a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U11
Securing Internet of Things (IoT) Devices

1. Introduction

1.1 Internet of Things (IoT) Devices pose special risks and must be assessed to ensure that they do not put UBC Electronic Information and Systems at risk.

1.2 This standard defines the minimum security requirements that Users must comply with to protect these Devices throughout their lifecycle. University IT Support Staff, including staff in the IT Service Centre, are available to assist Users in implementing these requirements where necessary.

1.3 All IoT Devices used for University Business—no matter whether they are owned by the University, by the User, or by a third party—need to be protected from theft of the device and/or unauthorized access to UBC Electronic Information and Systems.

1.4 This standard is meant to cover only IoT Devices, including but not limited to:

1.4.1 Devices used for remote automation and/or monitoring (e.g. controllers, sensors, HVAC systems);

1.4.2 network-connected imaging Devices (e.g. scanners, printers, webcams, multi-function devices);

1.4.3 Devices with network-connected controllers (e.g. medical devices, scientific instruments, industrial control systems, PLCs);

1.4.4 “Smart” Devices or appliances (e.g. speakers, TVs, lightbulbs, refrigerators, doorbells, IoT bridges and hubs);

1.4.5 single board computers (SBCs) (e.g. Raspberry Pis, Arduinos, Tinkerboards), when not configured as Mobile Devices, Servers or Workstations; and

1.4.6 if there is any doubt about whether or not a Device is covered, consult the CISO.

1.5 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. IoT Device Risk

2.1 Users must take a risk-based approach to securing IoT Devices based on the UBC Electronic Information that the Device stores or has access to. Consideration must be given to:

2.1.1 what information can be collected, accessed or stored, e.g. what can be listened to, seen or captured through audio or imaging;

2.1.2 what other Devices (including sensors) the IoT Device is connected to;

2.1.3 what Devices or systems can be controlled, e.g. temperature of a research sample fridge or control of a power system;

2.1.4 where the IoT Device is physically located; and

2.1.5 whether the Device is integral to University Business.

2.2 Users must minimize the risk to UBC as much as possible by capturing the least amount of data required for the operation of the IoT Device. For example:

2.2.1 reduce camera field of view to only capture the minimum required area, or disable camera when not required;

2.2.2 ensure IoT Devices that capture audio are located or configured such that they won’t capture unintended audio or conversations (including voice recognition commands that could be issued by unauthorized personnel); and

2.2.3 disable or remove any sensors that are not required.

2.3 IoT Devices that capture video images must also be in compliance with Policy SC16, Safety and Security Cameras.

2.4 When deploying IoT Devices, the security classification of information collected and transmitted must be identified. The Device must be assessed to determine if any UBC Electronic Information is being transmitted, and to what location(s).

2.4.1 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.

2.4.2 IoT Devices that store Medium, High or Very High Risk Information on third party systems must have a copy of this information stored on UBC Systems at all times.

3. Physical Security

3.1 Based on IoT Device risk, the following physical security measures should be taken to protect IoT Devices against theft, alteration or misuse. Consideration should be given to removable components of IoT Devices, e.g. memory cards, batteries.

3.1.1 Where possible, unattended IoT Devices must be located in a room or other enclosed space (e.g. cabinet or other fixed container such as a server cabinet/cage) that is alarmed, locked and/or otherwise accessed-controlled.

3.1.2 Keys or swipe cards giving access to IoT Devices must be limited to authorized individuals.

3.2 To prevent unauthorized access, all physical interfaces to IoT Devices (e.g. USB, serial or Ethernet ports) must be secured against unauthorized physical access.

4. Electronic Security

4.1 All interfaces (e.g. mobile applications, web applications, APIs) to IoT Devices must be configured based on the Principle of Least Privilege and secured where necessary.

4.2 All control interfaces used to configure IoT Devices must be secured against unauthorized access and changes.

4.3 Passwords and passphrases used with IoT Devices must be in compliance with UBC's Passphrase and Password Protection standard (e.g. not weak, re-used, pre-defined or hardcoded). These include passwords and accounts used for third party vendor accounts (e.g. Facebook, Google, Apple), and for IoT Device firmware and applications used to manage them.

4.3.1 Where a hard-coded password exists, the risk must be mitigated with compensating controls approved by the CISO.

4.4 To facilitate restoration of services dependent upon IoT Devices, a backup of the configuration of IoT Devices should be maintained in a secure location. Examples of backups include screenshots or exports of configuration details, or configuration scripts.

4.5 IoT Devices that store Medium, High or Very High Risk Information must be regularly backed up to a secure location and checked periodically (preferably quarterly) to ensure the integrity and availability of the information such that it can be restored. See the Backup guideline.

4.6 Where possible, enable features that will allow the IoT Device, including data and configuration, to be remotely erased in the event of loss or theft.

5. Network Security

5.1 All network traffic to or from IoT Devices must be secured against unauthorized access, in compliance with the Transmission and Sharing of UBC Electronic Information standard.

5.2 Interference with other University wireless networks must be managed in compliance with Policy SC11, Management of the Wireless Network. Wireless Access Points (including extenders/repeaters) used to facilitate connectivity for IoT Devices must also be in compliance with Policy SC11.

5.3 If the only traffic an IoT Device delivers over TCP/IP networks is publicly-accessible or Low Risk Information then the IoT Device must be secured in compliance with the Internet-facing Systems and

Services standard. This includes IoT bridges and hubs, such as Zigbee, Z-Wave, Bluetooth and other non-TCP/IP devices that are connected to TCP/IP networks.

5.4 All other TCP/IP network-connected IoT Devices (including IoT bridges and hubs) must only be internet accessible via a Virtual Private Network (VPN) unless an exception has been approved by the CISO.

6. Hardening Requirements

6.1 To prevent unauthorized access, pairings or connections, IoT Devices must not be left in set-up, reset or pairing mode.

6.2 Unless required for the function of the Device, IoT Devices must not be left in Bluetooth Discovery Mode.

6.3 Prior to being deployed in production, default settings of IoT Devices must be reviewed to ensure insecure configurations have been remediated.

6.4 Unneeded or insecure network services running on IoT Devices must be disabled.

6.5 Unneeded physical and wireless interfaces on IoT Devices must be disabled where possible.

6.6 IoT Devices must not use weak or unencrypted protocols for data transmission anywhere within the ecosystem, including at rest, in transit, or during processing.

6.7 Operating system, firmware and software on IoT Devices must be updated to address IT vulnerabilities in compliance with the Vulnerability Management standard. Following every update, the implications of changes must be assessed to ensure the device is still secure.

6.8 Operating system, firmware and software updates to IoT Devices must be controlled so that all updates are automated where possible, or only delivered by authorized personnel. Updates should be made in a secure manner, using secure mechanisms where possible. Examples of secure mechanisms are:

6.8.1 update is signed and signature-verified;

6.8.2 update is delivered to the Device through an encrypted communication channel;

6.8.3 update is manually transferred to the Device by an authenticated administrator only; and

6.8.4 update is received only from a vendor-authorized site.

6.9 Deprecated or unsupported hardware must be replaced, or compensating controls approved by the CISO must be implemented.

6.10 UBC Electronic Information on IoT Devices must be destroyed and/or sanitized before the device is decommissioned, in compliance with the Destruction of UBC Electronic Information standard.

6.11 Any customization of the operating system or firmware of an IoT Device not performed by the manufacturer must be in compliance with the Development and Modification of Software Applications standard.

7. Requirements for Merchant Systems

7.1 Point of Interaction (POI), e.g. PIN pad, Unattended Cardholder-Activated Terminal (UCAT), and other IoT Devices must not be used in Merchant Systems without authorization from the UBC PCI Compliance Working Group.

8. Logging and Monitoring Requirements

8.1 IoT Device logs should be captured and monitored in compliance with the Logging and Monitoring of UBC Systems standard where possible.

8.2 Based on section 2, IoT Device Risk, IoT Devices must be:

8.2.1 monitored for availability and checked for unusual behavior or performance to ensure a timely and appropriate response; and

8.2.2 recorded in an inventory, maintained by the User and provided to University IT Support Staff prior to going into production. Refer to the sample inventory attached to this standard. At a minimum, the inventory should contain the Device make, model, serial number (or other method of unique

identification), description, associated service(s), location, technical contact and security classification of information collected. Where applicable, include the following:

8.2.2.1 radio frequency bands in use, e.g. 900 MHz, 2.4 GHz, 5.4 GHz; and

8.2.2.2 active over-the-air modes and protocols, e.g. LoRa, Z-Wave, Zigbee, Thread.

9. Loss Reporting Requirement

9.1 Users who lose an IoT Device used for University Business (no matter who owns the IoT Device) or suspect that there could have been an unauthorized disclosure of UBC Electronic Information must report the loss/disclosure in accordance with the Reporting Information Security Incidents standard.

10. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Policy SC16, Safety and Security Cameras

Privacy Impact Assessment (PIA)

Passphrase and Password Protection standard

Backup guideline

Transmission and Sharing of UBC Electronic Information standard

Policy SC11, Management of the Wireless Network

Internet-facing Systems and Services standard

Vulnerability Management standard

Destruction of UBC Electronic Information

Development and Modification of Software Applications standard

Logging and Monitoring of UBC Systems standard

Sample Inventory

Reporting Information Security Incidents standard