|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information Security Policy | | | | |
| Cyber Incident Response Policy | | | | |
| Policy # |  | | Effective Date |  |
| Version |  | Contact | |  |

**Table of Contents**

[Purpose and Scope 2](#_Toc115086102)

[Policy 2](#_Toc115086103)

[IR-1 INCIDENT RESPONSE POLICY, PROCESS AND PROCEDURE: 2](#_Toc115086104)

[IR-2 INCIDENT RESPONSE TRAINING: 2](#_Toc115086105)

[IR-4 INCIDENT HANDLING: 3](#_Toc115086106)

[IR-5 INCIDENT MONITORING: 3](#_Toc115086107)

[IR-6 INCIDENT REPORTING: 3](#_Toc115086108)

[Categories of Incidents: 3](#_Toc115086109)

[Severity of Incident: 4](#_Toc115086110)

[IR-7 INCIDENT RESPONSE: 5](#_Toc115086111)

[IR-8 INCIDENT RESPONSE PROCESS: 5](#_Toc115086112)

[Roles and Responsibilities 6](#_Toc115086113)

[General Guidelines for all Roles 6](#_Toc115086114)

[Role: All Individuals with Computer Accounts 6](#_Toc115086115)

[Role: <COMPANY> IRT Leader 7](#_Toc115086116)

[Role: Senior Management 8](#_Toc115086117)

[Role: Information Security 8](#_Toc115086118)

[Role: Risk & Compliance 9](#_Toc115086119)

[Role: Data Owner 10](#_Toc115086120)

[Role: Information Technology 10](#_Toc115086121)

[Role: IT Subject Matter Expert 11](#_Toc115086122)

[Role: Application Subject Matter Expert 11](#_Toc115086123)

[Role: Major Incident Management (MIM) 11](#_Toc115086124)

[Role: Corporate Security 11](#_Toc115086125)

[Role: Legal 11](#_Toc115086126)

[Role: Human Resources 12](#_Toc115086127)

[Role: Public Relations 12](#_Toc115086128)

[Role: Client Relations 13](#_Toc115086129)

[Role: Financial Audit 13](#_Toc115086130)

[Training 13](#_Toc115086131)

[Policy Compliance 13](#_Toc115086132)

[Definitions 14](#_Toc115086133)

[Resources 14](#_Toc115086134)

[Approval and Ownership 14](#_Toc115086135)

[Revision History 14](#_Toc115086136)

Purpose and Scope

The purpose of this document is to describe the actions <company> will take in response to a cyber-security related incident, including the subsequent investigations on the causes, a damage assessment, and remedial actions to prevent recurrence. These measures are necessary to ensure the confidentiality of the data, the integrity of the data, and the reliability/availability of the information systems.

This policy applies to all business units within <COMPANY>. It sets the minimum requirements for recognizing and responding to a cyber-security related incident within <COMPANY>.

This policy applies to any type of cyber security incident. A cyber security incident is an event that adversely affects some portion of the computing resources such as malware propagation, unauthorized intrusions, or security volitions originating from within our own organization.

This policy does not cover responding to a cyber “crisis” but should be included as part of the <COMPANY> crisis response process. A crisis is an unplanned event with the potential for significant injury to people or the environment, or the potential for significant damage to the company, its employees, facilities, products, finical condition or reputation.

Policy

<COMPANY> has chosen to adopt the incident management principles established in the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations” and the NIST SP 800-61 Revision 2 “*Computer Security Incident Handling Guide*,” as the basis for <COMPANY>’s incident response policy and process. The following subsections outline the incident management policies that are the basis for the <COMPANY> incident response process and procedures.

## IR-1 INCIDENT RESPONSE POLICY, PROCESS AND PROCEDURE:

<COMPANY> shall develop, document, and disseminate to <COMPANY> businesses and <COMPANY> Tech:

1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
2. Processes and procedures to facilitate the implementation of the incident response policy and associated incident response controls;

The incident response policy will be reviewed at a minimum every three (3) years. Incident response processes and procedures will be reviewed every year at a minimum.

## IR-2 INCIDENT RESPONSE TRAINING:

<COMPANY> must provide incident response training to information system users consistent with assigned roles and responsibilities.

This training should occur within 90 days of assuming an incident response role or responsibility; when required by information system changes; and at least annually for individuals with an incident response role or responsibility on industry best practices associated with incident response.

## IR-4 INCIDENT HANDLING:

<COMPANY> shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

<COMPANY> coordinates incident-handling activities with contingency planning activities.

<COMPANY> incorporates lessons learned from ongoing incident handling activities into incident response processes and procedures, training, and testing/exercises, and implements the resulting changes accordingly.

## IR-5 INCIDENT MONITORING:

<COMPANY> shall track and document information system security incidents.

## IR-6 INCIDENT REPORTING:

<COMPANY> requires personnel to report suspected security incidents to the <COMPANY> Incident Response Team by contacting the <COMPANY> Service Desk as soon as possible.

### Categories of Incidents:

Based on the initial report incidents will be categorized into one of three categories:

**Data Incident**: A data incident is defined as a detected or suspected unauthorized access, alteration, acquisition, use or disclosure, or the loss (includes inability to locate) of Personal Information or other confidential information, of or regarding the company, its employees, its clients, or other third parties (personal information and confidential information are collectively referred to as company data), whether held by the company or by its vendors or other third parties for or on behalf of the company. A data incident may involve company data that exists in any format – electronic, hard copy, or oral. Personal Information is defined as “information that directly relates to an identified or identifiable individual.”

Examples of Data Incidents include:

* The loss of any electronic storage media (e.g., CD, DVD, flash drive, laptop or desktop computer, hard drive, iPad, tablet computer or other hand held device) that contains unencrypted company data, or such a device where there is indication that the encryption might be compromised (for example if the password is lost with the asset);
* The theft of company data;
* An email containing sensitive company data, personal information (PI) or personal health information(PHI) sent inadvertently to the wrong recipient;
* Improper disposal of company data;
* A mailed package containing company data which was lost or sent or delivered to the wrong recipient; or
* An oral conversation about personal information or confidential information that was overheard by an unauthorized party.

**Note:** These are examples and are not meant to present an exhaustive list.

In general, data incidents do not directly involve an information system (PC, server, network systems or components, etc.). Should a data incident involve information systems, then the incident should be categorized as “Cyber/Data Incident” and the joint process should be followed.

**Cyber Security Incident:** A cyber security incident involves any of the following criteria:

* The identification of a new vulnerability within, malicious attack upon, or compromise of an <COMPANY> information system or resource held or hosted by the company or a third party on <COMPANY>’s behalf;
* The violation of company security policies or procedures negatively affecting the operation of company information systems or resources.

Examples of Security Incidents are:

* Detection of malware, or similar malicious software, with remote access capabilities with and no evidence of data breach;
* A denial of service attack;
* Identification of active email attacks or campaigns targeting the firm (e.g. phishing);
* Harassment utilizing electronic means;
* Unauthorized changes to application or system configurations or code;
* Colleague installed software deemed malicious or inappropriate given their responsibilities (*e.g.*, hacking software, password crackers, avoidance software, etc.)

**Note:** These are examples and are not meant to present an exhaustive list.

In cyber security incidents suspecting unauthorized access, alteration, acquisition, use or disclosure of personal/other confidential information, regarding <COMPANY>, its employees/clients/other third parties, held by <COMPANY> or other third parties on behalf of <COMPANY>, then the incident should be categorized as “Cyber/Data Incident” and the joint process should be followed.

**Joint Cyber / Data Incident**: These incidents involve elements of both a cyber and data incident. These incidents shall be handled using the “Joint Cyber / Data Incident Process”.

### Severity of Incident:

Once the incident has been categorized, it is given an initial severity based on the criteria below:

|  |  |  |
| --- | --- | --- |
| Business  Severity | <COMPANY> Severity | Criteria (one or more) |
| Significant | 1 | * Potential revenue impact >$25MM * Likely notification required to >10,000 individuals or >500 clients * Meets the threshold for making a disclosure under the U.S. SEC rules * Likelihood of significant adverse media attention * Is determined by the <COMPANY> CRCO or CISO to be Significant |
| High | 1 | * Potential revenue impact $5-100MM * Likely notification required to 3,000-10,000 individuals or 25-500 clients * Likely to have a cross-business unit impact * Confirmed financial loss/ID Theft affecting >25 individuals * Involves highly confidential information like M&A activity * Involves or likely to involve law enforcement, supervisory regulators or result in media exposure |
| Medium | 2 | * Potential revenue impact $500K-$5M * Likely notification required to 250-3,000 individuals or 5-25 clients * Confirmed financial loss/ID Theft affecting 5-25 individuals * Involves confidential information that is likely to require client notification * Involves or likely to involve data protection authorities or other government agencies that need to be notified when a breach notification letter is issued |
| Low | 3-5 | * Potential revenue impact <$500K * Likely notification required to <250 individuals or <5 clients and does not require any notification to data protection authorities or other government agencies * Confirmed financial loss/ID Theft affecting <5 individuals * Incidents covered by approved simplified processes |

The category and severity drive both the incident response process used and the timeline for the response. At any point, the incident response leader can change either the category or the severity.

## IR-7 INCIDENT RESPONSE:

<COMPANY> shall provide a support resource for incident response, integral to the organizational incident response capability, which offers advice and assistance to users of the information system for the handling and reporting of security incidents.

## IR-8 INCIDENT RESPONSE PROCESS:

<COMPANY> shall:

1. Develop an incident response process that:
   1. Provides the organization with a roadmap for implementing its incident response capability;
   2. Describes the structure and organization of the incident response capability;
   3. Provides a high-level approach for how the incident response capability fits into the overall organization;
   4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   5. Defines reportable incidents;
   6. Provides metrics for measuring the incident response capability within the organization;
   7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   8. Is reviewed and approved by both the Corporate Information Security Officer (CISO) and the Chief Risk & Compliance Officer (CRCO).
2. Distributes copies of the incident response process to all elements under Risk and Compliance;
3. Reviews the incident response process and procedures at a minimum every year;
4. Updates the incident response process and processes to address system/organizational changes or problems encountered during process implementation, execution, or testing;
5. Communicates incident response process changes to the necessary elements within Risk & Compliance;
6. Protects the incident response process from unauthorized disclosure and modification.

Roles and Responsibilities

The <COMPANY> Incident Response policy identifies a set of roles that have certain responsibilities during the incident response process. The sequence of this list indicates neither the timeline nor relative importance of any one role over another.

*Note: All comments to any news media or the public must come from the Marketing and Communications department, NOT from members of the Incident Response Team. Make no statements to anyone except <COMPANY> management or the <COMPANY> IRT Leader in charge of the response.*

***Incidents, which might be turned over to an external agency, such as law enforcement or another company, must be coordinated through Risk & Compliance department based on the nature of the incident.***

## General Guidelines for all Roles

1. When you first learn of a potential incident, make sure you verify the name and phone number of all individuals involved in the discussion (unless the report is anonymous);
2. Do not jump to conclusions;
3. With the exception of virus activity on an end user computer, DO NOT log into a computer in an attempt to investigate until you have cleared it with the local Information Security / Cyber Incident Response Team (CIRT) representative. If reservation of evidence becomes a requirement, your actions could be detrimental to the investigation and increase the company's liability for any damage;
4. Make certain what happened is really an incident and not an error or breach of procedure. If you believe it is an incident, report it to the <COMPANY> Service Desk;
5. As long as you are involved with the incident response, make detailed notes, being careful not to include suppositions;
6. All information relating to an incident and its investigation shall be disclosed only on a need-to know basis. All documents related to the investigation shall be marked and treated as <COMPANY> confidential information;
7. When involving others in the cyber incident response, present facts in a clear, organized manner with sufficient detail to support the allegation. Be prepared to explain all technical details as clearly as possible.

## Role: All Individuals with Computer Accounts

Preparation:

* Take prompt action to facilitate the installation of all updates, etc. to permit immediate elimination of known vulnerabilities on your machine(s);
* Follow <COMPANY> policies on third party software and acceptable use of computer resources to minimize exposure to sources of viruses, spyware, malware, etc.;
* Learn how to disconnect your computer from the network before you are infected with malicious software;
* Be aware of common types of events that can be security incidents.

Identification and Assessment:

* If you think your machine has become infected, disconnect it from the network and leave it disconnected until you receive the all-clear from <COMPANY> Tech;
* Quickly report to the <COMPANY> Service Desk:
  + <contact info>

Containment, Remediation, and Follow-Up:

* Follow instructions from the Cyber Incident Response Team.

## Role: <COMPANY> IRT Leader

The <COMPANY> Incident Response Team (IRT) Leader shall be a trained member of the <COMPANY> Incident Response Team. The category of the incident will determine what organization provides the incident response leader:

|  |  |
| --- | --- |
| Incident Type | Designates the Incident Response Leader |
| Data Incident | GPL |
| Cyber Incident | CISO |
| Joint Cyber/Data Incident | GPL / CISO |

In the case of a joint cyber/data incident, the GPL and CISO shall determine if the incidents will be managed under one or two IRTs and which IRT shall take the lead on handling the Incident.

The <COMPANY> IRT Leader leads overall incident response activities and directs actions of sub-teams by achieving or delegating the following, as warranted by the seriousness of the current incident:

1. Gather facts, determine approach based on the specific incident, and request resources required for the remaining processes;
2. Act as liaison among Legal, Human Resources, Security, Compliance, Crisis Management, and executive management as needed;
   1. Severity 1 Events:
      1. Notify within one (1) hour of identification the Corporate Information Security Officer (CISO) and/or the Chief Risk & Compliance Officer (CRCO) of the incident.
      2. Notify the Incident Response team via email distribution list to ensure non-involved team members are aware of the incident and response. For cyber incidents, the <contact info> distribution list shall be used.
   2. Severity 2 Events:
      1. Notify within four (4) hours of identification Corporate Information Security Officer (CISO) and/or the Chief Risk & Compliance Officer (CRCO) of the incident.
      2. Notify the Incident Response team via email distribution list to ensure non-involved team members are aware of the incident and response. For cyber incidents, the <contact info> distribution list shall be used.
3. Ensure proper general communication is formulated and distributed to internal personnel when necessary;
4. Ensure proper record keeping of discussions, actions, daily logs of activities, and summary updates as appropriate to the nature of the incident;
5. If required by the nature of the incident, establish a secure “war room” in a secure environment that will allow incident –related documents and graphics representations to remain posted and available to the team at all hours. This war-room may be physical or virtual, however, if it is virtual it should be out-of-band from the cyber incident;
6. Assist with the seizure of evidence to ensure proper handling and effective chain of custody;
7. Conduct examination according to guidelines in appendices for specific types of incidents;
8. Notify stakeholders of resolution;
9. Document all findings and provide a summary report and evidence files to HR, Legal, Compliance and IT management as determined by the nature of the incident. (Not all incidents will warrant a formal report; IRT Leader, CISO and CRCO should determine the requirements)

## Role: Senior Management

Apart from providing the team, the authority for operation, Senior Management, particularly the CISO and CRCO, has to make business-related decisions based on the input from the other members of the team. Senior <COMPANY> Management shall:

1. Act as key decision makers when an incident and/or the response involve, major financial or other significant impact to the business;
2. Make an informed decision for systems running core business systems to be shut down to stop and attack or left running to study the attack.

## Role: Information Security

Information security shall be responsible for the response on cyber incidents and shall work in tandem with Risk & Compliance on join cyber/data incidents. Information security shall:

1. Prepare for cyber incidents prior to an incident by documenting or preparing:
   1. Communications and Facilities:
      1. Contact information
      2. On-call information
      3. Incident reporting mechanisms
      4. Issue tracking system
      5. Encryption capabilities
      6. War room
      7. Secure storage facility
   2. Analysis Hardware and Software
      1. Forensic workstation
      2. Forensic software
      3. Analysis software
      4. Blank removable media
      5. Evidence gathering accessories
   3. Analysis Resources:
      1. Documentation
      2. Network diagrams
      3. Current baselines
   4. Training
2. Detection and analysis of an incident:
   1. Determine if an incident has occurred based on specific event(s);
   2. Determine the type of incident that has occurred;
   3. Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)
3. Containment of an incident:
   1. Determine containment process;
   2. Collect evidence for analysis;
4. Eradicate the incident:
   1. Identify all vulnerabilities that were exploited;
   2. Act as a consultant to <COMPANY> Tech as they mitigate the vulnerabilities that were exploited;
   3. Act as a consultant to <COMPANY> Tech as they remove malware, inappropriate materials, and other components;
   4. If more affected hosts are discovered (e.g., new malware infections), repeat the detection and analysis steps to identify all other affected hosts, then contain and eradicate the incident for them;
5. Recover from the incident:
   1. Act as a consultant to <COMPANY> Tech as they return affected systems to an operationally ready state;
   2. Confirm that the affected systems are functioning normally;
   3. If necessary, implement additional monitoring to look for future related activity;
6. Post Incident Activity
   1. Document lessons learned;
   2. Hold a lessons learned meeting with CIRT involved in the incident;
   3. Improve process / procedures;
   4. Retain evidence

## Role: Risk & Compliance

Risk & Compliance shall be responsible for the response on data incidents and shall work in tandem with information Security on join cyber/data incidents.

1. Prepare for data incidents prior to an incident by documenting or preparing:
   1. Communications and Facilities:
      1. Contact information
      2. On-call information
      3. Incident reporting mechanisms
      4. Issue tracking system
      5. Encryption capabilities
      6. War room
      7. Secure storage facility
   2. Analysis Resources
   3. Training
2. Detection and analysis of an incident:
   1. Determine if an incident has occurred based on specific event(s);
   2. Determine the type of incident that has occurred;
   3. Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)
3. Containment of an incident:
   1. Determine containment process;
   2. Collect evidence for analysis;
4. Eradicate the incident
5. Recover from the incident:
   1. If necessary, implement additional monitoring to look for future related activity;
6. Post Incident Activity:
   1. Document lessons learned;
   2. Hold a lessons learned meeting;
   3. Improve process / procedures;
   4. Retain evidence

## Role: Data Owner

Data Owners shall:

1. Provide assessment of business impact of the incident and any measures required to contain, eradicate, and recover;
2. Act as consultant during initial analysis of systems that may need to be brought offline;
3. Make an informed decision as to when systems are ready to be returned to production status;
4. Provide resources and information as requested to support investigations.

## Role: Information Technology

The Information Technology role, which may be performed by other business unit’s IT organizations as well as <COMPANY> Tech, is responsible to minimize the impact to system end users and to assist the response team with technical issues. At <COMPANY>, this role can include <different teams>

IT or equivalent is a critical resource before, during, and after a cyber-incident. Potential incidents may be reported to a system administrator, desktop support, network support, the <COMPANY> Service Desk, remote site support staff, and/or non-IT staff doing similar jobs. Expert technical support is usually required during cyber incident response, and much of the recovery depends on such expertise as well. IT is expected to be involved in the following ways:

* Individuals who serve in these functions shall become familiar with the types of events that are potential cyber security incidents and report them immediately to the local Information Security / CIRT representative;
* Distributed Operations (DO) shall provide resources to perform initial response on local computers reporting a potential virus or other malicious code that cannot be cleaned or quarantined (see virus response procedure for more detailed information). The assigned individual shall notify the local Information Security /CIRT representative if that machine is found to be spreading the virus or other malicious code;
* Messaging shall provide support for analysis and response to any incident pertaining to Messaging-related services (such as Email and Instant Messaging);
* CO/DO/TO shall provide expert resources to aid in cyber incident response as requested by the <COMPANY> CIRT Leader for the current incident. Examples include network disable/re-enable; data capture, restore, or quarantine; emergency patch distribution; etc.
* A designated incident response business unit leader shall be advised when an incident causes impact to the business unit they support, and they shall serve as the response team's liaison to the business unit as needed

<COMPANY> Service Desk shall, depending on the category of incident:

* Create a service desk ticket regarding the possible incident;
* Notify the local Information Security / IRT representative according to the incident response process;
* Notify the person(s) who reported the incident when they may use their computer again;
* Close service desk tickets after the response team has either resolved the incident or determined the event is not a security incident.

Potential incidents may be reported to or discovered by any IT staff member, as well as non-IT staff performing similar functions:

* All IT staff members shall become familiar with the types of events that are potential cyber security incidents, report them immediately to the <COMPANY> Service Desk, and provide support as requested by CIRT for response to technology-specific issues;

## Role: IT Subject Matter Expert

* IT subject matter experts shall provide expert resources to aid in cyber incident response as requested by the <COMPANY> CIRT Leader.
* IT subject matter experts may be required to perform initial response on devices or services that they are considered a subject matter expert in to determine if a cyber-security incident exists;

## Role: Application Subject Matter Expert

* Application subject matter experts shall perform initial response on application issues to determine if a cyber-security incident exists;
* Application subject matter experts shall provide expert resources to aid in cyber incident response as requested by the <COMPANY> CIRT Leader.

## Role: Major Incident Management (MIM)

The Major Incident Management role is responsible for the coordination of resources across <COMPANY> and <COMPANY> as needed by the CIRT leader to minimize the impact to system end users and to assist the response team with technical issues. This includes:

* Locating and contacting various resources to participate in the CIRT. This includes not only resources within <COMPANY> but resources within the business unit as necessary;

## Role: Corporate Security

This role, performed by <COMPANY> corporate security staff, involves assessment of physical damage incurred, investigation of physical evidence, and guarding of evidence during a forensics investigation. Due to the overlap between physical and computer-related incidents and investigations, it is imperative Security and Information Security departments work closely together to ensure that expertise is shared appropriately to guarantee an effective, efficient process. The Security Department has its own internal procedures which shall include the following related to Information Security incidents:

1. Coordinate with the local Information Security / IRT representative when a security investigation involves computer resources on the network;
2. Contact and maintain liaison with Local, State, and Federal/National law enforcement or emergency services as required;
3. Provide physical access control to areas containing potential evidence;

## Role: Legal

The Legal role shall be performed by the Legal Department and is responsible to ensure the usability of any evidence collected during an investigation if the company chooses to take legal action. The role also includes providing advice regarding liability issues in the event that an incident affects clients, customers, vendors, and/or the general public.

Preparation:

* The General Counsel shall designate principal and back up attorneys to support the activities of the Incident Response Team.

Identification:

* Review requests for legal advice from <COMPANY> for indications of a cyber-incident and report possible incidents to the Incident Response Team.

Assessment, Containment, Remediation, and Follow-Up:

* Provide legal advice;
* Coordinate with law enforcement authorities;
* Manage civil litigation;
* Provide prior review for any proposed communications, both internal and external, which may have legal implications;
* Provide legal documents as needed.

## Role: Human Resources

This role, performed by the Human Resources management team, provides advice in situations involving employees.

The Human Resources Vice President and Director shall:

* Assign priorities to cases of inappropriate use;
* Delegate summary reports to HR Managers for review;
* Advise the local Information Security / CIRT representative on potentially volatile labor matters that could result in a technical security incident;
* Assist with any situations involving treatment of injuries or emergency services.

Human Resources Managers sometimes request investigations into an individual's use of computer resources. At other times, cases are assigned to them by the Human Resources Vice President and Director based on automated reports from the local Information Security / CIRT representative. Human Resources Managers shall:

* Review investigation reports with the Information Security staff member, requesting clarification and additional information as required;
* Follow up with investigated employee, manager, etc., as required;
* Conduct interviews and handle any disciplinary action required;
* Report outcome of turned-over investigation cases back to the local Information Security / CIRT representative for closure and proper retention of data;
* Advise the local Information Security / CIRT representative on potentially volatile labor matters that could result in a cyber-security incident;
* Assist with any situations involving treatment of injuries or emergency services.

## Role: Public Relations

The role referred to as "Public Relations within the <COMPANY> incident response policy are typically performed by the Marketing & Communications department. The Marketing & Communications role includes communication with team leaders to have an accurate understanding of the issues and the company's status before communicating with the press and/or informing the stakeholders of the current situation. The Client Relations role adds communicating with our clients, both directly and indirectly impacted.

All comments to any news media or the general public must come from either the Legal or the Risk & Compliance department, which is responsible for preparing all information destined for external public communication. Most cyber security incidents will not require public communication. When necessary, the appropriate department shall:

* Coordinate all relations with media;
* Work with Crisis Management and the <COMPANY> CISO and/or CRCO as required to develop position statements or messages on issues, and develop strategies for communicating all public messages related to a cyber-security incident;
* Ensure news releases are up to date and accurate;
* Field all media calls, maintain logs of media questions, and monitor/evaluate success or failure of communication efforts;
* Manage media personnel who may gather at <COMPANY> facilities;
* Appoint a spokesperson for the cyber security incident to be the sole person responsible for delivering any information to the public, media, or anyone outside the company.

CISO and/or CRCO shall provide resources to:

* Make internal announcements where necessary to prevent spread of malicious activity;
* Inform computer users of service issues related to the incident.

## Role: Client Relations

The role referred to as “Client Relations" within the <COMPANY> incident response policy are typically performed by a business unit representative. The Client Relations role is used for communicating with our clients, both directly and indirectly impacted.

All comments to clients must come from either the Legal or the Risk & Compliance department.

## Role: Financial Audit

The Financial Audit role is responsible for assessing the damage incurred in terms of monetary value, which is frequently required for insurance companies or if the company intends to press charges against the perpetrator. The <COMPANY> Finance Department shall:

1. Consult with IRT as needed during an incident;
2. Assess the damage incurred in terms of monetary value when required;

Training

Training shall be provided / completed as necessary to ensure individuals identified as having a role or responsibility within this policy have the skills necessary to perform the responsibilities identified.

Policy Compliance

This process becomes effective upon publication.

Definitions

Terms contained within this document are standard international terms used for information security. For general definitions, see NISTIR 7298, Rev 2 - Glossary of Key Information Security Terms (<http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>)

Resources

* NIST SP800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations

(<http://dx.doi.org/10.6028/NIST.SP.800-53r4>)

* NIST SP800-61 Rev 2, Computer Security Incident Handling Guide

(<http://dx.doi.org/10.6028/NIST.SP.800-61r2>)

* NISTIR 7298 Rev 2, Glossary of Key Information Security Terms (<http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>)

Approval and Ownership

Copy in the electronic approval of each approver. Type the name of the approver, and the date approved on each approval line on the cover page.

|  |  |  |
| --- | --- | --- |
| Owner | Title | Date |
|  |  |  |
| Approved By | Title | Date |
|  |  |  |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Rev** | **Date** | **Author** | **Description** |
|  |  |  | **Initial Draft** |