Merchant Procedures for suspicious or confirmed incidents

Report any suspicious or unusual behavior, or any security notification from your third-party vendors using the following steps.

1. Contact your supervisor on duty.

2. Contact the SIRT at 307-766-3205 or 307-766-4391 and by sending a brief email to pci-sirt@uwyo.edu and copy your supervisor.
    - Provide a brief explanation of the incident.
    - Keep the suspicious incident confidential.
    - All further communications will be handled through your supervisor and the Payment Card Incident Response Team.

3. Do NOT touch or compromise any possible evidence.
   Do not shut off or restart any computer or Point of Sale (POS) system or unplug any card reader or other device. Leave all programs running.

4. The SIRT will send a follow-up email to the incident reporter and the supervisor included on the initial email confirming receipt of the notification.

5. Use the Payment Card Incident Log below to document all steps taken during the incident, and write down contact information for anyone else that was involved with the situation, see next page.

6. Assist the SIRT as they investigate the incident, and email the Payment Card Incident Log when requested.

Payment Card Incident Log – copy this page for additional entries as needed.

Date/Time of Incident	Person(s) Involved	Person Responsible	Location of Incident	Action(s)
Supervisor Contacted				
SIRT Contacted				
Ensure devices not restarted or shut off				

Recognizing Incidents:

Events that may be symptoms of an incident:

Detecting incidents can be a difficult task that requires planning, diligence and participation from staff from multiple departments across the institution. You as a merchant play an integral part in protecting the University against security incidents. There are many symptoms that may be detected by staff during the course of their normal, daily activities.

Below is a list of examples of suspicious or unusual security incidents. It is not an exhaustive list.

- Social engineering – someone trying to gain access to administrative computers or credit card terminals.
- Customers or other patrons showing an unusual interest in devices or operations of the credit card system or device functionality.
- Visitors attempting to get access to devices without identifying themselves and showing appropriate credentials.
- Devices – slowness, failure to respond, erratic behavior of devices, computer point-of-sale systems, registers, or card readers.
- Customers using more than two credit cards to purchase items.