# Incident Response Process

|  |
| --- |
| Contents  * 1 Purpose and Scope * 2 Definitions * 3 Roles & Responsibilities * 4 Reporting Security Events & Weaknesses   + 4.1 Open Reporting Principle   + 4.2 Internal Monitoring and Reporting * 5 Incident Declaration, Evaluation and Prioritization   + 5.1 Declaration   + 5.2 Evaluation   + 5.3 Impact Prioritization * 6 Evidence Collection * 7 Incident Containment * 8 Recovery   + 8.1 Data Backup Processes   + 8.2 Business Recovery and Continuity Procedures * 9 External Communications and Reporting * 10 Contacts and Communications * 11 Post Incident   + 11.1 Lessons Learned Meeting   + 11.2 Incident Report * 12 Plan Testing, Review & Revision * 13 Enforcement and Exceptions * 14 Response Tools and Procedures |

## Purpose and Scope

The purpose of the Incident Response Plan is to define the requirements needed to ensure that security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. This scope of this plan applies to all ACME employees, contractors and third parties.

## Definitions

* CSIRT - The Computer Security Incident Response Team (CSIRT) is the group of individuals that will assemble and work collaboratively during a security incident.
* Intrusion - The act of gaining some level of unauthorized access that violates the security policy.
* Security Event - A single instance or indication of a security weakness that might indicate a loss of confidentiality, integrity, or availability.
  + Security events may include, but are not limited to: suspicious log entries, suspicious access attempts, unexplained password change, website defacement, loss of storage media, disclosure of confidential information, disclosure of encryption key material, discovery of unauthorized software, unauthorized computer systems, or unauthorized wired or wireless networking equipment.
* Security Incident - A collection of related security activities or events that indicates the strong possibility of a loss of confidentiality, integrity, or availability.
* Security Team - The team of individuals at ACME who are primarily responsible for carrying out the daily security duties for the company.

## Roles & Responsibilities

Incident management is a discipline that requires many actors in the organization to take on certain roles and responsibilities before, during, and after an incident.

**Everyone**

* All employees, contractors, and third parties are responsible for reporting security events under the Open Reporting Principle.

**Security Team**

* Monitors systems and their associated alerts in order to detect information security incidents including intrusion detection, intrusion prevention, and file integrity monitoring systems on a daily (M-F) basis.
* Declares security incidents and assembles the CSIRT at the onset of an incident.
* Identifies an incident coordinator for each unique incident.
* Maintains relationships with law enforcement, ISPs, 3rd-party contractors, managed security providers, and other security experts (e.g. CERT/CC, SANS, etc.).
* Develops corporate incident response procedures and coordinate incidents that affect the company.

**CSIRT**

* Computer Security Incident Response Team (CSIRT) will be assembled by the Security Operations team to address a new incident.
* Comprised of Security Operations staff, technical staff, and management representatives.
* Members may also include business unit owners, legal counsel, corporate communications, human resources, corporate security, regulatory/legal liaisons, additional technology experts, etc. These members must be familiar with the CSIRT procedures and understand their roles and responsibilities, when requested, during an incident.
* Communications may occur face-to-face or through email, text, phone bridge, IM or other means of collaboration and sharing.

**Incident Coordinator**

* Security Operations team may designate an Incident Coordinator for each incident if needed.
* Responsible for coordinating communications.
* Holds high level management decision-making ability and/or influence
* Understands the legal implications of unauthorized activity
* Understands the “Big Picture” view
* Coordinates with PR/Corporate communications for providing information to internal employees, public, etc.

**Analysts/Investigators**

* Security Operations team may designate analysts and investigators who will determine the extent of damage and the effects on systems, data, and operations.
* Determines the root cause of the computer security event and its scope.
* Preserves data according to the incident response plan.
* Takes steps necessary to identify the perpetrator and quantify damages (under the direction of the incident coordinator)

**NOC**

* Functions as a communications hub, arranges a conference bridge, and pages key individuals during an incident (if directed by the CSIRT).
* Conducts new monitoring and alerting activities during an incident (if directed by the CSIRT).

**Other**

Other departments may have representation or consultation during a computer incident, including but is not limited to:

* Finance Division
* Legal Division
* Corporate Communications (PR)
* Online Customer Relations (Community)
* Customer Support (Game Masters, Billing Support, Tech Support)
* Disaster Recovery and/or Business Continuity Plans (BCPs)
* Human Resources Division

## Reporting Security Events & Weaknesses

### Open Reporting Principle

ACME encourages open and full disclose of all security events, including human errors, without the fear of reprisal. All employees, contractors, and third parties are responsible for reporting security events to security@acme.com

### Internal Monitoring and Reporting

* Security Operations monitors systems and their associated alerts in order to detect information security incidents including intrusion detection, intrusion prevention, and file integrity monitoring systems on a daily (M-F) basis.
* The NOC monitors systems for security, performance, and availability on a 24x7 basis. The NOC also monitors email discussions regarding systems problems, which often indicates a possible security incident. The NOC should report all security events to Security Team. The NOC should page the Security Team "on call" person for all suspected incidents.
* Security Team may offer reporting forms or templates to support an accurate and repeatable reporting process.
* Employees, contractors, or third parties are advised not to attempt to prove suspected security weaknesses.

## Incident Declaration, Evaluation and Prioritization

### Declaration

Security Team declares security incidents, assembles the CSIRT, and begins executing the Incident Response Plan when evidence is present to indicate a security incident.

Incidents are named and numbered according to the following conventions:

* **Incident YYYYMMDD: System Name compromise through vulnerability name**

### Evaluation

During a security incident the CSIRT members will meet so that all members can be informed of their tasks related to the event and to ensure that there is no duplication of effort and corruption of evidence. The CSIRT will handle the initial evaluation of the security incident. All CSIRT members will report to the incident coordinator during the evaluation phase to ensure effective coordination, collection, and response.

CSIRT members will evaluate the related security events and evidence to determine:

* Has a genuine security event occurred?
* What is the suspected scale of the event?
* Which ancillary groups need to be involved?
* Is the event malicious or unintentional?
* What additional information is needed?
* What should our initial response be?
* How can we begin to contain or minimize the damage?
* What kind(s) of information may have been compromised? (e.g. Cardholder Data, Intellectual Property, other)

If the incident involves a disclosure of stolen customer credentials, test the list of credentials against our actual credential database to determine what percentage of the stolen credentials are actually valid.

### Impact Prioritization

The CSIRT will prioritize based on the impact of the incident according to the matrix below.

|  |  |  |
| --- | --- | --- |
| **High** | **Medium** | **Low** |
| * Loss of availability * Confirmed loss of confidentiality or integrity of ACME confidential information * Other security incidents that may have a significant, company-wide impact | * Possible loss of availability * Confirmed or possible loss of confidentiality or integrity of company or customer information * Other security incidents that may have a moderate impact | * Possible loss of confidentiality or integrity of company or customer information * Harassment or degradation of system resources * Other security incidents that may have a low impact |

Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should be prioritized based on two factors:

* Current and Potential Technical Effect of the Incident. Incident handlers should consider not only the current negative technical effect of the incident, but also the likely future technical effect of the incident if it is not immediately contained (e.g., root compromise).
* Criticality of the Affected Resources. Resources affected by an incident have different significance to the organization. The criticality of a resource is based primarily on its data or services, users, trust relationships and inter dependencies with other resources, and visibility.

Combining the criticality of the affected resources and the current and potential technical effect of the incident determines the business impact of the incident—for example, root compromise of a user workstation might result in a minor loss of productivity, whereas unauthorized user-level access to a public Web server could result in a major loss of revenue, productivity, access to services, reputation, and the release of confidential data.

## Evidence Collection

* Security Team must be involved in all evidence collection activities either directly or in a consultative role.
* Security Team must have a process demonstrating that proper evidence handling is achieved.
* Forensics work should only be performed on copies of the evidenced material in secure areas.
* The integrity of all evidential material should be protected.

Proper handling is established under the following conditions:

* For paper documents: the original is kept securely with a record of the individual who found the document, where the document was found, when it was found, and who witnessed the discovery; any investigation should ensure that originals are not tampered with.
* For information on computer media: mirror images or copies of any removable media, information on hard disks or in memory should be taken to ensure availability; the log of all actions during the copying process should be kept and the process should be witnessed; the original media and the log should be kept securely and untouched.

A detailed log should be kept for all evidence, including the following:

* Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) address, and IP address of a computer)
* Name, title, and phone number of each individual who collected or handled the evidence during the investigation
* Time and date (including time zone) of each occurrence of evidence handling
* Locations where the evidence was stored.

Collecting evidence from computing resources presents some challenges. It is generally desirable to acquire evidence from a system of interest as soon as one suspects that an incident may have occurred. Many incidents cause a dynamic chain of events to occur; an initial system snapshot may do more good in identifying the problem and its source than most other actions that can be taken at this stage. From an evidentiary standpoint, it is much better to get a snapshot of the system as-is rather than doing so after incident handlers, system administrators, and others have inadvertently altered the state of the machine during the investigation. Users and system administrators should be made aware of the steps that they should take to preserve evidence.

Before copying the files from the affected host, it is often desirable to capture volatile information that may not be recorded in a file system or image backup, such as current network connections, processes, login sessions, open files, network interface configurations, and the contents of memory.

After acquiring volatile data, an incident handler with computer forensics training should immediately make a full disk image to sanitized write-protectable or write-once media. A disk image preserves all data on the disk, including deleted files and file fragments. If it is possible that evidence may be needed for prosecution or internal disciplinary actions, the handlers should make at least two full images, label them properly, and securely store one of the images to be used strictly as evidence. (All evidence, not just disk images, should be tagged and stored in a secure location.) Occasionally, handlers may acquire and secure the original disk as evidence; the second image can then be restored to another disk as part of system recovery.

During evidence acquisition, it is often prudent to acquire copies of supporting log files from other resources—for example, firewall logs that show what IP address an attacker used. As with hard drive and other media acquisition, logs should be copied to sanitized write-protectable or write-once media. One copy of the logs should be stored as evidence, whereas a second copy could be restored to another system for further analysis.

## Incident Containment

When an incident has been detected and analyzed, it is important to contain it before the spread of the incident overwhelms resources or the damage increases. Most incidents require containment, so it is important to consider it early in the course of handling each incident.

The CSIRT will determine containment strategy while considering the following:

* Potential damage to and theft of resources
* Need for evidence preservation
* Service availability (e.g., network connectivity, services provided to external parties)
* Time and resources needed to implement the strategy
* Effectiveness of the strategy (e.g., partially contains the incident, fully contains the incident)
* Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

## Recovery

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malicious code and disabling breached user accounts. In recovery, administrators restore systems to normal operation and (if applicable) harden systems to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security.

### Data Backup Processes

* Backup Procedures
* SQL Backup Destinations
* SQL Database Fail Over Procedure

### Business Recovery and Continuity Procedures

* A business continuity team meets quarterly to discuss BCP strategy.
* ACME has established a timeline of 7 days for recovering the CDE in the event of a major outage.
* ACME is insured for up to 15 days of lost-revenue caused by any major outage in our CDE.
* Recovery site is our second datacenter.
* Priority 1: Reestablish the MAIN\_PROD database.
  + The MAIN\_PROD database information (excluding credit cards) is replicated to the second datacenter and could be reestablished in a matter of days.
  + The hardware storage module (HSM) can be reestablished in about two to three days. The development unit will be shipped from Austin to second datacenter and reconfigured as production.
* Priority 2: Reestablish back end systems and connectivity with payment processor.
  + Network firewalls will be reconfigured to permit connectivity with Payment Processor.
  + The back end systems that run the Payment Application application will be reinstalled in second datacenter.
* Priority 3: Reestablish front end systems and customer transactions.
  + Source code for front end systems is kept in redundant source control repositories and can be republished quickly.
  + Web servers are ESX virtual machines and can be provisioned in less than 1 day.
  + SSL certificates can be reissued from Public CA in 1 hour.

## External Communications and Reporting

* The incident coordinator will work with the legal, HR, or corporate communications team as necessary to coordinate external communications and reporting.
* A security incident may require external reporting to law enforcement, payment processors, or customers.

**When to contact law enforcement** (guidelines): Is this a physical theft? Is any person in danger as a result of the theft? In the event of a stolen computer hard drive, laptop, or other device, along with any identity theft issues, report the crime to the proper legal authorities. Consult with ACME's legal council before contacting law enforcement.

**When to contact customers** (guidelines): The Federal Trade Commission (FTC) has a list of notification guidelines, when sending notification to individuals. Allow the affected individuals to request police reports, contact law officials, contact credit bureaus and urge the victims to contact the FTC, if needed. Consult with ACME's legal council before contacting law enforcement.

Under most laws, it is the “reasonable belief” that sensitive data were acquired by an unauthorized person that triggers the requirement of notification. And once a system has been breached, the legal assumption is that everything on the system was accessible to the intruder.

**When to contact payment processors**:

1. **Payment Processor** – breach notification rules
   * If you have detected an incident ….
2. **Visa** - [breach notification procedures](http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf) *(page 9)*
   * Entities that have experienced a suspected or confirmed security breach must take prompt action to help prevent additional exposure of cardholder data and ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS), PCI Payment Application Data Security Standard (PA-DSS)2, and PCI PIN Security Requirements.
3. **MasterCard** - [account data compromise guide](http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf) *(chapter 2)*
   * If you suspect a compromise you must immediately complete an [ADC Reporting Form](http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf) and submit it to account\_data\_compromise@mastercard.com.
4. **Discover** - [breach notification procedures](http://www.discovernetwork.com/fraudsecurity/databreach.html)
   * Proper communication must be provided to appropriate parties to help ensure affective handling of the incident. Work with your internal information security group to ensure they are aware of the incident and contact the following organizations: Your Acquirer, Discover Network Incident Response Team 1-800-347-3083, Local United States Secret Service office.
5. **American Express** - [breach notification procedures](https://www209.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Merchant_US.pdf) *(Section 2 – Data Incident Management Obligations)*
   * Merchants must notify American Express immediately if they know or suspect that Cardmember Information has been accessed or used without authorization or used other than in accordance with their Agreement. To notify American Express, please contact the American Express Enterprise Incident Response Program (EIRP) toll free at (888) 732-3750/US only, or at 1-(602) 537-3021/International, or email at EIRP@aexp.com.

## Contacts and Communications

* Communication and Contact strategies
* Master Contact List
* Contact Information
* Brand Director
* VP of Corporate Communications
* Director of Operations

## 

## Post Incident

### Lessons Learned Meeting

The CSIRT may choose to hold a "lessons learned" meetings after a high severity incident. Lessons learned meetings are extremely helpful in improving security measures and the incident handling process itself. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident. Questions to be answered in the lessons learned meeting include:

* Exactly what happened, and at what times?
* How well did staff and management perform in dealing with the incident?
* Were the documented procedures followed? Were they adequate?
* What information was needed sooner?
* Were any steps or actions taken that might have inhibited the recovery?
* What would the staff and management do differently the next time a similar incident occurs?
* What corrective actions can prevent similar incidents in the future?
* What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

### Incident Report

After each high severity incident, Security Team will draft a post-incident report for management. Reports are good material for training new team members by showing them how more experienced team members respond to incidents. Updating incident response policies and procedures is another important part of the review process. Post-mortem analysis of the way an incident was handled will often reveal a missing step or an inaccuracy in a procedure, providing impetus for change. Because of the changing nature of information technology and changes in personnel, the incident response team should review all related documentation and procedures for handling incidents at designated intervals.

The incident report provides a reference that can be used to assist in handling similar incidents. Creating a formal chronology of events (including time stamped information such as log data from systems) is important for legal reasons, as is creating a monetary estimate of the amount of damage the incident caused in terms of any loss of software and files, hardware damage, and staffing costs (including restoring services).

Incident reports are stored in **V:\operations\security\incident reports\**

## Plan Testing, Review & Revision

This Plan will be executed or tested at least annually to ensure that the policies and procedures work as documented and are updated as needed based on this testing.

A program for periodic test and review of the Plan will accomplish the following:

* Schedule testing of major changes affecting organization structure or corporate infrastructure (e.g., a merger, a divisional size move Windows 2003 to 2008 systems, etc.)
* Include different scenarios for each test (e.g., a DDoS attack, an insider theft of IP (Intellectual Property), an insider scanning another organization’s network, etc.)
* Ensure testing is accomplished at different times of the day, week, and month (e.g., some at night, some on weekends, some during regular business hours, etc)
* Incorporate new industry developments including: changes in to our administrative controls (corporate policy), changes to our security awareness education, changes in attack vectors, changes in tools and technical controls.
* Review changes in legal or regulatory requirements.

Plan participants should submit recommended improvements to Security Team at the conclusion of each test or live incident.

## Enforcement and Exceptions

* Strict compliance with this Plan is essential to the effective protection of ACME. Any detected Plan violation will be forwarded to the appropriate manager, Security Team, and HR representative for appropriate action.
* Security Team must approve any exceptions to this Plan. You can initiate a request for exception by sending a detailed request to security@acme.com.

## Response Tools and Procedures

* Phishing Website Response
* AntiVirus Detection
* Virus Outbreak Response
* Incident Response Tools
* NIST Special Publication 800-61 Computer Security Incident Handling Guide
* CERT Guidelines
* Incident Questionnaire