UNIVERSITY OF SASKATCHEWAN

End-point Security Management Procedure

The end-point security management process helps reduce the likelihood and impact of a security incident by:

- considering the role of the individual using the device (e.g. student, faculty, staff)
- assessing the sensitivity of the data that will be accessed or stored by the end-point device
- determining the consequence of compromise
- identifying threats
- recommending appropriate levels of security controls and safeguards
- determining the reduced residual risk remaining after the controls and safeguards are implemented.

Some standard security controls and safeguards will apply to all end-point devices.

The following scenarios would need to follow the end-point security management procedure. Other activities may also need to follow this procedure.

- Acquisition of network-capable devices such as desktops, laptops, tablets, phones, printers, multimedia equipment, etc. that will be connecting to the University of Saskatchewan network.
- Acquisition of network-focused devices such as door locks, video surveillance, supervisory control and data acquisition (SCADA) systems, internet-controlled appliances, lights or other devices, etc., that will be connected to the University of Saskatchewan network.

Contact the ICT Service Desk at servicedesk@usask.ca or your local IT support personnel to start the end-point security management procedure. The process is summarized in the three-steps below:

1. **Acquisition of Network-capable Device or Network-focused Device:**
   For each end-point device acquired, the risk to the university must be assessed to help reduce the likelihood and impact of a security incident caused by a university-owned end-point device.

   a) **Assessment of Role of Individual or System Using the Device**
   The role of the individual or system using the end-point device must be assessed. Individuals or systems with access to more sensitive data will require more security controls and safeguards than those with access to less sensitive data. Systems controlling or mentoring other services including safeguarding the university community's interests.

   b) **Assessment of the Sensitivity of Data Accessed or Stored on Device**
   The data sensitivity must be assessed. There are three types of sensitive data:
   - Any university sensitive data. This is data that if compromised would have implications to the university, its faculty, its staff, its students, or the community.
   - Any personal data, such as personal health information (PHI) or personally identifiable information (PII).

- Any third-party data, such as credit card or payment card information or licensed or copyrighted materials.

For the data being access or stored by the device, consideration must be given to the impact if the end-point device was compromised, including disclosure, loss, modification, corruption, or loss of availability.

2. **Identification of Security Controls and Safeguards for Device**
   Based on the assessed risk, security controls and safeguards for the end-point device will be identified. All end-point devices will need to ensure they have security policies applied, use university credentials, and have their operating systems up to date. This includes the end-point device:
   - has all available security patches applied to its operating system and software
   - is in a secure configuration (administration rights have been set, configured to meet minimum university security requirements, etc.)
   - has known vulnerabilities mitigated through patching or other security methods (i.e., cost effective security controls to prolong service life).

   Additional security controls and safeguards available to mitigate risk for end-point devices that will be used to access, store, monitor, or control sensitive data include restricting the devices to a more secure segmenting of the network to limit exposure, restricting access to the device, or requiring two-factor authorization.

3. **Maintenance of the Security of the Device**
   Once the security controls and safeguards have been implemented, the security of the device must be maintained. This includes continuing to update software and operating systems as patches as new versions are released, ensuring the device maintains its secure configuration and continuing to mitigate known vulnerabilities as new ones emerge.

To start the end-point security management procedure, or if you have questions or comments, contact the ICT Service Desk at servicedesk@usask.ca.