Bring Your Own Device and Personally Managed Device Standard

Version: 1.0
Published: July 9, 2021
Published By: Information Security Office, Information Services
Approved By: ISET
Approval Date: April 21, 2021

1. Introduction

The University of Regina recognizes the requirement and benefit brought by the use of personally owned and managed devices for purposes of your work role, which is known as 'bring your own device' (BYOD).

This document is intended to provide direction for using personally owned and managed devices when processing University data to reduce risk in BYOD scenarios. Risks associated with BYOD usage may include being lost, stolen, or used in such a way as to exploit the device owner or the University.

The University is obligated to protect data in its care. When individuals use personally owned or managed devices as a work tool, they are required to maintain the security of the University data on these devices. Moreover, implementing these requirements will help ensure that personal data processed on personally owned or personally managed devices are also protected.

This information security standard provides the requirements for processing University data when using personally owned or personally managed technology.

The requirements prescribed to the device owner or manager depend on the sensitivity of the processed data by the personally owned or personally managed device. The security standard requirements are therefore more rigorous as data sensitivity increases.

2. Scope

This standard applies to all:

- Employees,
- volunteers, information management service providers, independent contractors and agents engaged by a department who process University data

Where a personally owned or personally managed device such as smartphones, tablet and desktop computers, laptops, and similar equipment is used to process University data.

3. Definitions

- *Bring your own device (BYOD)* – the use of personally owned devices to undertake University work or process University data.
- *Personally Owned Device* – A device owned by an employee and not purchased with University funds.
- *Personally Managed Device* – A device that may be owned by the University but is not managed by the University. For example, devices procured with APEA funds or research funds but are not centrally maintained by Information Services or Departmental Information Technology

Administrators are considered personally managed - excludes systems managed under the Evergreen program.

- *Employee* - A person who receives a University salary for full-time or part-time work or services normally performed by an employee, including a person currently on an employment leave.
- *Low Risk Information* – Information that presents no risk to the University in accordance with the Information Classification Framework.
- *Moderate Risk Information* – Information that presents a risk to the University but not High Risk in accordance with the Information Classification Framework.
- *High Risk Information* – Information that presents a significant risk to the University in accordance with the Information Classification Framework.
- *University Data* – Materials, records, documents, communications, and information processed during duties, employment, or work for the University or on its behalf will have a Data Trustee at the University, regardless of device ownership or device management responsibilities.
- *Process Data* – Obtaining, accessing, recording, storing, sharing, modifying, or deleting of data.
- *Data Trustee* – Highest ranking position responsible for data within a domain at the University.

4. Standard

4.1. Requirements for Personal Device Use with Data Sensitivity Classification Low

Users of personally owned or personally managed devices that use data classified as low sensitivity are required to comply with all items contained in section 4.1.

4.1.1. Whenever feasible, University owned and managed systems should be used to perform employee's job-related duties and processing University data.

4.1.2. When 4.1.1 is not feasible, and University data is required to be processed via a personally owned or managed device, University provided remote access or web interfaces are preferred access methods. For example, rather than saving data to your personally owned or managed system, processing data on University owned systems via remote access is preferred. Examples include VPN and Remote Desktop services (remote access mechanism) or FILR for file access (web interface).

4.1.3. Devices are required to be configured to automatically lock after a period of inactivity no longer than 30 minutes.

4.1.4. Devices are required to be configured with authentication (PIN, Password, Fingerprint, or facial recognition) to start and unlock the device.

4.1.5. Devices are required to be kept up to date using the software vendor's update service. Devices that are no longer under support from the vendor, such that they no longer receive software/security updates, should not be used for University purposes.

4.1.6. Devices that have had manufacturer's security mechanisms disabled (i.e. jailbreak, or rooted) are not be used for University purposes.

4.1.7. Antivirus software is required for laptops and desktops which run Windows. Antivirus software is recommended for smartphones, tablets, Apple computers, and Linux computers.

4.1.8. Device backups are to be securely stored and password protected.

4.1.9. Utilizing only secure, encrypted wifi is recommended. Avoid the use of insecure, unencrypted public wifi.

4.2. Requirements for Personal Device Use with Data Sensitivity Classification Moderate

Users of personally owned or personally managed devices that use data classified as moderate sensitivity are required to comply with all items contained in sections 4.1 and 4.2.

4.2.1. The loss or theft of a personal device that contains University data, or where you believe that the device has been accessed by an unauthorized person or otherwise compromised should be reported as an information security incident (https://www.uregina.ca/is/security/reporting-is-incident.html).

4.2.2. If your device supports remote wipe and location tracking, this feature is to be enabled. If your device is lost or stolen and cannot be recovered, a remote wipe is required.

4.2.3. If the device is retired/replaced, assigned a new owner, or an owner is no longer an employee of the University, the owner must securely delete all University information from the device and device backups. A factory reset is recommended.

4.2.4. If other members of your household, family, or friends use your device, ensure they cannot access University information. For example, ensure they use an additional account on the device with a different account passcode. Any additional accounts cannot be administrative accounts or have ability to access other accounts, which are used for processing University information.

4.2.5. Personal devices shall not be the source of authoritative data. For example, where the master copy of a record is held in an electronic form, it should be stored on University approved servers or services and not on a personal device.

4.2.6. Do not use non-authorized third party, cloud, or personally provisioned storage services for University data that is considered sensitive (moderate or higher data classification). For example, do not use Dropbox, iCloud, OneDrive. Rather, University approved and supported applications such as FILR for storage are required.

4.2.7. Processing of University data is required to be associated with a University account and not personally provisioned accounts (i.e. Gmail).

4.2.8. Utilizing only secure, encrypted wifi is required. If using unencrypted or public wifi, University of Regina VPN must be utilized while processing University data to ensure traffic is secure and encrypted.

4.3. Requirements for Personal Device Use with Data Sensitivity Classification High

Users of personally owned or personally managed devices that use data classified as high sensitivity are required to comply with all items contained in sections 4.1, 4.2, and 4.3.

4.3.1. Devices which store or access data classified as high sensitivity cannot be shared devices. Members of your household, family, or friends cannot use this device. The device owner is to be the sole user and administrator of the device. This requirement supersedes 4.2.4.

4.3.2. Personally owned devices storing data classified as high sensitivity must store the data in an encrypted manner.

4.3.3. Data classified as high sensitivity being processed via a personally owned or managed device should be an extremely limited use case. All reasonable efforts to avoid this situation should be undertaken. Such a case should be reviewed with your manager or Information Services.

4.4. The University may request that personally owned or managed devices be utilized as a second factor of authentication where multifactor authentication is in use on University systems and applications.

4.5. The University will not monitor the content of personally owned devices. However, the University reserves the right to log traffic between your device and University systems. This logging may be monitored to ensure authorized use as per the Use of Computer and Network Systems (Policy OPS-080-005).

Exceptions

Exceptions to this standard require written approval by the AVP Information Services or designate.

In determining whether an exception is warranted, consideration will be given to any comparable security measures in place or mitigating controls used to manage information security risks in a manner consistent with the intent of this standard.

Related Information

- Use of Computer and Network Systems Policy OPS-050-035
- Classification of Information by Risk Policy OPS-080-XXX (Authorizing Policy)
- Information Classification Framework

Revision History

Version	Version Date	Status	Summary of Change	Author
0.1	March 12, 2021	Draft	Initial Draft	R. Jesse
0.2	March 15, 2021	Draft	Changes from IS Communications	R. Jesse
0.3	March 24, 2021	Draft	Contributions from M. Haidl, A. Exner	R. Jesse
0.4	April 19, 2021	Draft	Editorial	R. Jesse
1.0	April 21, 2021	Final	ISET Approval	R. Jesse