**Incident Response Plan**

This template is general, and must be updated to apply to your specific merchant operation. Please contact the Campus PCI Coordinator for assistance in customizing your plan.

To guide the response to an incident, the following team has been assigned specific responsibilities:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Contact Details** | **Duties** |
| [FILL IN] | Departmental PCI Coordinator | [FILL IN] | Inform UCSC PCI Coordinator and departmental staff |
| Scott Morley | Campus PCI Coordinator | 831-459-1686merchantservices@ucsc.edu | Inform all appropriate parties, including ITS/Core-Tech, UCPD, and Bank if necessary |
| [FILL IN] | Department Head | [FILL IN] | Assist Departmental PCI Coordinator with resources to accomplish resolution of incident |

For Card-Present Breaches

If a terminal device shows evidence of tampering, is missing or stolen, the departmental PCI Coordinator or Department head will immediately notify Campus PCI Coordinator by phone and email using the contact information above. Isolate the machine and ensure that no further credit card transactions are run on it until it is inspected by the Campus PCI Coordinator.

For digital/ecommerce breaches:

As the probability that an attack will impact our operations increase, we have established a process to respond to the attack and minimize the impact of an incident. The incident response process includes several phases as outlined in the following diagram.



While each step in the process described above requires careful planning and implementation guidelines, the major steps that should be performed when a technical professional believes that a serious incident has occurred and the organization does not have an incident response capability available. This serves as a basic reference of what to do for someone who is faced with a crisis and does not have time to read through this entire document.

1. **1. Document everything**. This effort includes every action that is performed, every piece of evidence, and every conversation with users, system owners, and others regarding the incident.
2. **2. Find a coworker who can provide assistance.** All staff will be trained to contact Departmental PCI Coordinator and UCSC Payment Card Coordinator to report an incident. Ensure that everyone knows to contact them when a suspected or real incident occurs. Handling the incident will be much easier if two or more people work together. For example, one person can perform actions while the other documents them.
3. **3. Analyze the evidence to confirm that an incident has occurred.** Perform additional research as necessary (e.g., Internet search engines, software documentation) to better understand the evidence. Reach out to other technical professionals within the organization for additional help.
4. **4. Notify the appropriate people within the organization if it appears that an incident has occurred.** This should include the departmental PCI Coordinator, the department head, and the UCSC Payment Card Coordinator. Use discretion when discussing details of the incident with others; tell only the people who need to know and use communication mechanisms that are reasonably secure. (If the attacker has compromised e-mail services, do not send e-mails about the incident.)

The UCSC Payment Card Coordinator will inform all necessary authorities that an event has occurred. Please contact them immediately using the information in the table below.
5. **5. Stop the incident if it is still in progress.** The most common way to do this is to disconnect affected systems from the network. In some cases, firewall and router configurations may need to be modified to stop network traffic that is part of an incident, such as a denial of service (DoS) attack.
6. **6. Preserve evidence from the incident.** Make backups (preferably disk image backups, not file system backups) of affected systems. Make copies of log files that contain evidence related to the incident.
7. **7. Wipe out all effects of the incident**. This effort includes malicious code infections, inappropriate materials (e.g., pirated software), Trojan horse files, and any other changes made to systems by incidents. If a system has been fully compromised, rebuild it from scratch or restore it from a known good backup.
8. **8. Identify and mitigate all vulnerabilities that were exploited**. The incident probably occurred by taking advantage of vulnerabilities in operating systems or applications. It is critical to identify such vulnerabilities and eliminate or otherwise mitigate them so that the incident does not recur.
9. **9. Confirm that operations have been restored to normal**. Make sure that data, applications, and other services affected by the incident have been returned to normal operations. If sensitive data is restored, ensure that all security steps be followed when handling the sensitive back up data and recovery systems.
10. **10. Create a final report**. This report should detail the incident handling process. It also should provide an executive summary of what happened and how a formal incident response capability would have helped to handle the situation, mitigate the risk, and limit the damage more quickly.

**11. Meet after the breach to discover “lessons learned”.** After the breach has been resolved, the Departmental PCI Coordinator, UCSC PCI Coordinator, Department Head, and other senior staff will meet to discuss the nature of the breach and establish processes and procedures to prevent future breaches.

To improve the process and staff ability to execute the plan summarized above, the company will test the plan each year. Improvements to the plan will be incorporated into the annual risk review and policy update.