PRIVACY MATTERS @ UBC

ISS Review – Phase I

Summary of Changes

LAST UPDATED: 05 OCTOBER 2018

THE UNIVERSITY OF BRITISH COLUMBIA

STANDARDS REVIEWED

User Standards

- #1 Security Classification of UBC Electronic Information
- #2 Password and Passphrase Protection
- #3 Transmission and Sharing of UBC Electronic Information
- #5 Encryption Requirements

Management and Technical Standards

- #14 Vulnerability Management

PRIVACY MATTERS @ UBC

ISS #1 - SECURITY CLASSIFICATION OF UBC ELECTRONIC INFORMATION

Feedback Items: 9

- **S.4 -** Scope statement added to Introduction
- **S.5 -** Updated with different Information Security Classification model (Low, Medium, High, Very High Risk) with examples and potential impact for each
  - Formerly Public, Sensitive, Confidential
  - All standards updated to reflect new terminology
- **S.7 -** Removed requirement for Administrative Head of Unit to maintain inventory of all UBC Electronic Information
  - Instead, Administrative Head of Unit is responsible for knowing the types of UBC Electronic Information under their control, its information security classification and where it is stored
  - Made recommendation to keep inventory of types of records that contain High Risk and/or Very High Risk Information
  - Sample inventory template provided as a Related Document

PRIVACY MATTERS @ UBC

ISS #2 - PASSWORD AND PASSPHRASE PROTECTION

Feedback Items: 11

- **S.5 -** Updated password standards
  - Passphrase required over password (where system allows)
  - 8 character minimum password extended to 10 characters
  - Requirement to change CWL password annually left in place – to be revisited when ability to detect compromised accounts is improved
- **S.12 -** Added recommendation to use a Password Safe
  - Supplementary Password Safe Guideline updated
- Added new sections
  - **S.15 -** Biometric Alternatives (fingerprint readers/facial recognition)
  - **S.16 -** Multi-Factor Authentication

PRIVACY MATTERS @ UBC

ISS #3 - TRANSMISSION AND SHARING OF UBC ELECTRONIC INFORMATION

Feedback Items: 13

- **S.2 -** Clarified scope in Introduction
- **S.9 -** Updated requirements on how to appropriately share UBC Electronic Information using new Information Security Classification
  - Expanded on methods of transmission (e.g. social media)
- **S.10 -** Added section noting that Users are responsible for ensuring that a copy of the UBC Electronic Information that they share using personal accounts is stored on UBC Systems at all times.
- **S.13/14 -** Added information regarding “Email Forwarding from UBC Email Accounts”

PRIVACY MATTERS @ UBC

ISS #5 - ENCRYPTION REQUIREMENTS

Feedback Items: 8

- **S.1 -** Updated encryption requirement to apply to all Devices that access UBC Electronic Information, rather than devices that safeguard Confidential Information
- **S.6 -** Updated Device-Level Encryption Requirements table to include 3rd party servers. Added Device Categorization (Mobile Devices / Stationary Devices)
- **S.10-12 -** Added accommodation for "Encryption of Devices using Operating Systems other than Microsoft Windows and Apple macOS (e.g. Linux)"

PRIVACY MATTERS @ UBC

ISS #14 - VULNERABILITY MANAGEMENT

Feedback Items: 9

- **S.2 –** Clarified scope in Introduction
- **S.5 –** Removed references to specific version of Severity Ratings for Vulnerabilities (CVSS) – changed to 'current version'
- **S.8 –** Updated to indicate that compensating controls must be approved by the CISO (where impossible or impractical to install)
- **S.11 –** NEW. Added that the Office of the CIO is responsible for scanning Web Applications on UBC Systems.
- **S.12 –** Updated to indicate that University IT Support Staff have the responsibility to obtain a vulnerability scan and mitigate vulnerabilities.
- **S.26-27 –** NEW. Added IoT (Internet of Things) Devices sections, making special note that IoT devices must be considered.