment Card Industry - Data Security Standard (https://www.pcisecuritystandards.org/) describes how credit card data must be protected. The standard was defined by the 5 major brands: VISA, MasterCard, American Express, Discover and JCB.

A31 **PDA**: a personal digital assistant is a form of a mobile (computing) device.

A32 **PHI:** Protected Health Information (sometimes referred to as Personal Health Information) consists of demographic information, medical history, test and laboratory results, insurance information and other data that is collected by a health care professional to identify an individual and determine appropriate care.

A33 **PII:** Personally Identifiable Information is information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

A34 **QSA:** Qualified Security Assessors are used in the certification process for credit card handling through the PCI-DSS. These are independent 3rd party vendors who assess a merchant's compliance with the PCI-DSS.

A35 **Record:** in a database, a record holds all the information about one item or subject. It is like one index card in an index card file. In a file, a "record" probably has some fixed length, in contrast to a "line" which may have any length. A database record is also called a "row". In a spreadsheet it is always called a "row".
In all these cases, a record represents an entity with certain field values. Fields may be of a fixed width (bits or characters) or they may be separated by a delimiter character, often comma (CSV) or tab (TSV).

A36 **Removable Media:** refers to storage media which is designed to be removed from the computer without powering the computer off. Removable media may also refer to removable storage devices used to transport or store data.

A37 **SAQ:** Self Assessment Questionnaires (SAQ) are used in the certification process for credit card handling through the PCI-DSS. SAQs are categorised as "A" through "D".

A38 **Spoof:** to fool. In networking, the term is used to describe a variety of ways in which hardware and software can be fooled. IP spoofing, for example, involves trickery that makes a message appear as if it came from an authorised IP address. Also see e-mail spoofing (source: Webopedia).

A39 **TLS:** Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

A40 **Transparent Data Encryption:** Transparent Data Encryption (often abbreviated to TDE) is a technology employed by both Microsoft and Oracle to encrypt database content. TDE offers encryption at a column, table, and tablespace level. TDE solves the problem of protecting data at rest, encrypting databases both on the hard drive and consequently on backup media. Enterprises typically employ TDE to solve compliance issues such as PCI DSS.

A41 **University IT Personnel:** any personnel (faculty, staff, consultants, students, etc.) carrying out university information technology administrative/technical duties on behalf of the University or a unit within the University.

A42 **User:** a person who uses a computer or a computing network, especially a person who has received a user account (source: Wiktionary).

A43 **Vulnerability Assessment:** a systematic search for weaknesses/exposures, by which threats can be manifested, in order to apply a patch or fix to prevent a compromise; also used to validate that one or more patches or fixes were correctly installed. See CVSS v2 for definitions of High, Medium and Low Severity vulnerabilities.

A44 **WEP:** Wired Equivalent Privacy (WEP) is a weak security algorithm for wireless networks. Although its name implies that it is as secure as a wired connection, WEP has been demonstrated to have numerous flaws and has been deprecated in favour of newer standards such as WPA2 (source: Wikipedia).

A45 **WPA2:** WPA2 (Wi-Fi Protected Access 2) provides network administrators with a high level of assurance that only authorised users can access the network. Based on the ratified IEEE 802.11i standard, WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm. WPA2 can be enabled in two versions - WPA2 - Personal and WPA2 - Enterprise. WPA2 - Personal protects unauthorized network access by utilizing a set-up password. WPA2 - Enterprise verifies network users through a server. WPA2 is backward compatible with WPA (source: Wi-Fi Alliance).

Appendix B – Available Tools

B1 **Anti-virus:** UBC has licensed Sophos Anti-Virus for all University owned systems, as well as for home systems of employees and students. Information on the UBC licensed version can be found on the UBC IT anti-virus site.

B1.1 **Email Server Security:** UBC has licensed Sophos PureMessage for the protection of UBC departmental email servers from phishing, spam and other malware. Information on the UBC licensed version can be found on the UBC IT PureMessage site.

B2 **Certificates:** TLS certificates may be purchased under the University's Enterprise account, via the Information Security Office, by contacting security@ubc.ca.

B3 **Firewall:** UBC has commercial tools available for both Network and Host-based firewalls.

B3.1 **Network Firewall:** UBC IT can provide departments with a virtual network firewall at no charge. Details can be found on the UBC IT Virtual Firewall website.

B3.2 **Host-based Firewall:** UBC has licensed Sophos Endpoint Security and Control as a host-based firewall solution for departmental systems. Information on the UBC licensed version can be found on the UBC IT PureMessage and Enterprise Console site.

B4 **Security Awareness Training:** UBC has licensed training, which is available in brief 1 to 7 minute video modules for all employees and graduate students. The training can be accessed on the UBC Learning Management System site.

Appendix C – ISO 27002:2005

The University of British Columbia follows the International Organization for Standardization (ISO) 27002:2005 "Code of Practice for Information Security Management", as a roadmap, for its information security programme. This is used in guiding the programme to ensure that the security of information assets, at the University, is effectively managed through conscious application of international standards wherever applicable and reasonable for the institution.