ADMINISTRATION PAYMENT CARD
SECURITY INCIDENT RESPONSE PLAN
AND PROCEDURES INCLUDING MERCHANT PROCEDURES

If you are a merchant that has experienced a suspicious or unusual security incident please immediately see Appendix A – Merchant Procedures.

I. Payment Card Incident Response Plan Summary

All suspicious incidents must be reported to the Security Incident Response Team (SIRT) as soon as discovered. Merchants will follow the Merchant procedures in this document to report and assist in the response.

1. The SIRT will confirm receipt of the incident notification.
2. The SIRT will investigate the incident and assist in limiting the exposure of cardholder data.
3. The SIRT will resolve the problem including business recovery and continuity and data backup steps as needed.
4. The SIRT will report the incident and findings to the appropriate parties as necessary.
5. The SIRT will determine if policies and processes need to be updated to avoid a similar incident in the future.

II. Merchant Procedures for suspicious or confirmed incidents

If you are a merchant that has experienced a suspicious or unusual security incident, please immediately see Appendix A – Merchant Procedures. A separate copy of appendix A should be used for each separate incident.

III. Payment Card Security Incident Response Team Process and Procedures

Current SIRT procedures are available through the PCI Chairperson.

IV. Security Incident Response Team (SIRT)

The UW Payment Card Security Incident Response Team is comprised of staff members that represent the Division of Administration, and Division of Information Technology as shown below:

Contact the SIRT at pci-sirt@uwyo.edu, and call 406-580-8900 or 307-766-4391 to report suspicious security incidents.

Name	**Department/Title**	**Role**	**Telephone**	**Email**
Pehl, Sam	Administration, Financial Affairs	PCI Committee Chairperson	(406) 580-8900	spehl@uwyo.edu
Courtney, Aaron	Administration, Senior Director of Student Business Services	PCI Financial Liaison	(307) 766-3205	courtne@uwyo.edu
Kelly, Matt	Information Technology, Network Security Analyst, Executive	PCI Technical IT Lead	(307) 766- 3479	mkelly@uwyo.edu
Reese, Ashlie	Administration, Associate Vice President, Finance	PCI Banking Liaison	(307) 766-4391	areese3@uwyo.edu
Hanna, Susan	Information Technology, Network Security Analyst, Sr.	PCI Technical IT staff	(307) 766-5302	hanna@uwyo.edu
Greenwald, Jeff	Information Technology, Project Manager	PCI IT Dept. Applications Mgt. staff	(307) 766-2934	jeffery@uwyo.edu
Wiseman, Tim	Chief Risk Officer	PCI Risk Management staff	(307) 766-6787	wwiseman@uwyo.edu

V. Procedures and Other Supporting Documents

Appendix A – 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 406-580-8900 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 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.