

UH PCI Security Incident Response Plan Guidelines

Merchant's Security Incident Response Plan (SIRP) must be developed for the Merchant's SAQ type and complexity

- Merchant's SIRP must include appropriate SAQ PCI DSS processes and procedures.
- Merchant's SIRP should encompass all phases of the security incident response: Preparation, Detection & Analysis, Containment, Eradication & Recovery, Post-Incident Activity & Analysis



Phase 1	Phase 2	Phase 3	Phase 4
Prepare Plan Assess Prevent	Detect Analyze Prioritize Notify (Internal)	Contain Collect Eradicate Recover	Notify (External) Review Recommend Report

Definition & Examples of a Security Incident:

- Severe violation of a security policy
- Server with regulated data allows unauthenticated access to the data
- A server is compromised
- A workstation or laptop with sensitive or regulated information is compromised
- Numerous computers are infected with a network worm
- Denial of Service attack with the potential to impact business critical services
- Loss or theft of a device/electronic media/paper that contains sensitive or regulated information

Phase 1: Preparation

- Identify what is “in-scope” for Merchant’s SAQ Requirements:
 - Inventory of devices, equipment, data
 - Current network map
 - Current data flow diagram
- Identify Security Incident Response (IR) Team; at a minimum, must include:
 - Merchant Account Contact
 - Merchant IT Contact
 - Fiscal Administrator
 - UH Treasury PCI Coordinator
 - UH CISO/UH Information Security Team member – Infosec will coordinate notifications if necessary

Phase 2: Detection & Analysis

- Potential Incident Detection (incident is not yet confirmed):
 - Automated alerts, anomalous activities/behavior, external notifications, etc.
- Assess situation quickly to determine if it is an actual security incident
 - Are there signs of compromise (e.g. suspicious file/process, logs show possible intrusion)?
 - Is there or is it possible that sensitive or regulated information is stored on the target?
 - What other data/systems did the target have access to (e.g. file shares, databases, development keys)?
 - Is the target a critical system?
- If “yes” to any of the above questions or if unsure about the situation, notify the UH Information Security Team (infosec@hawaii.edu) and UH Treasury Office immediately

Phase 3: Containment, Eradication, Recovery

- Determine incident priority
 - What type of security incident
 - What is the scope of the incident
 - What is the impact of the event
 - What are the details of the attack
- Contain the incident to prevent and stop further compromise, data exfiltration, and additional attacks. Never power off or restart affected devices without first consulting with the UH CISO or SIRT.
- The SIRT will
 - Collect evidence (e.g. RAM, hard drive image, system and network logs, packet captures, etc.)
 - Identify the point of entry and root cause of the incident
- Once notified by the SIRT, rebuild or restore affected systems from backup
- Provide frequent status reports to the SIRT

Phase 3 – continued:

- Typical IR/Analysis Work Flow includes:
 - Contain system (disconnect network)
 - Obtain volatile artifacts (capture RAM)
 - Image hard drive (raw format)
 - Analyze the image or copy of VM
 - Check for open network connections
 - Check running processes/services
 - Check startup locations/scheduled tasks/cron jobs
 - Check cache/temp folders
 - Check network and system logs/events/history
 - Check versions/patch level
 - Scan with anti-virus
 - Collect Evidence/Screenshots
 - Document activity and findings with date/times

Phase 4: Post-Incident Activity and Analysis

- Reporting
 - UH Treasury & UH Infosec will identify the reporting requirements as determined by applicable laws and regulations and work with the Merchant on the timeline, report format, and appropriate notifications
- After Action Analysis
 - Review cause of incident and implement technologies, policies, procedures to prevent it from re-occurring
 - Review response timeline, process and procedures to identify areas of improvement