PRIVACY MATTERS @ UBC

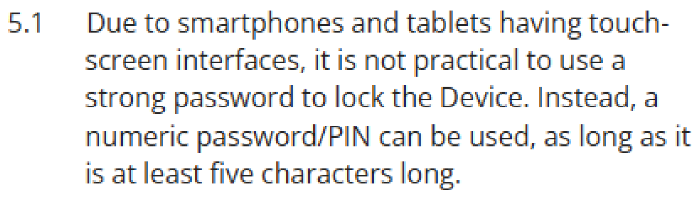
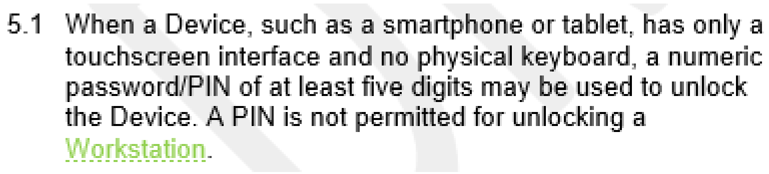
PRIVACY AND INFORMATION SECURITY MANAGEMENT

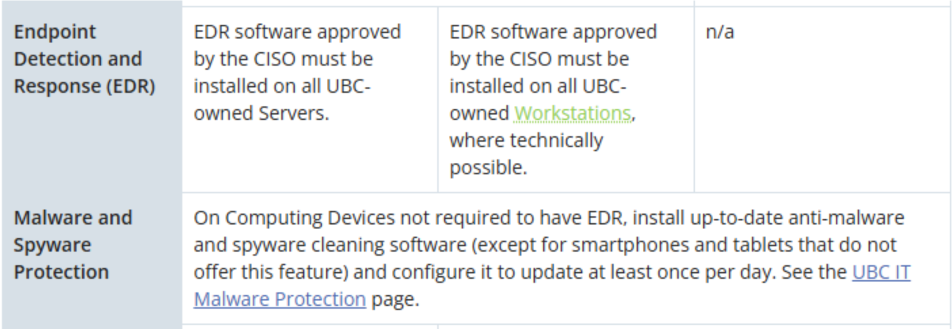
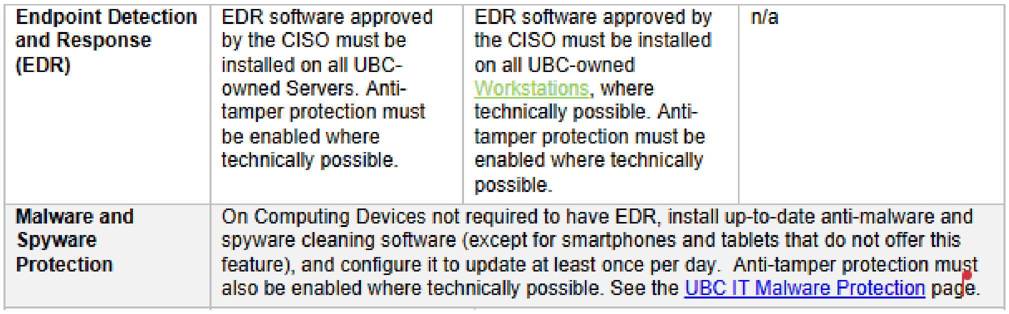
2024 Information Security Standards Review

Last updated: 11 March 2025

Contents

Standalone Updates

#	Std	Changes
U1	Security Classification of UBC Electronic Information and Services **Attachments:** UBC Asset Inventory Template & Guidance.xlsx	Updated Resource – Sample Inventory now includes tabs (with examples) for: • Inventory - Administrative Head • Inventory - IT Support Staff
U2	Passphrase and Password Protection	**Section 5, Passphrases/Passwords for Devices with Touchscreen Interfaces** (Modified)**:** Simplified and added clarity on PIN usage not being permissible for Workstations. **CURRENT:**  5.1 Due to smartphones and tablets having touch-screen interfaces, it is not practical to use a strong password to lock the Device. Instead, a numeric password/PIN can be used, as long as it is at least five characters long. **NEW:**  5.1 When a Device, such as a smartphone or tablet, has only a touchscreen interface and no physical keyboard, a numeric password/PIN of at least five digits may be used to unlock the Device. A PIN is not permitted for unlocking a Workstation.
U3	Transmission and Sharing of UBC Electronic Information	**Section 3, Acceptable Methods of Transmitting and Sharing UBC Electronic Information** (Modified): • Compute Canada updated to Digital Research Alliance of Canada • Latest approved Terms of Service for the Alliance Federation has been modified to be more explicit about intended data classification – specifically, Alliance Federation Systems and Services are not intended for the storage and processing of High-Risk and Very High-Risk Information. Authorized locations for UBC Electronic Information in Section 3.5 updated to include this. **NEW:** 3.5.4 Digital Research Alliance of Canada (not to be used for storage/processing of High and Very Risk Information);
U7	Securing Computing and Mobile Storage Devices or Media	**Section 2, Electronic Security** • Under EDR and Malware and Spyware Protection, updated to note that anti-tamper protection must also be enabled, to prevent removal. This has been a practice and requirement by CISO, was not formalized in the ISS.

<table>
<tr><th>#</th><th>Std</th><th>Changes</th></tr>
<tr><td></td><td></td><td>
<b>CURRENT:</b>

<table>
<tr><td><b>Endpoint Detection and Response (EDR)</b></td><td>EDR software approved by the CISO must be installed on all UBC-owned Servers.</td><td>EDR software approved by the CISO must be installed on all UBC-owned Workstations, where technically possible.</td><td>n/a</td></tr>
<tr><td><b>Malware and Spyware Protection</b></td><td colspan="3">On Computing Devices not required to have EDR, install up-to-date anti-malware and spyware cleaning software (except for smartphones and tablets that do not offer this feature) and configure it to update at least once per day. See the UBC IT Malware Protection page.</td></tr>
</table>
<b>NEW:</b>

<table>
<tr><td><b>Endpoint Detection and Response (EDR)</b></td><td>EDR software approved by the CISO must be installed on all UBC-owned Servers. Anti-tamper protection must be enabled where technically possible.</td><td>EDR software approved by the CISO must be installed on all UBC-owned Workstations, where technically possible. Anti-tamper protection must be enabled where technically possible.</td><td>n/a</td></tr>
<tr><td><b>Malware and Spyware Protection</b></td><td colspan="3">On Computing Devices not required to have EDR, install up-to-date anti-malware and spyware cleaning software (except for smartphones and tablets that do not offer this feature), and configure it to update at least once per day. Anti-tamper protection must also be enabled where technically possible. See the UBC IT Malware Protection page.</td></tr>
</table>
</td></tr>
<tr><td>U9</td><td>Outsourcing and Service Provider Management

<b>Attachments:</b>
Security and Confidentiality Agreements - New OUC Website Content (v2)</td><td>
<b>Section 5, Contractual Requirements</b> (Modified):
<ul>
<li>University Counsel website updated to reflect tightening of scope of when a SACA is required.</li>
<li>Details removed from standard, and SACA page updated</li>
<li>SACA Page: https://universitycounsel.ubc.ca/subject-areas/access-and-privacy-general/useful-resources/security-and-confidentiality-agreements/</li>
</ul>
<b>CURRENT:</b>
5.1 Service Providers must sign a Security and Confidentiality Agreement (SACA) prior to being granted access to Medium, High or Very High Risk 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.

<b>NEW:</b>
5.1 Before being granted access to Medium, High or Very High Risk Information, Service Providers must do one of the following:
5.1.1 enter into a service agreement with UBC that includes a Privacy Appendix in the form prescribed by Procurement Services;
5.1.2 sign a Security and Confidentiality Agreement (SACA) in the form prescribed by the Office of the University Counsel; or
5.1.3 obtain a waiver from the Office of the University Counsel.
5.2 Further information about these requirements is available from the Office of the University Counsel.
</td></tr>
<tr><td>M1</td><td>Requesting Variances from Information Security Standards</td><td>
<b>Section 2, Variance Request Procedure</b> (Modified):
Updated to include link to Variance Request Form (Word document)

<b>S2.1 CURRENT:</b> Initial Request - the Administrative Head of Unit must submit the following information to information.security@ubc.ca:
</td></tr>
</table>

#	Std	Changes
	Attachments: Variance Request Form	**S2.1 NEW:** Initial Request - the Administrative Head of Unit must submit the Variance Request Form to information.security@ubc.ca, which includes the following information:
M10	Internet-facing Systems and Services	**Section 2, Security Architecture Requirements** • S2.6 (New): Internet or Intranet-facing UBC Electronic Services such as websites or Web Applications used to conduct University Business must be provisioned within the ubc.ca domain name space, e.g. widget.ubc.ca, unless not technically possible.
M11	Development and Modification of Software Applications	**Section 5, Naming Requirements for Web Applications** • Section 5 removed entirely • Single bullet 5.1 revised and moved to M10, Section 2, Security Architecture Requirements as S2.6 – see above ○ **S5.1 CURRENT:** Web Applications used to conduct University Business must be provisioned within the ubc.ca domain name space, e.g. widget.ubc.ca, unless not technically possible.

Changes Related to Auto-forwarding

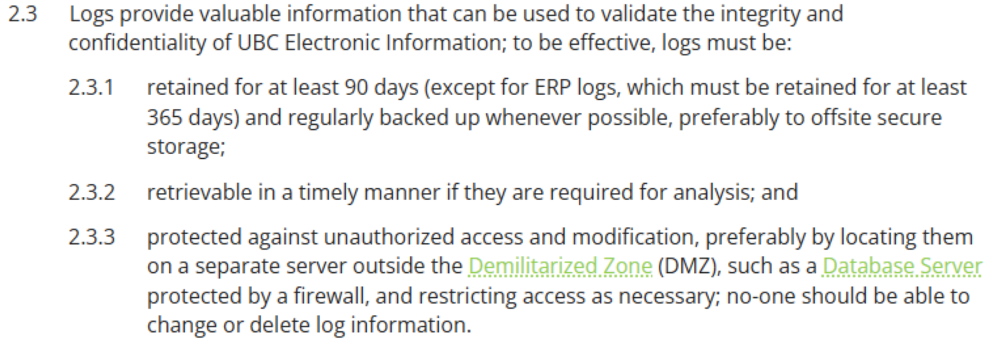
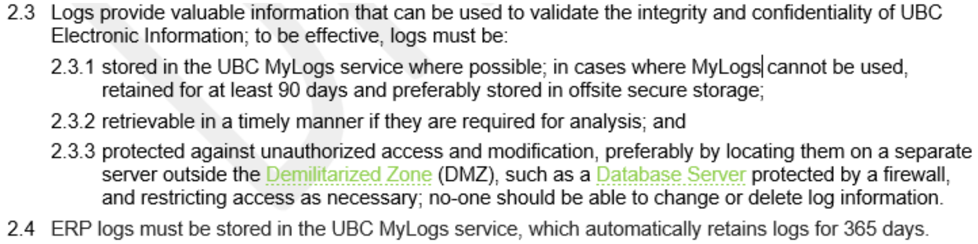
#	Std	Changes
U3	Transmission and Sharing of UBC Electronic Information **Attachments:** UBC Email Auto-forwarding Agreement	Section 4 – Renamed "Auto-forwarding from UBC Email Accounts" (previously "Email Forwarding from UBC Email Accounts") New Glossary term for ***Auto-forwarding*** • **S4.1 (previously 4.2)** (Modified)**:** **CURRENT:** Forwarding or redirecting UBC email accounts that are used to transmit UBC Electronic Information to a personal email account is not permitted. **NEW:** Automatically forwarding or redirecting UBC email accounts (Auto-forwarding) to a non-business email account (e.g. a personal Gmail, Hotmail or Yahoo account) is not permitted. • **S4.2 (previously 4.1)** (Modified)**:** Revised circumstances where Auto-forwarding from UBC email accounts is acceptable. Introduced new "Managing Multiple Email Accounts" guideline document **CURRENT:** Automatically forwarding or redirecting UBC email accounts to non-UBC accounts ("auto-forwarding") is only acceptable for UBC faculty and staff members who have appointments at other institutions and have difficulty managing multiple work email accounts. Under these circumstances, it is acceptable to auto-forward the UBC email account to the email account at the other institution, provided that: ○ the other institution is a public sector institution located in Canada; ○ the other institution's email system is at least as secure as UBC's email system; and ○ the staff or faculty member ensures that copies of emails of business value are returned to UBC Systems, so that they are managed in accordance with UBC's Records Management Policy. **NEW:** Auto-forwarding to non-UBC business email accounts is only acceptable for UBC faculty and staff members who have employment or appointments at other organizations and are unable to manage multiple work email accounts (see Managing Multiple Email Accounts guideline). Under these circumstances, Auto-forwarding is acceptable if:

#	Std	Changes
		○ the other organization is a public body located in British Columbia and is subject to the Freedom of Information and Protection of Privacy Act, including the associated data residency and security requirements; and ○ the faculty or staff member ensures that copies of emails are retained on or copied to UBC Systems in accordance with UBC's Records Management Policy. • **S4.3** (New)**:** Introduced new "UBC Email Auto-forwarding Agreement" **NEW:** Auto-forwarding to non-UBC business email accounts outside of the circumstances set out in section 4.2 is prohibited unless the User has submitted the UBC Email Auto-forwarding Agreement and it has been approved by the Administrative Head of Unit and CISO.

Changes Related to Incident Response

#	Std	Changes
U4	Reporting Information Security Incidents **Attachments:** Securing and Preserving Electronic Evidence guideline	Standard renamed "Reporting Cybersecurity Incidents", to align with revised UBC Cybersecurity Incident Response Plan New Glossary term for ***Cybersecurity Incident*** **Cybersecurity Incident Response Plan** rewritten to align with current practices that closely mirror "harmonized incident response" workflows. • Currently published to CC site as a PDF (requires CWL credentials), but will be moved to the Privacy Matters website and published in HTML format (requiring CWL credentials) **S3, How to Report Incidents**: • 3.1.1.2 (New): assess whether to engage UBC's contracted third party digital forensics and incident response (DFIR) services. The affected department or faculty will be responsible for any costs associated with the incident. • 3.3 (New): Incidents where a system is compromised and threat actors are interacting directly with the system (not an automated attack but a "hands on keyboard" attack), UBC Cybersecurity will isolate the system on the network to reduce damages, while making every effort to contact the Technical Owner and Information Stewards/Owners.

Changes Related to Logging and Monitoring

#	Std	Changes
M8	Logging and Monitoring of UBC Systems **Attachments:** M8	**Section 2, Logging and Monitoring Requirements** (Modified): **CURRENT:**  2.3 Logs provide valuable information that can be used to validate the integrity and confidentiality of UBC Electronic Information; to be effective, logs must be: 2.3.1 retained for at least 90 days (except for ERP logs, which must be retained for at least 365 days) and regularly backed up whenever possible, preferably to offsite secure storage; 2.3.2 retrievable in a timely manner if they are required for analysis; and 2.3.3 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. **NEW:**  2.3 Logs provide valuable information that can be used to validate the integrity and confidentiality of UBC Electronic Information; to be effective, logs must be: 2.3.1 stored in the UBC MyLogs service where possible; in cases where MyLogs cannot be used, retained for at least 90 days and preferably stored in offsite secure storage; 2.3.2 retrievable in a timely manner if they are required for analysis; and 2.3.3 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. 2.4 ERP logs must be stored in the UBC MyLogs service, which automatically retains logs for 365 days. **Section 5, Use and Disclosure of Logs:** Approval methods for access to logs updated to include: • **S5.1.4** (New): internally or externally in accordance with the Data Access Request (DAR) process.

Changes Related to Privacy Impact Assessments

#	Std	Changes
U3	Transmission and Sharing of UBC Electronic Information	**Section 2, Key Considerations when Transmitting and Sharing UBC Electronic Information** (Modified): **S2.4 CURRENT:** Computing services based outside of Canada (such as Gmail) are not permitted for transmission or sharing of Personal Information unless a Privacy Impact Assessment (PIA) has been conducted for that service, and the risks of storage outside of Canada have been considered and accepted. Please refer to the PIA Process Overview for more information. **S2.4 NEW:** Computing services based outside of Canada (such as Gmail) are not permitted for transmission or sharing of Personal Information unless a Privacy Impact Assessment (PIA) has been conducted for that service, and the risks of storage outside of Canada have been considered and accepted. When sensitive personal information will be stored outside of Canada, the initiative must receive approval through the PIA process. For academic research projects, a Security Threat Risk Assessment (STRA) may be required in place of a PIA when the tool is used solely for research purposes, as outlined in UBC's research-specific guidelines. Please refer to the PIA & STRA webpage for more information.
U9	Outsourcing and Service Provider Management	**Section 2, Security and Privacy Risk Assessment** (Modified): **S2.2 CURRENT:** In addition to the requirement to use the above checklist, a Privacy Impact Assessment (PIA) is required if Personal Information is involved. Please refer to the PIA Process Overview for more

#	Std	Changes
		information. **S2.2 NEW:** In addition to the requirement to use the above checklist, a Privacy Impact Assessment (PIA) is required if Personal Information is involved. For academic research projects, a Security Threat Risk Assessment (STRA) may be required in place of a PIA when the tool is used solely for research purposes, as outlined in UBC's research-specific guidelines. Please refer to the PIA & STRA webpage for more information.
U11	Securing Internet of Things (IoT) Devices	**Section 2, IoT Device Risk** (Modified): **S2.4.1 CURRENT:** Projects or initiatives involving IoT Devices that collect, store or access Personal Information must undergo a Privacy Impact Assessment (PIA), as set out in the Privacy Impact Assessment requirements. **S2.4.1 NEW:** Projects or initiatives involving IoT Devices that collect, store or access Personal Information must undergo a Privacy Impact Assessment (PIA). For academic research projects, a Security Threat Risk Assessment (STRA) may be required in place of a PIA when the tool is used solely for research purposes, as outlined in UBC's research-specific guidelines. Please refer to the PIA & STRA webpage for more information.
M11	Development and Modification of Software Applications	**Section 2, Assessing Security Requirements for Projects Involving Medium, High or Very High Risk Information** (Modified): **S2.2 CURRENT:** All new or substantially modified applications that store or access Personal Information must also undergo a privacy impact assessment (PIA), as set out in the Privacy Impact Assessment Requirements. This PIA may require additional security assessments. **S2.2 NEW:** All new or substantially modified applications that store or access Personal Information must also undergo a privacy impact assessment (PIA). For academic research projects, a Security Threat Risk Assessment (STRA) may be required in place of a PIA when the tool is used solely for research purposes, as outlined in UBC's research-specific guidelines. Please refer to the PIA & STRA webpage for more information.

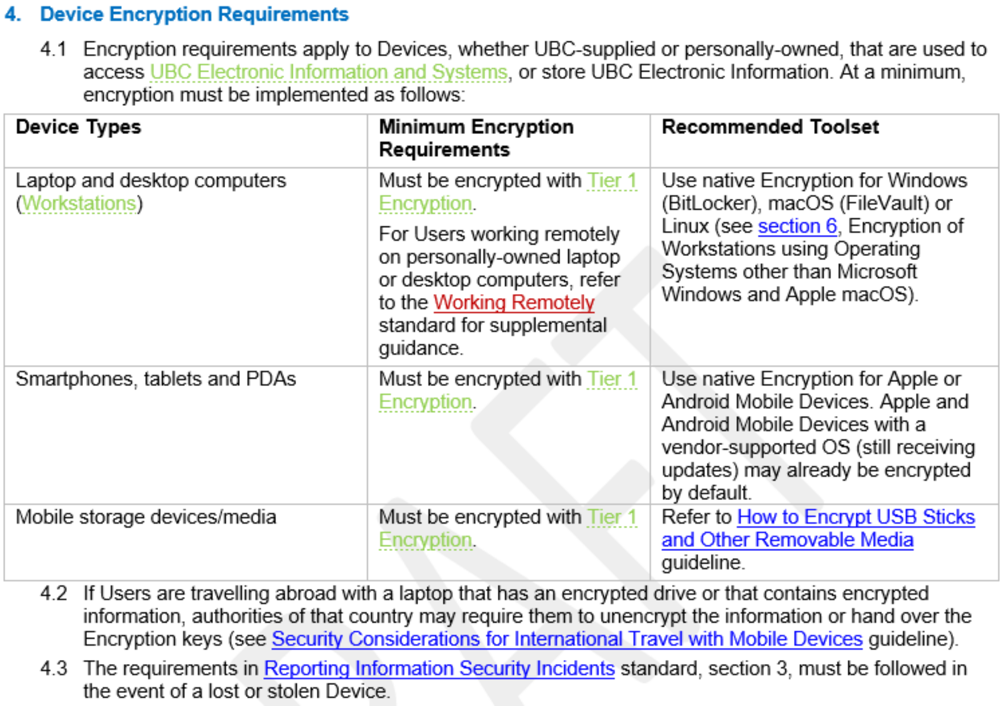
Changes Related to Encryption

#	Std	Changes
U4	Reporting Information Security Incidents **Attachments:** U4, U5	**Section 3, How to Report Incidents** • **S3.1.4** (Moved from U5, S3.5): Users must provide a written confirmation of the encryption status and method (e.g. encrypted with BitLocker) at the time of loss or theft. University IT Support Staff may be able to assist in providing this information. • **Related change:** U5, S3.5 (now S4.3) has been modified to read, “The requirements in Reporting Information Security Incidents standard, section 3, must be followed in the event of a lost or stolen Device.”
U5	Encryption Requirements **Attachments:** Variance for EduCloud (in progress)	**Section 2, Password Protection and Zipping** (Modified): • New S2.3/2.4 have been taken directly from Section 7, File-Level Encryption Requirements. That section is now eliminated. • S2.3 (Moved from S7): For instructions on encrypting Word, Excel and other general files, refer to the How to Encrypt Files Using Common Applications guideline. • S2.4 (Moved from S7): For requirements on emailing UBC Electronic Information, refer to the Transmission and Sharing of UBC Electronic Information standard. **Section 3, Storage Encryption Risk and Classification Model** (New): • New Glossary terms for ***Encryption*** and ***Encryption Tiers***

#	Std	Changes

- **S3.1 NEW:** For details on the types of risks associated with the storage of information, and which encryption tiers mitigate which risks, refer to section 3 of the Cryptographic Controls standard.

Section 4, Device Encryption Requirements (Modified):



4. Device Encryption Requirements

4.1 Encryption requirements apply to Devices, whether UBC-supplied or personally-owned, that are used to access UBC Electronic Information and Systems, or store UBC Electronic Information. At a minimum, encryption must be implemented as follows:

Device Types	Minimum Encryption Requirements	Recommended Toolset
Laptop and desktop computers (Workstations)	Must be encrypted with Tier 1 Encryption. For Users working remotely on personally-owned laptop or desktop computers, refer to the Working Remotely standard for supplemental guidance.	Use native Encryption for Windows (BitLocker), macOS (FileVault) or Linux (see section 6, Encryption of Workstations using Operating Systems other than Microsoft Windows and Apple macOS).
Smartphones, tablets and PDAs	Must be encrypted with Tier 1 Encryption.	Use native Encryption for Apple or Android Mobile Devices. Apple and Android Mobile Devices with a vendor-supported OS (still receiving updates) may already be encrypted by default.
Mobile storage devices/media	Must be encrypted with Tier 1 Encryption.	Refer to How to Encrypt USB Sticks and Other Removable Media guideline.

4.2 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).

4.3 The requirements in Reporting Information Security Incidents standard, section 3, must be followed in the event of a lost or stolen Device.

- Formerly Section 3, Device-level Encryption Requirements. "-level" dropped as section is separated into Device and Server Encryption Requirements.

- S4.1 (formerly 3.1):
  - Under Minimum Encryption Requirements, specifies required *Tier*
  - Recommended toolset updated for Smartphones, Tablets and PDAs for Apple and Android Mobile Devices that may be encrypted by default
    - **CURRENT:** iOS and Android Devices with a vendor-supported OS (still receiving updates) connecting to FASmail using the native ActiveSync client are automatically encrypted.
    - **NEW:** Apple and Android Mobile Devices with a vendor-supported OS (still receiving updates) may already be encrypted by default.
  - Servers section of table moved to new Section 5, IT Infrastructure Encryption Requirements

- S4.x (formerly 3.2) (Moved to S5):

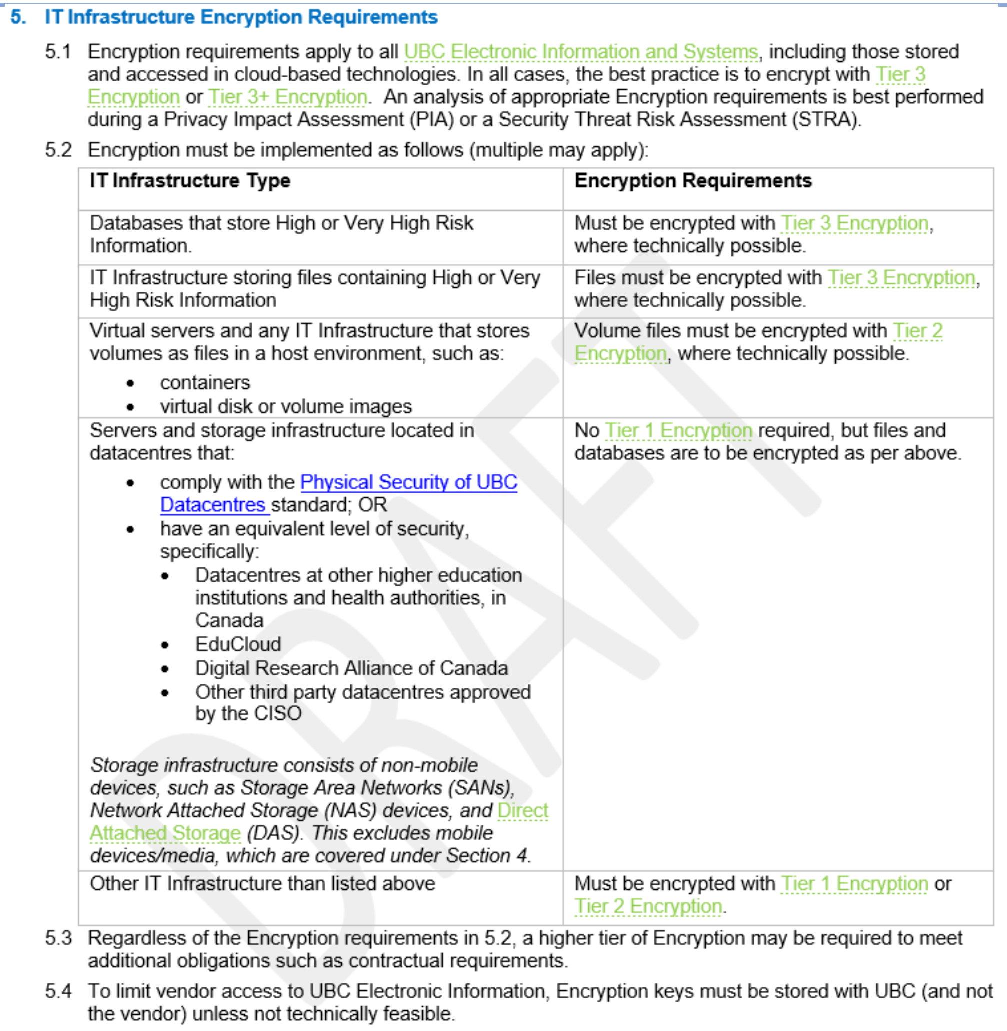
  S3.2 CURRENT: Even in situations where encryption is not required in section 3.1, encryption may nevertheless be required to meet additional obligations such as contractual requirements.

  S5.3 NEW: Regardless of the Encryption requirements in 5.2, a higher tier of Encryption may be required to meet additional obligations such as contractual requirements.

- S4.x (formerly 3.3) (Removed): Using Mobile Devices to store High or Very High Risk 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 High or Very High Risk Information) may be backed up automatically on the Device. In both of these situations, encryption would be required.

#	Std	Changes
		• S4.3 (formerly 3.5): **CURRENT**: If a Device is lost or stolen, it is essential for the University to be able to accurately report on its encryption status. Users must provide a written confirmation of the encryption status and method (e.g. encrypted with BitLocker) at the time of loss or theft. University IT Support Staff may be able to assist in providing this information. **NEW:** The requirements in Reporting Information Security Incidents standard, section 3, must be followed in the event of a lost or stolen Device. **Section 5, IT Infrastructure Encryption Requirements** (Modified): • Formerly Section 4, Cloud-based Encryption Requirements, completely rewritten. • Now includes 'Servers' section of table from S3(S4) in addition to previous Service Types (e.g. Virtual Servers) • S5.1/2: Under Encryption Requirements, specifies *IT Infrastructure* Type (new Glossary term) and required Tier • S5.3 (formerly 3.2): **CURRENT:** Even in situations where encryption is not required in section 3.1, encryption may nevertheless be required to meet additional obligations such as contractual requirements. **NEW:** Regardless of the encryption requirements in 5.2, a higher tier of encryption may be required to meet additional obligations such as contractual requirements.

#	Std	Changes



5. IT Infrastructure Encryption Requirements

5.1 Encryption requirements apply to all UBC Electronic Information and Systems, including those stored and accessed in cloud-based technologies. In all cases, the best practice is to encrypt with Tier 3 Encryption or Tier 3+ Encryption. An analysis of appropriate Encryption requirements is best performed during a Privacy Impact Assessment (PIA) or a Security Threat Risk Assessment (STRA).

5.2 Encryption must be implemented as follows (multiple may apply):

IT Infrastructure Type	Encryption Requirements
Databases that store High or Very High Risk Information.	Must be encrypted with Tier 3 Encryption, where technically possible.
IT Infrastructure storing files containing High or Very High Risk Information	Files must be encrypted with Tier 3 Encryption, where technically possible.
Virtual servers and any IT Infrastructure that stores volumes as files in a host environment, such as: • containers • virtual disk or volume images	Volume files must be encrypted with Tier 2 Encryption, where technically possible.
Servers and storage infrastructure located in datacentres that: • comply with the Physical Security of UBC Datacentres standard; OR • have an equivalent level of security, specifically: • Datacentres at other higher education institutions and health authorities, in Canada • EduCloud • Digital Research Alliance of Canada • Other third party datacentres approved by the CISO *Storage infrastructure consists of non-mobile devices, such as Storage Area Networks (SANs), Network Attached Storage (NAS) devices, and* Direct Attached Storage *(DAS). This excludes mobile devices/media, which are covered under Section 4.*	No Tier 1 Encryption required, but files and databases are to be encrypted as per above.
Other IT Infrastructure than listed above	Must be encrypted with Tier 1 Encryption or Tier 2 Encryption.

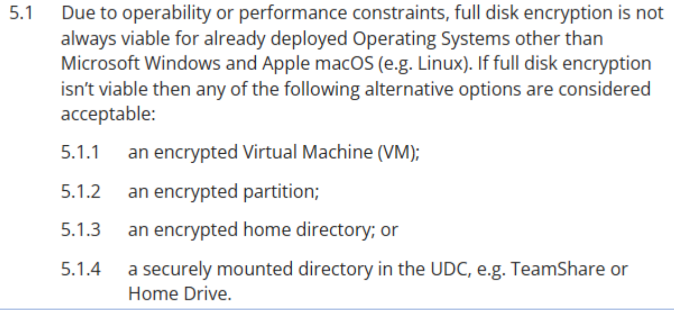
5.3 Regardless of the Encryption requirements in 5.2, a higher tier of Encryption may be required to meet additional obligations such as contractual requirements.

5.4 To limit vendor access to UBC Electronic Information, Encryption keys must be stored with UBC (and not the vendor) unless not technically feasible.

Section 6, Encryption of Workstations using Operating Systems other than Microsoft Windows and Apple macOS (e.g. Linux) (Modified)**:**

- Formerly “Encryption of Devices using… “
- Revisions to specify required Tier of encryption

S5.1 CURRENT:



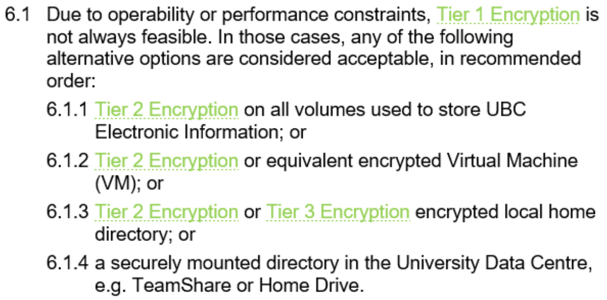
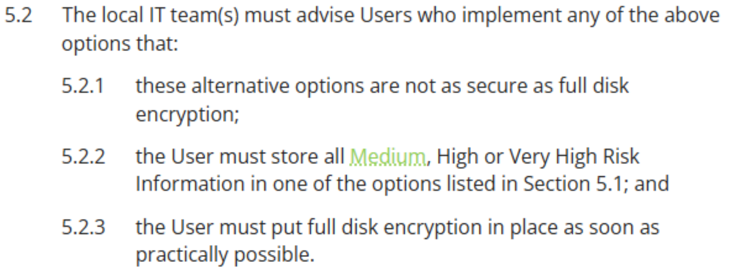
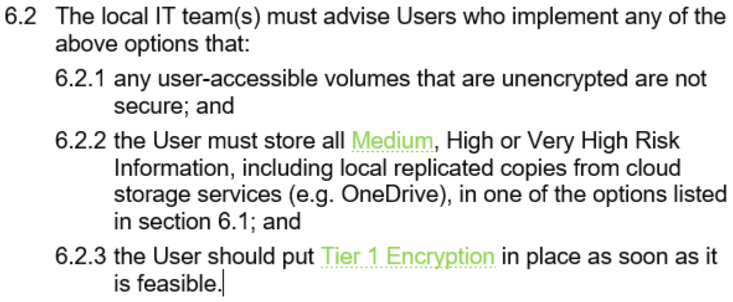
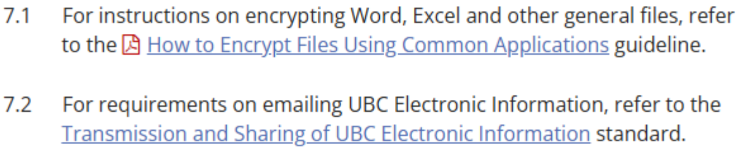
5.1 Due to operability or performance constraints, full disk encryption is not always viable for already deployed Operating Systems other than Microsoft Windows and Apple macOS (e.g. Linux). If full disk encryption isn’t viable then any of the following alternative options are considered acceptable:

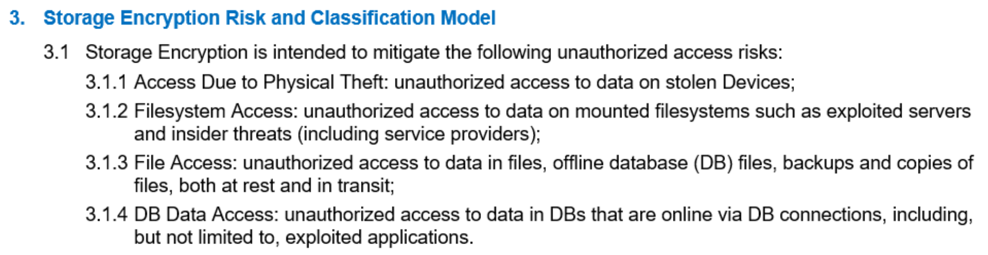
5.1.1 an encrypted Virtual Machine (VM);

5.1.2 an encrypted partition;

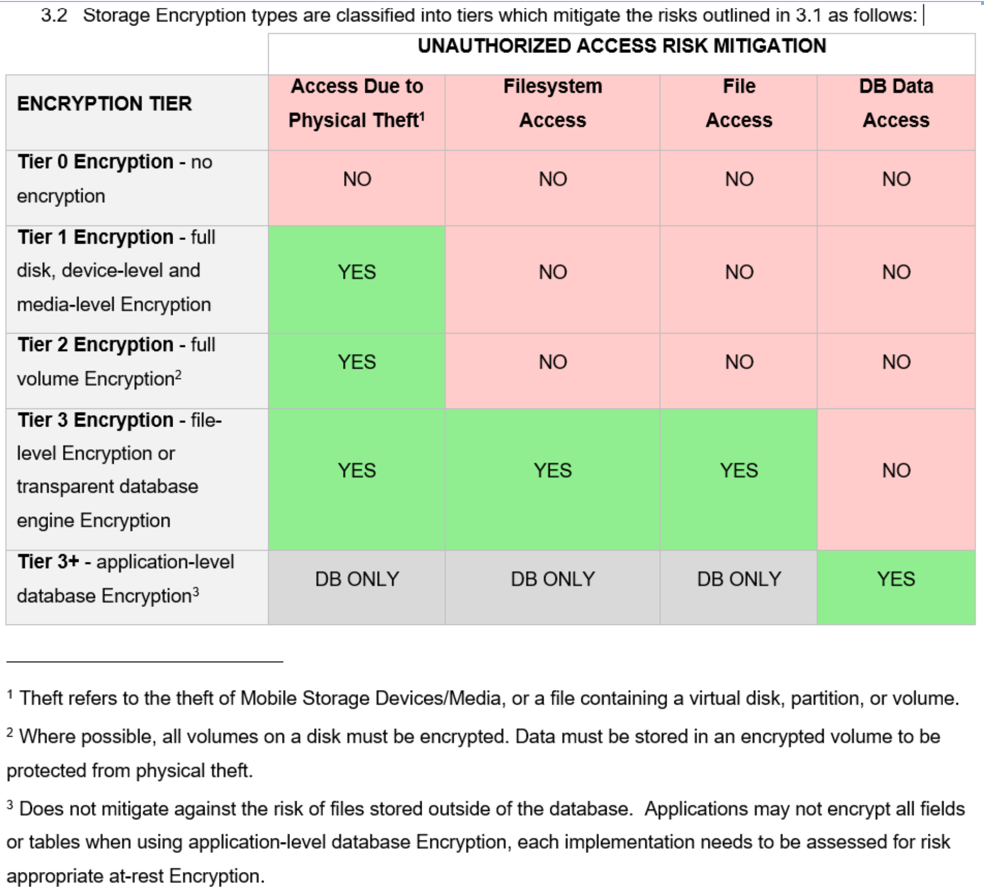
5.1.3 an encrypted home directory; or

5.1.4 a securely mounted directory in the UDC, e.g. TeamShare or Home Drive.

#	Std	Changes
		S6.1 NEW:  6.1 Due to operability or performance constraints, Tier 1 Encryption is not always feasible. In those cases, any of the following alternative options are considered acceptable, in recommended order: 6.1.1 Tier 2 Encryption on all volumes used to store UBC Electronic Information; or 6.1.2 Tier 2 Encryption or equivalent encrypted Virtual Machine (VM); or 6.1.3 Tier 2 Encryption or Tier 3 Encryption encrypted local home directory; or 6.1.4 a securely mounted directory in the University Data Centre, e.g. TeamShare or Home Drive. **S5.2 CURRENT:**  5.2 The local IT team(s) must advise Users who implement any of the above options that: 5.2.1 these alternative options are not as secure as full disk encryption; 5.2.2 the User must store all Medium, High or Very High Risk Information in one of the options listed in Section 5.1; and 5.2.3 the User must put full disk encryption in place as soon as practically possible. **S6.2 NEW:**  6.2 The local IT team(s) must advise Users who implement any of the above options that: 6.2.1 any user-accessible volumes that are unencrypted are not secure; and 6.2.2 the User must store all Medium, High or Very High Risk Information, including local replicated copies from cloud storage services (e.g. OneDrive), in one of the options listed in section 6.1; and 6.2.3 the User should put Tier 1 Encryption in place as soon as it is feasible. **Section 7, File-level Encryption Requirements** (Removed): • Bullets moved to Section 2, Password Protection and Zipping, as new 2.3 and 2.4  7.1 For instructions on encrypting Word, Excel and other general files, refer to the How to Encrypt Files Using Common Applications guideline. 7.2 For requirements on emailing UBC Electronic Information, refer to the Transmission and Sharing of UBC Electronic Information standard. **Section 8, Password Requirements** (Modified): • S8.2 Removed reference to Key Escrow Service, added reference to Password Safe **CURRENT:** 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. Where operationally feasible, faculty and staff can use the University’s Key Escrow services, 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. **NEW:** 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. Where possible, faculty and staff should use a password safe (refer to the Password Safe guideline), or simply write down the password and store it in

#	Std	Changes
		a secure location such as a safe. Further information about key recovery can be found in the Cryptographic Controls standard. **Section 9, Technical Requirements** (Modified)**:** - Recommendation to use AES-256 bit Encryption modified to read AES-256 bit **or better**
n/a	Encryption Exemptions	**Containers** added to Encryption Exemptions. UBC Systems are exempt from encryption requirements if they are fully compliant with the criteria below, and they have been documented in a completed and submitted Encryption Exemption Attestation Form: **Containers** Containers are executable software units that package application code with its libraries and dependencies, enabling it to run consistently across desktops, traditional IT and cloud environments. 1. The Container does not store UBC Electronic Information, including cached information. 2. Logs containing information needed for security investigation, as outlined in Section 2 of M8, Logging and Monitoring of UBC Systems are stored outside the Container. 3. Endpoint Detection and Response (EDR) software approved by the CISO has been installed where technically possible.
U9	Outsourcing and Service Provider Management **Attachments:** U9, Service Provider Security Checklist	**Section 6, Storage and Transmission of Information** - Addition of requirements to comply with encryption requirements at rest. - S6.2 (Modified): Service Providers must ensure that they store and transmit UBC Electronic Information in accordance with the Encryption Requirements and Transmission and Sharing of UBC Electronic Information standards. - Service Provider Security Checklist updated to match.
M7	Cryptographic Controls **Attachments:** M7, Key Escrow guideline	**Section 1, Introduction** - S1.1 (Modified): Revised for clarity ○ This document defines standards for the implementation and use of encryption technologies within UBC to maintain the confidentiality and integrity of UBC Electronic Information. For additional requirements, including ~~standards on when~~ where encryption is required, see the Encryption Requirements standard. **Section 3, Storage Encryption Risk and Classification Model** - Formerly "Full Disk Encryption (FDE)" - Complete section revamp, including list of access risks mitigated by storage encryption and tiers  **3. Storage Encryption Risk and Classification Model** 3.1 Storage Encryption is intended to mitigate the following unauthorized access risks: 3.1.1 Access Due to Physical Theft: unauthorized access to data on stolen Devices; 3.1.2 Filesystem Access: unauthorized access to data on mounted filesystems such as exploited servers and insider threats (including service providers); 3.1.3 File Access: unauthorized access to data in files, offline database (DB) files, backups and copies of files, both at rest and in transit; 3.1.4 DB Data Access: unauthorized access to data in DBs that are online via DB connections, including, but not limited to, exploited applications.

#	Std	Changes



3.2 Storage Encryption types are classified into tiers which mitigate the risks outlined in 3.1 as follows:

	UNAUTHORIZED ACCESS RISK MITIGATION			
ENCRYPTION TIER	**Access Due to Physical Theft**[1]	**Filesystem Access**	**File Access**	**DB Data Access**
Tier 0 Encryption - no encryption	NO	NO	NO	NO
Tier 1 Encryption - full disk, device-level and media-level Encryption	YES	NO	NO	NO
Tier 2 Encryption - full volume Encryption[2]	YES	NO	NO	NO
Tier 3 Encryption - file-level Encryption or transparent database engine Encryption	YES	YES	YES	NO
Tier 3+ - application-level database Encryption[3]	DB ONLY	DB ONLY	DB ONLY	YES

[1] Theft refers to the theft of Mobile Storage Devices/Media, or a file containing a virtual disk, partition, or volume.

[2] Where possible, all volumes on a disk must be encrypted. Data must be stored in an encrypted volume to be protected from physical theft.

[3] Does not mitigate against the risk of files stored outside of the database. Applications may not encrypt all fields or tables when using application-level database Encryption, each implementation needs to be assessed for risk appropriate at-rest Encryption.

Section 4, Key Management

- **S4.1** (Modified)**: Minor changes to improve conciseness/clarity**
    - 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 should be performed with automated software. ~~A Key management plan must also be in place that covers the following process areas:~~
- **S4.2** (Modified):
    - (Moved from 4.1) A Key management plan must also be in place that covers the following process areas:
    - **Key Generation:** Updated to include process requirements for both software-generated and manually generated keys
    - **Key Storage and Protection:** Process requirements updated to include bullet that keys should be stored with UBC (and not the vendor) unless not technically possible.
    - **Key Recovery:** Process Requirements adjusted to remove reference to central Key Escrow services (now retired)

Editorial Updates

- All standards revised to refer to new (Capitalized) Glossary terms
- All standards revised to use “where possible” or “where technically possible” as opposed to “where feasible”.
- Additional examples (passphrases/passwords, keys) added to Very High Risk Information (U1 and Glossary)
- Links to Services added

Resource Updates

#	Resource	Status
U1	Sample Inventory	Updated
U3	Managing Multiple Email Accounts Guidelines	New (to be published mid-March)
U3	UBC Email Auto-forwarding Agreement	New
U4	Securing and Preserving Electronic Evidence Guideline	Updated
U5	Case Studies in Encryption Requirements	New
U9	Service Provider Security Checklist	Updated
M1	Variance Request Form	Pre-existing, now linked from Standard
M7	Key Escrow Guideline	Updated

New Glossary Terms

Term	Description
Auto-forwarding	***Auto-forwarding***, in the context of email, refers to the automatic process of redirecting incoming emails from one email account to another. This feature allows all or certain specified emails to be forwarded to a different email address without manual intervention. It is often used to consolidate multiple email accounts into one inbox.
Cybersecurity Incident	A ***Cybersecurity Incident*** includes events where there is suspicion that: • Confidentiality, integrity or availability of UBC Electronic Information or Systems has been compromised • Computer systems or infrastructure has been attacked or is vulnerable to attack
Encryption (+Tiers)	***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. UBC defines multiple tiers of encryption as follows: ***Tier 0 Encryption*** - no encryption ***Tier 1 Encryption*** - full disk, device-level and media-level encryption ***Tier 2 Encryption*** - full volume encryption ***Tier 3 Encryption*** - file-level encryption or transparent database engine encryption ***Tier 3+ Encryption*** - application-level database encryption
IT Infrastructure	***IT Infrastructure*** is the group of technologies and components that make up an organization’s IT environment that support the delivery of business systems and IT-enabled processes. Various types of IT Infrastructure include network infrastructure, wi-fi infrastructure, storage infrastructure, etc.