UNIVERSITY OF SASKATCHEWAN

IT Security Incident Response Procedure

The IT Security Incident Response procedure helps to reduce the impact of a security incident by providing a consistent response.

IT security incidents may occur as a result of a variety of scenarios and for a variety of reasons but the primary result to gain access to university resources. Some of the common types of IT security incidents experienced by the university occur as a result of accounts being compromised in the following ways:

- **Phishing**: Sending fake emails that look like they are from the university (or other reputable businesses) that manipulate people to click on links and submit usernames and passwords to harvest account and authentication information.
- **Eavesdropping**: Spying on or intercepting digital communications that are insecure or installing devices that log keystrokes if they can get physical access to a device in order to obtain university account passwords.
- **Guessing:** Using software to manually trying to guess a password through a trial and error process.
- **Hijacking:** Taking over the electronic identity of a member from the university community to intercept or divert account and authentication information.
- **Stealing:** Stealing physical devices and then running software to analyze, extract or tamper with the account and password.

Signs that you may be experiencing an IT security incident or have a compromised account include:

- Your username and password no longer work.
- Files or emails are being deleted.
- People tell you they are getting weird or unexpected emails from you.
- You get replies to emails you did not send.
- Software is being installed unexpectedly.
- Your anti-virus software has been disabled.
- Your device has unexpected popups appearing, runs very slowly, or crashes frequently.
- You cannot access system programs that you normally can access.

If you think you have experienced an IT security incident or have a compromised account, contact the ICT Service Desk at:

- servicedesk@usask.ca
- 306-966-2222
- 1-800-966-4817 (Toll Free in Canada)

The IT security incident process is summarized in the four-steps below:

1. **Identification of IT Security Incident**
   IT security incidents are identified through both preventative and reactive measures.
   - ICT's Security Incident and Event Management (SIEM) system will automatically identify potential instances of compromised accounts based on analysis of suspected irregular activity.

- Any member of the university community may report to the ICT Service Desk or to the university Protective Services department that it suspects or has confirmed that it has an IT security incident.
- Notification from ICT's third-party partners of compromised activity or appearance of a university credential on a hacked site list.
- External parties may notify the university of suspected or confirmed compromise of a university account by contacting the ICT Service Desk or the Protective Services department.

2. **Assessment of Impact of the IT Security Incident**
   Once the IT security incident is identified, the Service Desk and ICT Security, Access and Compliance units assess the impact and scope (i.e., triages) of the incident to the university's information, IT assets and IT systems, and categorizes the incident by severity. The Service Desk is the first responder to assess the impact of IT security incidents.

3. **Response to the IT Security Incident**
   ICT's SIEM system will interface with the university's identity management service to disable accounts that are suspected to be compromised as a result of the IT security incident. In the case of a manually reported incident, the Service Desk will request the ICT Identity Management team to disable the impacted account. Once the accounts are disabled ICT will perform further containment and eradication practices based on the severity of the IT security incident, prior to reactivating the accounts and instructing the account holder to change passwords.

4. **Follow Up to IT Security Incident**
   The extent of follow up activities are dependent on the severity impact of the incident. Generally, the Service Desk will deliver a review of IT security awareness training to the impacted account holder. ICT will implement enhanced account activity monitoring on the impacted account holder for a period of one week to one month, depending on the severity of the incident. In specific cases, additional security measures may be implemented.

To start the IT security incident procedure, or if you have questions or comments, contact the ICT Service Desk at servicedesk@usask.ca.