PRIVACY MATTERS
@ UBC

ISS Review – Phase II

Summary of Changes

LAST UPDATED: 29 JANUARY 2021

THE UNIVERSITY OF BRITISH COLUMBIA

TABLE OF CONTENTS

1. Renumbering the standards
2. Overview of standards reviewed in Phase II
3. Summary of changes
4. Glossary updates

RENUMBERING THE STANDARDS

User Standards

- Prefixed with ‘U’

Management and Technical Standards

- Prefixed with ‘M’

Standard #	Legacy #	Standard
STANDARDS FOR ALL USERS		
U1	#01	Security Classification of UBC Electronic Information
U2	#02	Password and Passphrase Protection
U3	#03	Transmission and Sharing of UBC Electronic Information
U4	#04	Reporting Information Security Incidents
U5	#05	Encryption Requirements
U6	#06	Working Remotely
U7	#07	Securing Computing and Mobile Storage Devices/Media
U8	#08	Destruction of UBC Electronic Information
U9	#09	Outsourcing and Service Provider Management
U10	#10	Accessing Electronic Accounts and Records
U11	NEW	Securing Internet of Things (IoT) Devices
MANAGEMENT AND TECHNICAL STANDARDS		
M1	#21	Requesting Variances from Information Security Standards
M2	#11	User Account Management
M3	#12	Privileged Account Management
M4	#13	Securing User Accounts
M5	#14	Vulnerability Management
M6	#15	Security of Wi-Fi Infrastructure
M7	#16	Cryptographic Controls
M8	#17	Logging and Monitoring of UBC Systems
M9	#18	Physical Security of UBC Datacentre
M10	#19	Internet-Facing Systems and Services
M11	#20	Development and Modification of Software Applications

STANDARDS REVIEWED (FULL REVIEW)

- Std U6 (#6), Working Remotely
- Std U11, Securing Internet of Things (IoT) Devices *(new)*
- Std M3 (#12), Privileged Account Management
- Std M5 (#14), Vulnerability Management *(also published in Phase I)*
- Std M6 (#15), Security of Wi-Fi Infrastructure *(formerly Wireless Networks)*

STANDARDS REVIEWED (PARTIAL REVIEW)

- Std U3 (#3), Transmission and Sharing of UBC Electronic Information *(also published in Phase I)*
- Std U5 (#5), Encryption Requirements *(also published in Phase I)*
- Std U7 (#7), Securing Computing and Mobile Storage Devices/Media
- Std U8 (#8), Destruction of UBC Electronic Information
- Std U9 (#9), Outsourcing and Service Provider Management
- Std M4 (#13), Securing User Accounts
- Std M8 (#17), Logging and Monitoring of UBC Systems
- Std M11 (#20), Development and Modification of Software Applications

GLOSSARY UPDATES

- Devices *(updated to accommodate new IoT Devices term)*
- Direct Attached Storage (DAS) *(new)*
- ERPs *(formerly Core Systems, also updated to include EMMS)*
- Internet of Things (IoT) Devices *(new)*
- Personal Health Information (PHI) *(new)*
- Principle of Least Privilege *(new)*
- Privileged Access Management (PAM) *(new)*
- Technical Owner *(new)*
- UBC Systems *(updated to accommodate new IoT Devices term)*
- Work Remotely *(removed) – term defined (with examples) in ISS U6 (#6), Working Remotely*

SUMMARY OF CHANGES

Formatting Updates *(applies to all standards)*

- Renumbered the standards *(U# for User Standards, M# for Management and Technical Standards)*
- Updated document numbering (1, 1.1, 1.1.1)
- Fixed broken links to resources
- Ensured ISS Glossary terms are highlighted
- Changed ‘Related Documents’ heading to ‘Related Documents and Resources’, and added links to referenced standards and websites (in order of reference)

PHASE I

PARTIAL REVIEW

U3 (#03), TRANSMISSION AND SHARING OF UBC ELECTRONIC INFORMATION

- **S3.1** – Revision to accommodate new UBC file sharing, messaging and collaboration tools
- ★ **S3.2** – NEW – Clarification added for Acceptable Methods of Transmitting and Sharing UBC Electronic Information
  - It reads, “Section 3.1 does not prevent the use of UBC scanners/copiers to scan documents and email them to UBC email accounts regardless of the classification of the information in those documents.”
- **S3.4/5** – Added clarifying language
- **S3.5** - Q9 Datacentre (Kamloops) added as an authorized backup location
- **S4.1.3** - Added link to Policy GA4, Records Management *(formerly Policy 117)*
- *Additional community feedback (2 items) will be reviewed in a future phase.*

U5 (#05), ENCRYPTION REQUIREMENTS

- **S1.1** – Scope adjusted
  - **CURRENT:** […] This document defines standards that Users must comply with for encrypting Devices and files to safeguard UBC Electronic Information when they are accessing it for University Business purposes. […]
  - **NEW:** […] This document defines standards that Users must comply with for encrypting Devices and files used to access or store UBC Electronic Information so that the information is protected from unauthorized access. […]

U5 (#05), ENCRYPTION REQUIREMENTS

- **S3.1** – Language updated to match Section 1.1, and better align with language used in Oct 2018 encryption mandate.
  - **CURRENT:** Encryption requirements apply to devices, whether UBC-supplied or personally-owned, that are used for University Business. Wherever possible, encryption should be implemented at the Device level, as follows:
  - **NEW:** Encryption requirements apply to Devices, whether UBC-supplied or personally-owned, that are used to access UBC Electronic Information and Systems. Encryption must be implemented as follows:

U5 (#05), ENCRYPTION REQUIREMENTS

- **S3.1** (TABLE)
  - Removed ‘Mobile Devices’ and ‘Stationary Devices’ headings from table.
  - ★ Updated Device-Level Encryption Requirements to require full disk encryption on desktop computers (regardless of security classification of information on the computer).
  - Updated list of “Third party servers that have an equivalent level of security to the Physical Security of UBC Datacentres” to not include AWS Canada.
    - This is to remove cloud-based servers (AWS/Google/Azure) from the accepted Datacentre list because we need to change requirements for servers in the cloud to be encrypted.
  - Under Third party servers, specified ‘Compute Canada HPC’, rather than just Compute Canada

U5 (#05), ENCRYPTION REQUIREMENTS

- **S3.1** (TABLE, cont’d)
  - ★ Updated Device-Level Encryption Requirements for “Other Servers than listed above” to require full disk encryption. (Previously, it was required for servers containing High or Very High Risk Information only.)
    - This is the new addition for encryption of servers in the cloud. The desire is to require encryption for servers including IaaS, PaaS and SaaS.
  - Removed references to UBC IT’s Encryption Service
  - For **Other servers**, added reference to new ‘Cloud-Based Encryption Requirements’ section.

PHASE I

PARTIAL REVIEW

U5 (#05), ENCRYPTION REQUIREMENTS

- **S3.5** - Specified “UBC IT” as owner of Encryption Service. Revised to note that users must provide a written confirmation of the encryption status and method (e.g. encrypted with BitLocker) at the time of loss or theft, and that University IT Support Staff may be able to assist in providing that information.

★ **S4** – **NEW** – Added new ‘Cloud-based Encryption Requirements’ section

  - Includes reference to virtual servers (e.g. AWS Canada and IaaS), object-based storage (e.g. AWS S3 bucket), SaaS and PaaS.

PHASE I

PARTIAL REVIEW

U5 (#05), ENCRYPTION REQUIREMENTS

- **S5 (formerly S4):**
  - Added 'a securely mounted directory in the UDC, e.g. TeamShare or Home Drive' to list of acceptable options.
  - Modified 4.2.2. (now 5.2.2.) to note that M/H/VH risk information must be stored in one of the listed options (vs. an encrypted area on their Device).
- ★ **S6** – **NEW** – Added new ‘Encryption of Direct Attached Storage (DAS)’ section, with associated DAS glossary term and ‘Encryption Exemption for Direct Attached Storage with Low Risk Information’ checklist.
- *Additional community feedback (1 items) will be reviewed in a future phase.*

U6 (#06), WORKING REMOTELY

- **S1.1/1.2** – Expanded to clarify scope of ‘working remotely’, with examples to accommodate the complexity/variety of situations
- **S1.3** – Moved to separate list item, added reference to Encryption Requirements standard (new encryption requirements for desktop computers)
- **S2** – Revised Secure Access Methods to reflect updated recommendations (e.g. VPN/SSH preferred over VDI)
- ★ **S3** – **NEW** – Added Supplemental Guidance for Personally-owned Workstations section, including encryption requirements and securing home networks.
- **S5.1/5.2** – Updated with more explicit information about collaborator owned devices, and clarified language
- **S6** – Added new ‘UBC IT Guide to Working Off Campus’ resource

PARTIAL REVIEW

U7 (#07), SECURING COMPUTING AND MOBILE STORAGE DEVICES/MEDIA

- **S2** – Electronic Security
  - Updated “Screensaver Locks” row heading to include Idle Timeout, and added clarifying language for Servers and Computing Devices (console/user interface).
  - ★ **NEW** - To accommodate new required cybersecurity controls (as per Executive Mandate April 2020), added new rows for Endpoint Detection and Response (EDR) and Automatic Blocking of Malicious Websites (DNS firewall protection).
  - Changed 'Antivirus & Spyware' row heading to 'Malware and Spyware Protection‘ *(aligned with UBC IT Malware Protection page)*.
- *Submitted community feedback (8 items) will be reviewed in a future phase.*

PARTIAL REVIEW

U8 (#08), DESTRUCTION OF UBC ELECTRONIC INFORMATION

- Revisions to accommodate records retention consideration:
  - **S1.2** – Clarified that standard applies to Users, including Information Stewards/Owners.
  - **S2.1** – Updated from "Users should only retain information as long as required" to "...as long as needed or required by policy, legislation or agreement."
  - **S2.2** – Updated to include Devices taken with a User upon leaving the University (with authorization from Administrative Head of Unit).
  - **S3.3** – **NEW** – Additional section that reads, "This does not apply to collaborations with other research institutions for research purposes where a data retention agreement is in place."
- **S5.3** – **NEW** – Under Special Cases, added section for IoT Devices
- *Submitted community feedback (1 item) will be reviewed in a future phase.*

PARTIAL REVIEW

U9 (#09), OUTSOURCING AND SERVICE PROVIDER MANAGEMENT

- Renamed, formerly ‘Outsourcing and Service Provider Access’
- **S1.1** – Added clarification that “This standard is not intended to cover collaborations with other research institutions for research purposes.”
- **S2.1** – Updated language to indicate that Service Providers must complete the Security Risk Assessment checklist before they provision software for University Business; Updated the checklist (related resource)
- ★ **S2.2** – **NEW** – Added requirement to complete a PIA if Personal Information is involved before Service Providers provision software applications or are granted access to UBC Electronic Information and Systems.
- **S6.1** – Adjusted to require Service Providers to store UBC Electronic Information in a “logically separated environment” vs. a “separate system or database”.
- *Submitted community feedback (4 items) will be reviewed in a future phase.*

NEW FULL REVIEW

U11, SECURING INTERNET OF THINGS (IOT) DEVICES

- Developed using OWASP recommendations
  - "OWASP Top 10 Things to avoid when building, deploying, or managing IoT systems"
- **Sections:**
  - Introduction
  - IoT Device Risk
  - Physical Security
  - Electronic Security
  - Network Security
  - Hardening Requirements
  - Requirements for Merchant Systems
  - Logging and Monitoring Requirements
  - Loss Reporting Requirement

M3 (#12), PRIVILEGED ACCOUNT MANAGEMENT

- **S1.3 (and related)** – Revised who is responsible for compliance from ‘Information Steward/Owner’ to ‘the Administrative Head of Unit, in consultation with the Technical Owner of the UBC System’ *(new Glossary term for Technical Owner)*
- **S2.1** – Added ‘Named’ vs ‘Unnamed’ distinction to the table
- **S4** – Renamed ‘Protecting Privileged Account Passwords’ to ‘Protecting Privileged Account Passphrases, Passwords and SSH Keys’
  - **S4.3** – **NEW** – Added section to accommodate SSH Keys

★ **S4.3** – For ‘Passwords for Unnamed Privileged Accounts’, added PAM requirement *(new Glossary term)*

- **S7.4** – Revised to include “all IT professionals” as needing to comply with the Sys Admins’ Code of Ethics

PARTIAL REVIEW

M4 (#13), SECURING USER ACCOUNTS

- **S2** – Renamed “Account Protection Requirements” from “Password Protection Requirements”
- ★ **S2.3** – NEW – Addition of expiration timelines for account activation and password reset links, and temporary passwords.
- ★ **S3.4** – NEW – Addition of timeout specification for authenticated application sessions. Specifically, Users must reauthenticate to continue an existing session or establish a new session:
    - 3.4.1 after a maximum session length of 12 hours; and
    - 3.4.2 where reasonable, after 30 minutes of User inactivity.
- *Submitted community feedback (8 items) will be reviewed in a future phase.*

M5 (#14), VULNERABILITY MANAGEMENT

- **S1.1** – Added reference to vulnerability mitigation
- **S1.3** – NEW - Notes that all University IT Support staff with access to Privileged Accounts, and all IT professionals must comply with the System Administrators' Code of Ethics
- **S2,** Patch Management – Reordered list items
- **S2.2** – Added link to the Vulnerability Awareness and Patching Prioritization guide
- **S2.5** – Updated language to accommodate CVSS ratings; added Critical-Severity Vulnerabilities and adjusted recommended patch timing for each severity level
- **S2.6** – Revisions to accommodate new IoT standard; added reference to virtual appliances
- **S5.4** – NEW - Notes that applications should be appropriately hardened against attacks. Includes reference to Mozilla Observatory.

FULL REVIEW

M6 (#15), SECURITY OF WI-FI INFRASTRUCTURE

- Renamed, formerly ‘Wireless Networks’
- **S1.2** – Updated those with responsibility for ensuring compliance to “UBC IT Network and Infrastructure Team”
- **S2**, Deployment of WAPs – section renamed from ‘Physical Protection’, added new “All deployment of WAPs must be authorized by UBC IT” list item.
- **S3**, Secure Configuration – Updated to recommend a *minimum* of WPA2
- **S4.2** – Notes that WAPs and wireless controllers must be replaced if they have reached end of life for software support
- **S5** – renamed from ‘Additional Wireless Requirements for Payment Card Industry (PCI) Information’ to ‘Additional Requirements for Merchant Systems’ *(consistent with other standards)*

PARTIAL REVIEW

M8 (#17), LOGGING AND MONITORING OF UBC SYSTEMS

- **S2.3.1** – Modified to require that logs for ERPs be retained for at least 365 days.
- *Submitted community feedback (3 items) will be reviewed in a future phase.*

PARTIAL REVIEW

M11 (#20), DEVELOPMENT AND MODIFICATION OF SOFTWARE APPLICATIONS

★ **S5** – NEW – Added Naming Requirements for Web Applications section

- 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.

★ **S6** – NEW – Added Email Requirements for Applications and ERPs section

- The inclusion of clickable links in unsolicited emails generated from ERPs is prohibited.
- Use of the svc.ubc.ca managed mail subdomain service is required for all ERPs, e.g. widget.svc.ubc.ca.
- Guidelines to make emails generated from ERPs more difficult to replicate.

- *Submitted community feedback (5 items) will be reviewed in a future phase.*

OTHER MINOR CHANGES

- **ISS U2, Password and Passphrase Protection**
  - **S4.2** – Updated to include that passwords should not be shared with supervisors **or University IT Support Staff**.
- **ISS M2, User Account Management**
  - **S2.1** – Updated to note that applications for User Accounts must be approved by Information Steward/Owners.
  - **S2.6** – Updated sources of record to include new systems, e.g. Workday, PersonHub and other ERPs