PRIVACY MATTERS @ UBC

2021 ISS REVIEW **SUMMARY OF CHANGES**

LAST UPDATED: 27 JANUARY, 2022

TABLE OF CONTENTS

- Changes related to Multi-factor Authentication
- Other revisions, including revisions related to:
  - Endpoint Detection and Response (U7)
  - Patching of critical vulnerabilities (M5)
  - Split tunneling (M10)

TOPIC: MFA

REVISED STANDARDS (MFA-RELATED)

- Glossary
- U2, Passphrase and Password Protection
- U4, Reporting Information Security Incidents
- U6, Working Remotely
- M4, Securing User Accounts
- M10, Internet-facing Systems and Services

TOPIC: MFA

GLOSSARY

- Clarified definition of MFA to specify that access is granted after successfully presenting evidence from 2+ *categories*, not just 2+ pieces of evidence.
  - **Original: *Multi-Factor Authentication*** (MFA) is a method of confirming a user's identity in which a user is granted access only after successfully presenting two or more pieces of evidence. Evidence falls into the categories of something they know, something they have or something they are. MFA Devices are one way to enable a secondary challenge during a Multi-Factor Authentication process.
  - **NEW: *Multi-Factor Authentication*** (MFA) is a method of confirming a user's identity in which a user is granted access only after successfully presenting evidence from two or more of the following categories: something they know, something they have or something they are. MFA Devices are one way to enable a secondary challenge during a Multi-Factor Authentication process.

TOPIC: MFA

GLOSSARY

- Expanded glossary definition for Multi-Factor Authentication (MFA) Devices to include that they are devices or mechanisms used for Multi-Factor Authentication.

Multi-Factor Authentication Devices (MFA Devices) are devices or mechanisms used for Multi-Factor Authentication, including dongles, yubikeys and smartphones with MFA applications.

U2, PASSPHRASE AND PASSWORD PROTECTION

TOPIC: MFA

- Addition of MFA challenge requirement for CWL passphrase/password resets.
  - **NEW S3.1.4** Each time a password/passphrase change or reset occurs, a Multi-Factor Authentication (MFA) Device challenge is required for Campus-wide Login accounts. For all other accounts, it is recommended.
- Expanded recommendation to not respond to emails or phone calls requesting passphrases/passwords to include MFA passcodes.
  - **S4.4** Do not respond to emails or phone calls requesting passphrases/passwords and Multi-Factor Authentication (MFA) passcodes, even if they appear to be from a trusted source. These requests are often attempts to steal Users' credentials.

U4, REPORTING INFORMATION SECURITY INCIDENTS

TOPIC: MFA

- **NEW** – Addition of requirement to report loss or theft of an MFA Device under ‘Incidents That Must Be Reported’
  - **S2.1.1.5** loss or theft of any Multi-Factor Authentication Device (MFA Device)

U6, WORKING REMOTELY

TOPIC: MFA

- Clarified that physical security of devices used to access/protect UBC Electronic Information includes MFA Devices.
  - **S4.1** Reasonable measures must be taken to prevent or reduce the possibility of loss or theft of Devices (including Multi-Factor Authentication Devices) that are used to access or protect UBC Electronic Information
- Highlighted new Remote Access glossary term (added to support revisions to M10).
  - ***Remote Access*** is access of UBC Systems from a non-UBC network or location, e.g. home, hotel or café.

M4, SECURING USER ACCOUNTS

TOPIC: MFA

- **NEW S2.3:** Where technically possible, Servers and Software Applications must be protected by Multi-Factor Authentication (MFA).
- Expansion of Account Protection Requirements section to include procedures to verify the identity of a User prior to providing a new password for an account.
  - **S2.5** Procedures must be established to verify the identity of a User prior to providing a new, replacement or temporary password for an account. Identification validation procedures must follow one of the following standard practices, listed in order of preference:
    - MFA application push to the User's MFA Device that must be approved by the User;
    - Validation of the answers to three questions that were previously created by the User during account creation; or
    - In-person visit by the User to present valid photo identification, preferably University or government-issued.

M10, INTERNET-FACING SYSTEMS AND SERVICES

TOPIC: MFA

- **NEW:** Added new Glossary definition for Remote Access.
  - ***Remote Access*** is access of UBC Systems from a non-UBC network or location, e.g. home, hotel or café.
- Addition of MFA requirements (where possible) for Remote Access.
  - **S3.4** Users frequently access desktops, laptops and servers remotely. Remote Access covers a broad range of technologies, protocols and solutions (e.g. RDP, SSH, VNC, VDI, terminal services, etc.). Remote Access ~~transmissions~~ must comply with the following requirements, where possible:
    - **NEW S3.4.1** Multi-Factor Authentication (MFA) must be used;

PRIVACY MATTERS @ UBC

OTHER REVISIONS

- U7, Securing Computing and Mobile Storage Devices/Media
- M5, Vulnerability Management
- M10, Internet-facing Systems and Services
- U10, Accessing Electronic Accounts of Other Users
- U5, Encryption Requirements
- U8, Destruction of UBC Electronic Information

U7, SECURING COMPUTING AND MOBILE STORAGE DEVICES/MEDIA

- Updated Endpoint Detection and Response (EDR) requirements to align with new mandate from Cybersecurity, where requirement to install is not tied to the security classification of information on the Device.
  - **EDR (Servers):** EDR software approved by the CISO must be installed on all UBC-owned Servers.
  - **EDR (Desktops & Laptops):** EDR software approved by the CISO must be installed on all UBC-owned Workstations, where technically possible.
  - **Malware and Spyware Protection:** 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.

U7, SECURING COMPUTING AND MOBILE STORAGE DEVICES/MEDIA

- **NEW** – Under Electronic Security for **Operating Systems**, added requirement that Workstations be regularly restarted to facilitate patching of vulnerabilities. The recommended frequency for restarting is at least once per week.

M5, VULNERABILITY MANAGEMENT

- Modification to patch window for Critical-Severity Vulnerabilities (48 to 72 hours). Addition of note that patches may necessitate service outages.
  - **S2.5** Unpatched software is frequently exploited by malicious individuals to access information or resources. To mitigate this threat, vendor provided patches for UBC Systems (e.g. operating systems, applications, databases, etc.) must be patched, with service outages where required, in accordance with Severity Ratings for Vulnerabilities (CVSS) or as defined by the vendors or other third parties as follows:
    - **S2.5.1** Critical-Severity Vulnerabilities as soon as possible, preferably within 72 hours of the patch release;

M5, VULNERABILITY MANAGEMENT

- **NEW S3.4** University IT Support Staff must not block UBC's Vulnerability Scanners.
  - Linked to Cybersecurity CC site - https://cc.cybersecurity.ubc.ca/tech-ref/scanners-min/ (CWL login required)

M10, INTERNET-FACING SYSTEMS AND SERVICES

- Modification to clarify acceptable use of split tunneling for VPN connections.
  - **S3.4.4** *(formerly 3.4.3)* VPN connections must be encrypted and restricted at both ends to the minimum number of systems necessary~~; split tunneling must not be enabled~~. To support this:
    - DNS or service-based split tunnelling (e.g. Dynamic Split Tunnelling) may be used with authorization of specific services by the CISO;
    - IP or subnet-based split tunneling must not be enabled; and
    - Local LAN access may be enabled with authorization by the CISO.

U10, ACCESSING ELECTRONIC ACCOUNTS OF OTHER USERS

- Modifications to title and Introduction section of standard in order to clarify the scope.
  - **Title:** Changed from “Accessing Electronic Accounts and Records” to “Accessing Electronic Accounts of Other Users”
  - **S1.1** This document defines standards that Users (typically supervisors and investigators) must comply with to gain access to electronic accounts of other Users on UBC Systems, such as UBC email accounts, UBC file sharing, collaboration and messaging accounts, Home Drive, voicemail accounts, internet usage records and telephone logs.
  - **NEW - S1.2** This standard does not apply to electronic accounts that are not owned by individual Users, such as building access logs or shared email accounts.

U5, ENCRYPTION REQUIREMENTS

- Updated language to make consistent across sections.
- Updated Recommended Toolset for Device-Level Encryption of Smartphones, tablets and PDAs, and removed outdated ‘Encrypting Mobile Devices’ guideline document.

U8, DESTRUCTION OF UBC ELECTRONIC INFORMATION

- Update to Acceptable Data Destruction Methods, removal of reference to “Secure Erase” utility
  - S4.1 Any of the following are acceptable methods of data destruction:
    - using a software utility, ~~such as Secure Erase,~~ that erases by overwriting or encrypting the data;
    - magnetically erasing (degaussing) the data;
    - formatting a Device after encrypting it in compliance with the Encryption Requirements standard; or
    - using a machine that physically deforms or destroys the Device to prevent the data from being recovered.