SAMPLE
Cybersecurity Incident Response Plan

AIG Cyber Risk Consulting

Cyberriskconsulting@aig.com

Revision Date: ***June 2019***

Ownership

The material contained in this Incident Response Plan, including all text, graphics, charts, and other content; all modifications, improvements, or derivative works based on or derived from the same; and all copyright, trademark, and other intellectual property and proprietary rights associated therewith, is the sole and exclusive property of American International Group, Inc.

Use Restrictions

This document is intended to act as a guide or template to assist an AIG Cyber policy holder to put in place a plan for responding to any Cybersecurity incident. This document is designed according to recommended best practices and includes AIG specific elements, such as claims contacts, etc. It is also designed in such a way that most medium to large organizations can fill in their specific information, make slight adjustments where needed, and then finalize as their plan. You may use this document only for internal business purposes. You may not utilize this document and any content herein, or any derivative work from this plan, for any commercial purpose. You may reproduce a reasonable number of copies of this document for use by your employees for your internal business purposes only. You may modify this document by incorporating your information into the blank fields within this Incident Response Plan, by adding your own definitions, by revising the sample materials, or by making other similar changes to suit your business needs, but any modified version or derivative work of this Incident Response Plan will automatically be the sole and exclusive property of American International Group, Inc.

Disclaimer

New technology, configuration changes, software upgrades and routine maintenance, among other items, inherently create new and unknown security exposures. Moreover, computer "hackers" and other third parties continue to employ increasingly sophisticated techniques and tools, resulting in ever-growing challenges to network and computer system security. This incident response plan document and the information, suggestions and recommendations contained herein are for general informational purposes only. No warranty, guarantee or representation, either express or implied, is made as to the suitability or sufficiency of this document for your business or as to the security of a company's network and/or computer systems including, but not limited to, any representation that a company's computer systems are or would be safe from intrusions, viruses, or any other security exposures. No responsibility is assumed for the discovery and/or elimination of any security exposures. The information contained herein should not be construed as financial, accounting, tax or legal advice and does not create an attorney-client relationship.

American International Group, Inc. (AIG) is a leading global insurance organization. Founded in 1919, today AIG member companies provide a wide range of property casualty insurance, life insurance, retirement products, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com and www.aig.com/strategyupdate | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance | LinkedIn: www.linkedin.com/company/aig. These references with additional information about AIG have been provided as a convenience, and the information contained on such websites is not incorporated by reference into this press release.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.

© American International Group, Inc. All rights reserved.

Contents

Document Control 5
Charter 7
Purpose of this Document 7
Security Incident Definition 7
Scope 7
Statement of Authority 7
Confidentiality 7
High Confidentiality 7
Plan Initiation 8
Severity Level Definitions 8
Critical Systems and Business Processes 10
CSIRT Organization 12
Executive Team 12
General Counsel 13
Human Resources 13
Public Relations 13
Corporate Risk Manager 13
Corporate Accounting or Finance Manager 13
Incident Response Team 14
Incident Manager 14
IT Security 14
Systems Administration 15
Network Administration 15
IT Help Desk 15
Database Administration 15
Application Development 15
Corporate Facilities 16
3rd Party Vendors 16
External Staffing Support 16
Incident Response Process Overview 17
Preparation 18
Identification 18
Triage 18
Analysis 19

© American International Group, Inc. All rights reserved.

Containment 19
Eradication 19
Recovery 20
Lessons Learned 20
Incident Documentation Requirements 21
Incident Handler's Notes 21
Reporting for Severity Level 4 21
Reporting for Severity Levels 1-3 22
AIG Claim Reporting 22
Appendix A: Definitions 23
Appendix B: IR Team Contact List 25
Appendix C: 3rd Party Vendor Contact List 27
Appendix D: External Staffing Support 28
Appendix E: AIG Claims Support 29
AIG Claims Contact 29
Appendix F: Sample Incident Summary Form 30

© American International Group, Inc. All rights reserved.

Document Control

Document Statistics

Type of Information	Document Data
Title	{Company Name} Cybersecurity Incident Response Plan
Document Version	1.0
Last Update	
Document Owner	

Document Change Approvers

Name	Role	Date Approved	Email Address

Document Change Reviewers

Reviewer	Role	Email Address

Revision History

Version Number	Version Date	Author/Reviser	Nature of Change	Date Approved
1.0			Initial Version	

Document Distribution

This document is not to be distributed to anyone outside of **<company name>** without the express written approval of the document owner and the execution of a confidentiality agreement where necessary. Due to its sensitive nature, the incident response plan and its contents will be classified as confidential and will not be freely distributed throughout the organization.

© American International Group, Inc. All rights reserved.

Document Maintenance and Testing

This incident response plan is to be considered a living document and, as such, necessitates maintenance on a regular basis. The Document Owner is responsible to update this incident response plan at a frequency of no less than once every six months.

In order to have an effective incident response plan and ensure that all CSIRT participants are well-versed in the process, the Document Owner will schedule and test the plan with members of the CSIRT team, as defined in this document, at a frequency of no less than once every year. Testing will include at least one significant mock scenario. All members of the CSIRT team, including the CSIRT Incident Manager, will participate in the mock incident.

Testing History

Test Date	Authority	Notes

© American International Group, Inc. All rights reserved.

Charter

Purpose of this Document

This Computer Security Incident Response Plan charters the ***<company name>*** Computer Security Incident Response Team (CSIRT) with providing coordinated computer security incident response throughout the entire infrastructure. The Incident Manager is the overall representative for the CSIRT, and has the responsibility and authority to manage the CSIRT and implement necessary actions and decisions during an incident.

Security Incident Definition

For the purposes of this document, an incident is defined as a security incident involving ***<company name>***'s IT infrastructure. However, a security incident may also involve business entities and third-parties that manage or provide product or support to the infrastructure and applications. Incidents involving the unauthorized disclosure, loss, or alteration of data or the inappropriate use of computer systems constitute a security incident. This document does not address availability, normal outages, and/or issues such as hardware failure and other similar issues arising from non-security related events. Such outages and issues are outside the scope of this incident response plan. However, this plan should be immediately activated if any standard incidents are discovered to involve computer security-related issues.

Scope

This incident response plan applies to all ***<company name>*** network infrastructures, systems and devices that are supported by both internal teams and third party providers, that are attached to ***<company name>***'s network, or that contain and ***<company name>*** owned data. This plan outlines the communications plans and actions taken to address computer security incidents throughout these infrastructures.

Statement of Authority

The Incident Manager is granted authority by ***<sponsoring executive>*****,** to request access to any and all systems within ***<company name>***'s infrastructure for the purpose of responding to a computer security incident.

The CSIRT has the authority to take preventive, reactive or other actions to control, mitigate and remediate an incident. Should systems critical to the environment or key business processes (defined under Critical Systems) need to be severed from the network or shut down, the Incident Manager will seek approval of executive leadership in advance of these actions. Decisions to pay any ransom demands will also require the Incident Manager to seek approval from executive leadership.

Confidentiality

During the response to an incident, the CSIRT may have access to confidential materials that are not normally accessible to its members. Individuals on the CSIRT will not disseminate, discuss, or otherwise disclose confidential material outside of the response to an incident.

High Confidentiality

Should a security incident require a high degree of confidentiality and the procedures outlined in this document be deemed inappropriate given the nature of the incident, General Counsel may determine that this CSIRP does not apply in such an incident.

© American International Group, Inc. All rights reserved.

Plan Initiation

This plan shall be activated whenever any CSIRT member discovers or is notified, through any channel, of a potential computer security incident. As the incident management process begins, the response activities will be directed by the severity level assigned to the incident. This incident severity will determine the required response and internal notification as indicated in the following section.

Severity Level Definitions

Severity levels are defined from level one through four with one being the most severe and four being the least severe. The table below provides a brief overview of how these levels may be determined based upon business impact or incident prevalence and the associated expectation of resource expenditure.

Severity	Business Impact	Scope
4	None	Isolated Systems
3	Limited	Isolated Environment
2	Moderate	Limited / More widespread
1	Severe	Widespread Sensitive Data Compromise

The following sections detail each severity level, describe the typical incident impact, incident characteristics, required notifications, and provide brief examples.

Severity Level 4

Security incidents that do not present a significant impact to business operations, financial standing, brand reputation, or regulatory obligations will be classified incident severity level 4, and handled as part of normal day to day operations. Severity Level 4 incidents require notification to the Incident Manager upon resolution or during monthly security committee meetings. However, should the incident increase in scope or severity, the Incident Manager should be notified immediately. Upon initial examination of a security event, the following characteristics will likely indicate a Severity Level 4 incident:

- Limited to very few individuals and/or systems
- Localized events requiring limited or no action outside the normal course of operations
- Minimal risk of the unresolved problem getting worse or spreading to other areas of the organization
- Normally can be resolved during normal business hours

Example Severity 4 Incident Types

- An isolated malware infection
- A single malicious phishing email or other social engineering attempt
- The identification of a system or software vulnerability
- Reports of endpoint security software policy gaps

© American International Group, Inc. All rights reserved.

Severity Level 3

Security incidents that may cause limited impact to business operations, financial standing, brand reputation, or regulatory obligations will be classified incident severity level 3. Severity Level 3 incidents must be reported to the Incident Manager immediately. The Incident Manager should update the executive team either post-resolution or as necessary, and formal lessons learned should be conducted after the incident is resolved. Upon initial examination of a security event, the following characteristics will likely indicate a Severity Level 3 incident:

- Limited to a single department and/or non-critical application
- Localized events likely requiring some action considered outside the normal course of operations
- Potential risk of the unresolved problem getting worse or spreading to other areas of the organization
- May require limited activity outside of normal business hours

Example Severity 3 Incident Types

- Localized malware event requiring limited action beyond normal operations
- Elevated levels of anomalous traffic or suspicious activity
- Unusual amounts of unsolicited email or a widespread phishing campaign
- HR investigation of or detection of inappropriate use of information assets
- Loss of an encrypted mobile device or laptop

Severity Level 2

Security incidents that present a moderate impact to business operations, financial standing, brand reputation, or regulatory obligations will be classified incident severity level 2. Incidents that have less impact but exhibit wide scale prevalence throughout the organization may also be classified severity level 2. Severity Level 2 incidents must be reported to the Incident Manager immediately. The Incident Manager should also notify the executive team immediately. The Incident Manager should update the executive team throughout the process of managing the incident to closure. Upon resolution of the incident, within a reasonable timeframe, the Incident Manager should conduct a formal lessons learned meeting. Upon initial examination of a security event, the following characteristics will likely indicate a Severity Level 2 incident:

- An incident that affects several location, systems and/or applications with direct business impact
- Increased probability of unresolved incident spreading or worsening
- Potential compromise or unauthorized release of company confidential information

Example Severity 2 Incident Types

- Observed activity indicating an active intrusion attempt
- Repeated internal attempts of inappropriate or unauthorized access attempts
- Localized malware events that require production changes to control and contain
- Localized denial of service impacting production systems
- A Cyber extortion event or any incident involving a ransom demand

© American International Group, Inc. All rights reserved.

Severity Level 1

Security incidents that present an immediate or severe impact to business operations, financial standing, brand reputation, or regulatory obligations will be classified incident severity level 1. Incidents that have less impact but are determined by legal counsel or the executive team to require increased handling may also be declared severity level 1. In addition, the potential for, or already determined, exposure of any confidential data incidents must be reported to the Incident Manager immediately. The Incident Manager should also notify the executive team immediately. The Incident Manager should update the executive team throughout the process of managing the incident so that the executive team may manage legal, reporting, PR, and other required elements for the incident. Upon resolution of the incident, within a reasonable timeframe, the Incident Manager should conduct a formal lessons learned meeting. Upon initial examination of a security event, the following characteristics will likely indicate a Severity Level 1 incident:

- An incident that affects enterprise-wide operations and/or systems and applications critical to the business
- Observed or reported unauthorized access to critical corporate IT systems
- Confirmed compromise or unauthorized release of any confidential or classified data(PII, PCI, HIPPA,GDPR etc.)
- High risk of the problem worsening or spreading to other areas of the organization

Example Severity 1 Incident Types

- Active compromise of systems containing sensitive company or client data
- Detected internal or external penetration of systems
- Denial of service activity impacting business operations
- Widespread malware event requiring coordinated enterprise activity to control
- Loss of unencrypted device containing confidential company or client data

Critical Systems and Business Processes

Security incidents involving critical systems or business processes, that if interrupted, would cause significant detriment to revenue, costs, and/or business reputation, such as the ones below, require immediate notification of the Incident Manager and a minimal classification as a Severity Level 2 incident. Any system or process including in this section must have an alternative means for ensuring business continuity documented as part of this organizations business continuity and recovery plan.

{This section should reference your corporate BCRS plan and be updated to list any systems with sensitive data or that are critical to business operations. Any critical business processes that would be affected by interruptions should also be considered and listed.}

Examples Include
Point of Sale Systems
Database Systems storing sensitive data (PCI, PII, HIPPA, GDPR, company confidential, etc.)
Active Directory
Corporate Commerce Website
Industrial controls managing the manufacturing line
IoT devices maintaining appropriate temperatures on refrigeration units

Ransom Demands and Payment

{This section should document corporate policy on paying ransom or not, or the process by which those decisions will be made in the event of an extortion or ransomware event. Resources for obtaining crypto currency, financial loans, or other to obtain necessary funds to make ransom payments, should also be considered and listed here, if applicable. Once determination has been made and wording added (you can select from examples below), remove this highlighted paragraph.}

© American International Group, Inc. All rights reserved.

{Example language 1 – No ransom payment.}
It has been determined by executive leadership of ***<company name>***, that it is our policy to never submit to any extortion or ransom demand made on our employees individually or on our business collectively. Should any ransom or extortion demand be made, the Incident Manager will work with general counsel and engage appropriate law enforcement agencies.

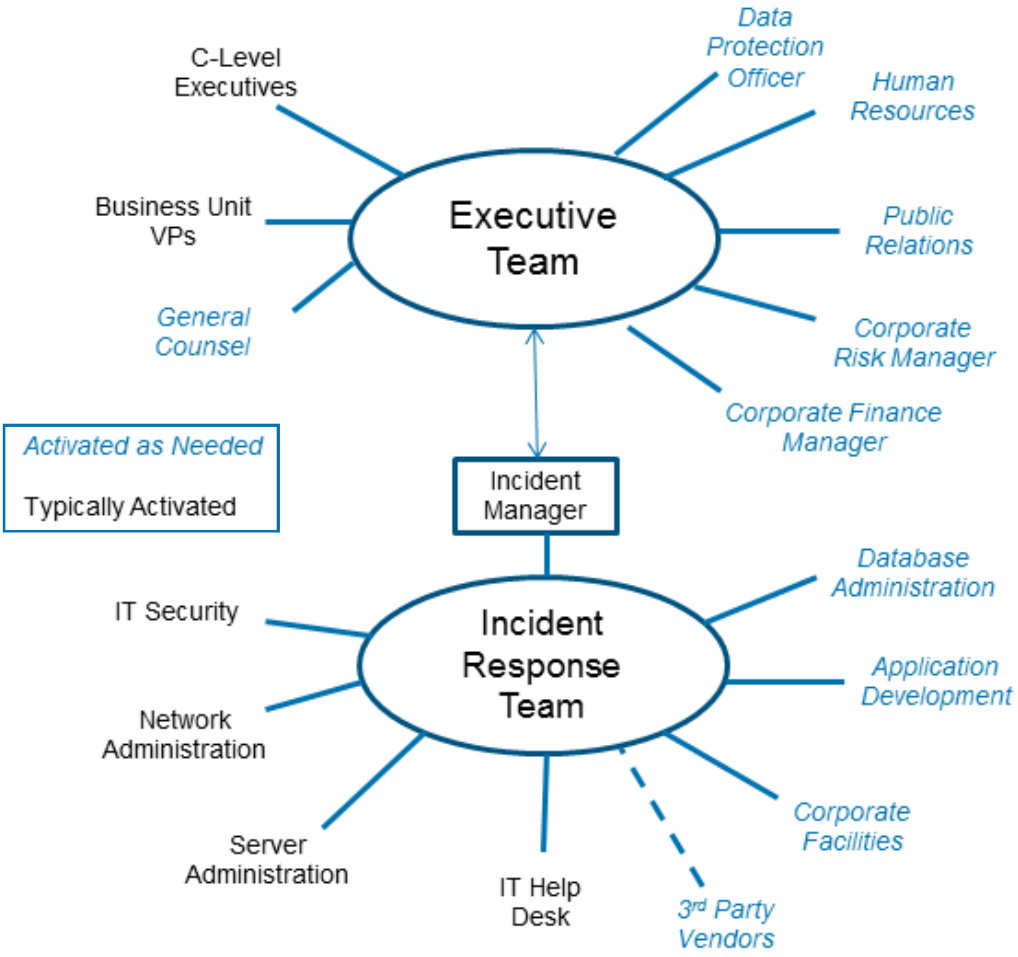
{Example language 2 – Case by case basis.}

It has been determined by executive leadership of ***<company name>***, that should any ransom or extortion demand be made, the Incident Manager will immediately engage general counsel, appropriate law enforcement agencies, and convene a meeting with executive leadership to discuss and review the current demand. Should the decision be made to pay the ransom, the Incident Manager will be authorized to work with general counsel and appropriate 3rd party resources, as identified in Appendix C, to secure the necessary funds, bitcoin, etc. and proceed with payment towards business recovery.

© American International Group, Inc. All rights reserved.

CSIRT Organization

The Computer Security Incident Response Team (CSIRT) will be led and managed by the Incident Manager under the oversight of the executive team. The CSIRT is composed of team members from several technology disciplines, as dictated by the nature and scope of the incident. The following diagram illustrates the CSIRT team structure.



Executive Team

The executive team shall evaluate key business impact decisions, and provide strategic direction to the Incident Manager. The executive team consists of vice president and above leaders in the organization as pre-determined, or as deemed appropriate by the particular incident. A member of the executive team, usually the CIO or CISO, that is not filling the role of Incident Manager, will be appointed as the focal point to receive updates from the Incident Manager and coordinate executive team actions during the course of an incident. The appointed executive will:

- coordinate necessary logistics for meetings (i.e., conference room, teleconference bridges, times)
- Provide appropriate updates to the CSIRT Strategic Team based upon incident status, issues, and findings
- Provide active, strategic oversight for Level 1 and Level 2 severity incidents
- Maintain active communication with the Incident Manager

© American International Group, Inc. All rights reserved.

- Evaluate and approve actions which may involve financial expenditure such as contracting 3rd party support vendors or ransom demand payments

Other roles, besides executive leadership, that participate in the executive team during an incident may include the following roles as described.

General Counsel

For severity level 2 or level 1 incidents, or any other incident as deemed appropriate, general counsel acts as a member of the executive team and acts as legal advisor to provide guidance in ensuring necessary legal requirements in the investigation and reporting of the incident take place in according with any federal and state legislation, and pursuant to any other applicable regulatory rules and protocols (e.g., PCI). General Counsel should understand and know these regulations prior to any incident and should train other members of the incident response team on the latest regulations. General Counsel also acts as a liaison with any outside counsel, law enforcement, and external entities/regulatory bodies, as deemed appropriate.

Human Resources

The human resources executive advises the executive team and incident manager on personnel related issues associated with misuse investigations and other incidents involving employees or employee PII. They also provide guidance on any matters pertaining to a security incident where the actions of an employee, nefarious or not, are the subject of the investigation. Any resulting disciplinary actions resulting from a violation of business policy will be also handled by the guidance of or directly by human resources.

Public Relations

Public relations is responsible for handling all internal and/or external communications that may be required during the course of handling an incident. Communications should be prepared ahead of time and pre-approved by General Counsel and Executive Leadership, especially for any external communications.

Corporate Risk Manager

The Corporate Risk Manager provides the necessary evaluation and determination of insurance claim requirements resulting from certain types of security incidents. The Corporate Risk Manager will provide appropriate insight to the Incident Manager for claims information gathering requirements, specifically regarding insurance applicability and corporate brand protection, throughout the incident management cycle. See Appendix E for AIG claims notification process and information.

Corporate Accounting or Finance Manager

The Corporate Finance manager proactively ensures that, in the event a ransom payment is involved as part of the cyber incident and the decision is made to pay the ransom, necessary means for appropriate funds are secured and available. This may include accounting contacts and securing loans from a 3rd party, or the securing of crypto currency. The Corporate Finance Manager will also provide appropriate insight to financial matters during an incident including tracking of related expenditures, costs, etc.

Data Protection Officer

The Data Protection Officer is a mandatory role for all companies that collect or process EU citizens personal data, under Article 37 of GDPR. The Data Protection Officer is responsible for educating CSIRT team members on data privacy requirements, maintaining compliance to GDPR policies, and acting as a liaison to GDPR supervisory authorities.

© American International Group, Inc. All rights reserved.

Incident Response Team

The incident response team includes the technical roles in dealing with and managing a security incident. Incident Response Team members will be assigned at the Incident Manager's discretion based upon the incident level, and on the skill sets required to effectively identify and respond to the incident. The team will execute all technical incident response tasks. Its members will:

- Perform incident response functions based on their training, in accordance with defined procedures and with guidance from the Incident Manager
- Follow the appropriate procedures and complete appropriate documentation
- Provide information on and analysis of affected systems
- Return all systems to secure, operational status in accordance with appropriate procedures (i.e., change control, business continuity/disaster recovery)

The team is managed and directed by the Incident Manager and is made up of other roles as described below.

Incident Manager

The Incident Manager shall provide direction for all members of the CSIRT Team, ensure effective management of the incident response process, and facilitate communications within the CSIRT and to the Executive Team. The Incident Manager provides oversight and direction for the CSIRT Tactical Team during an incident by:

- Directing all tasks and assignments to team members (e.g., logistics coordinator, incident scribe)
- Coordinating and directing any external support teams
- Ensuring that all appropriate incident specific response procedures are followed
- Ensuring that incidents are fully documented via the approved incident ticketing system, including lessons learned and recommendations upon closeout of the incident
- Providing appropriate status updates to the Executive Team
- Designates an alternate Incident Manager to handle incident management responsibilities as appropriate

IT Security

The IT Security team shall ensure the secure configuration and operation of the IT infrastructure. The IT Security team:

- Assesses the impact of an incident on the production server environment as appropriate
- Coordinates activities involving the systems in the environment
- Coordinates acquisition of data (i.e., volatile/non-volatile data from servers, etc.) from the production server environment
- Advises the Incident Manager regarding the impact and potential effects of an incident
- Provides guidance and support to the Incident Manager in key areas of information security
- Secures and evaluates security of network devices and/or systems
- Coordinates communication with Internet Service Providers (i.e., "upstream"), particularly during denial of service attacks, etc.

© American International Group, Inc. All rights reserved.

Systems Administration

The IT Systems Administration team shall ensure the secure configuration and operation of servers and endpoint desktop systems, either directly or via coordination with external support entities when appropriate. IT Systems Administration will:

- Assesses the impact of an incident on the production server environment as appropriate
- Coordinates activities involving all systems
- Coordinates the acquisition of data (i.e., volatile/non-volatile data, etc.) from production systems
- Advises the Incident Manager regarding the potential effects of an incident on system operations
- Provides replacement systems if end user desktops/workstations are affected by an incident

Network Administration

The Network Administration team shall ensure the secure configuration and operation of all network routers, firewalls, and other devices, either directly or via coordination with external support entities when appropriate. Network Administration will:

- Assesses the impact of an incident on the network as appropriate
- Coordinates activities involving all firewalls, routers, and other network devices
- Coordinates the acquisition of logs from network devices
- Advises the Incident Manager regarding the potential effects of an incident on the network

IT Help Desk

Liaises with the organization's end user community during the incident and has responsibility to:

- Receive notifications of possible incidents from the end user community (and other sources, as appropriate)
- Develops the best process to validate changes and track tickets related to the incident
- Manages the incident ticketing system
- Escalates reported incidents as appropriate
- Can create a 'greeting message' to notify callers of a potential issue causing an impact to the workforce

Database Administration

- Advises the Incident Manager regarding the potential effects of an incident on database operations
- Helps to assess the impact/scope of any level of compromised sensitive data
- Collects and preserves database logs, schema information, backups, and other documentation to support incident response efforts involving database systems

Application Development

- Advises the Incident Manager regarding the potential effects of an incident involving any company developed applications
- Assists with the analysis of developed applications if a compromise is suspected or confirmed

© American International Group, Inc. All rights reserved.

- Provides development support for security vulnerability mitigation in developed applications

Corporate Facilities

- Supports the Incident Manager by providing access to physical facilities for vendors and contractors when necessary during incident response engagements
- Ensures and documents the secure handling of systems, media, or devices which are received via parcel shipping, and provides notifications to the Incident Manager as necessary
- In the event an incident involves a potential physical security breach, corporate facilities management will assist with security efforts to identify and mitigate the breach and implement any temporary defensive measures

3rd Party Vendors

Any 3rd party vendor support provided to manage organizational systems, data, or applications should have appropriate contractual agreements in place, prior to an incident, for necessary support. 3rd party vendors will:

- Alert to any incidents on the systems managed by them on behalf of ***<company name>***
- Provides tactical support for systems and applications under their purview
- Advises the Incident Manager regarding the potential effects of an incident on those systems
- Collects and preserve database logs, schema information, backups, and any other relevant documentation to support incident response efforts involving those systems
- Provides updates and reports to the Incident Manager on their activities

Please refer to *Appendix C: 3rd Party Vendor Contact List* for a list of contacts of third party vendors employed by ***<company name>***.

External Staffing Support

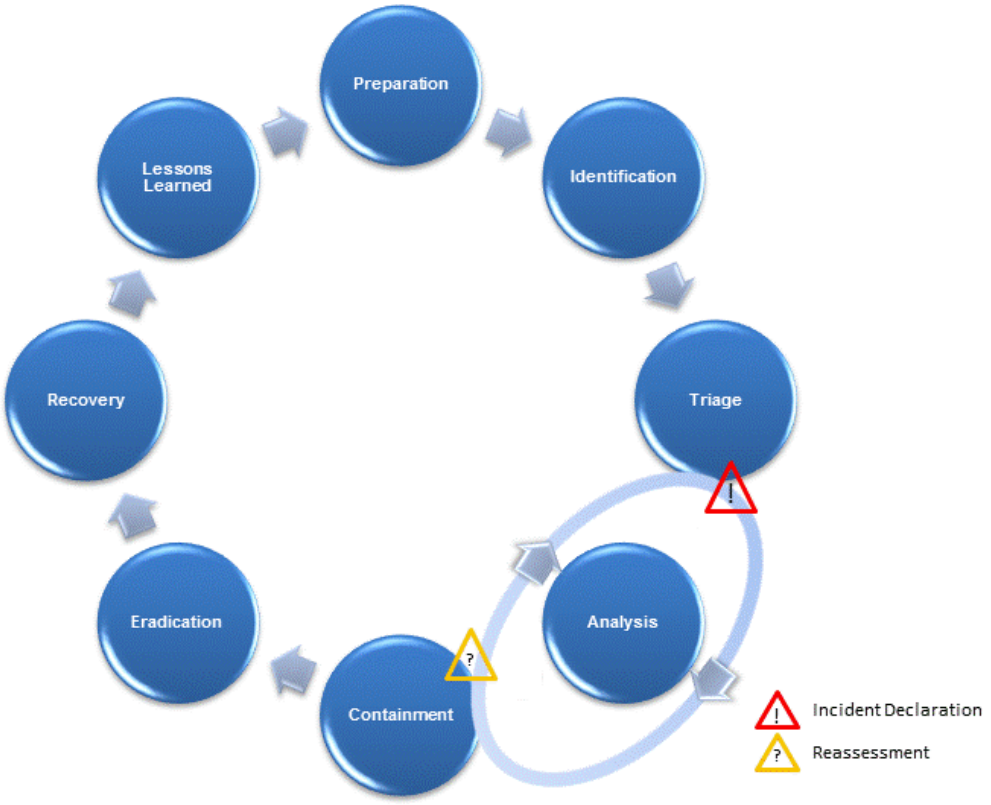
When required, and with the approval of the Executive Team, the Incident may choose to engage additional external, third party resources to support the incident response efforts. This necessity may arise in instances where additional technical knowledge and support is essential, when mandated by regulatory bodies, or when impartial due diligence is required. These external parties may include, but are not limited to security service providers, legal counsel, incident response and forensics support, and Internet Service Providers (ISP).

In some cases, relationships with these entities may already be contracted and in place. In these cases, please refer to Appendix D: External Staffing Support, for a list of contacts that may be employed for external staffing support. Where relationships are not pre-existing and yet support is required, work with the AIG Cyber claims team to secure necessary external support resources.

© American International Group, Inc. All rights reserved.

Incident Response Process Overview

This plan does not provide specific steps for handling different types of security incidents, but instead provides a general process for handling all IT security incidents. The following diagram outlines the phases involved in the handling of all IT security incidents. Although various industry standards[1] reference 4 to 7 distinct phases in the incident response process, this incident response plan contains 8 phases that have been adapted from those standards to highlight key points in the decision-making processes.



The following table provides a summary of each of these phases, which are detailed in the subsequent sections.

Preparation	Ongoing activities to prepare the incident response team for effective and efficient incident response
Identification	Security incident detection and initial reporting
Triage	Assessing the details, scope, and severity of the inident to determine incident declaration
Analysis	Conducting analysis as new incident indicators are discovered
Containment	Preventing the spreading of the incident
Eradication	Removing and resolving any and all problems related to the incidet
Recovery	Implementing mitigations and restoring normal operations
Lesons Learned	Identifying lessons learned and implementable recommendations

[1] NIST Special Publication (SP) 800-61 Revision 2, ISO/IEC 27035, CMU/SEI-2003-HB-002

© American International Group, Inc. All rights reserved.

Preparation

The preparation phase of the incident response process includes all those actions taken to prepare for computer security incidents, including maintenance of this incident response plan and the establishment of the CSIRT Team. Additional actions taken in this step may include, but are not limited to:

- Development of network diagrams showing logical locations and relationships of systems and devices
- Identification of critical systems, including those that store and/or process sensitive data
- Application and operating system hardening, performed in accordance with documented guidance
- Installation/deployment of security and security monitoring devices or applications
- Training of the CSIRT through online/classroom delivery, mock incidents, and self-study
- Ensuring appropriate logging at key locations is active and that the resulting logs are retained according to current retention policies
- Diligent monitoring of various security systems, applications, and logs such as intrusion detection systems, firewalls, proxy servers, antivirus consoles, and system event logs
- Incorporation of lessons learned and resulting recommendations from previous incidents

Identification

The identification phase involves the initial observation, whether receiving a tool based alert or call from an employee, of a potential security incident and the notification of the CSIRT. All employees should be trained and understand who to contact in the event an employee discovers or suspects an IT security incident. These notifications may include, but are not limited to:

- Communication to the help desk of an anomalous issue
- Policy violations or unauthorized activity observed during security monitoring and log review
- Security tool alerts monitored by IT personnel and identified as relevant security issues
- Reports of stolen laptops or other similar equipment, including mobile devices
- Reports from vendors managing systems or applications
- External report of a suspected compromise or data breach

Triage

The triage phase involves assessing the details of the reported incident to determine the validity and scope, and to determine the appropriate severity level. The CSIRT is organized by the Incident Manager, except in Severity Level 4 incidents – to collect data and conduct analysis of the incident regardless of the method by which the notification arrives. The activities of the triage phase include, but are not limited to:

- Determination of the scope of the compromise
- Initial assessment and classification of the incident
- Resource identification and assignment to response and recovery teams
- Volatile and non-volatile data collection
- Assessment of the possibility of sensitive information disclosure
- Official declaration of the incident

© American International Group, Inc. All rights reserved.

The result of the triage phase is a decision regarding ***incident declaration*** and the initiation of the remaining phases of the incident management cycle. Formal declaration by the designated authorized declarer for the incident severity level enforces the chain of command. It also provides the appropriate oversight for decisions which may lead to significant expenditure of corporate resources and/or finances. Once an incident declaration has taken place, depending on the severity, the executive team should consider notifying AIG Claims, see appendix E, for reporting First Notice of Loss and receiving additional assistance as needed.

Analysis

The analysis phase ultimately encompasses the activities undertaken during the adjacent phases of the response efforts. Reported and collected data must be analyzed and evaluated based upon both known and unknown facts about the incident. Depending upon the nature and severity of the incident, this phase may involve some or all of the following activities:

- Additional data collection and forensic imaging as necessary
- Network log analysis
- Volatile data analysis
- Forensic media analysis
- Timeline generation and analysis
- Threat research and analysis
- Basic root cause analysis

Containment

The objective of the containment phase is to take steps to contain the incident and prevent it from compounding or propagating to other areas of the environment. The Incident Manager will identify resources necessary to implement the containment plan and assign tasks to appropriate resources. If any tasks have a significant chance of impacting business operations, these tasks must be authorized by the Executive Team before being performed.

As this phase proceeds, additional incident intelligence may be gathered, prompting a ***reassessment*** which may result in additional analysis, new or modified containment plans, or even a re-evaluation of the scope and severity of the incident. Activities performed during this phase include:

- The CSIRT Team finalizes a current containment plan
- The Incident Manager assigns tasks to appropriate personnel
- Plans with no substantial risk of business impact are implemented immediately, adhering to any emergency change control procedures
- Plans having significant risk of business impact require approval of the CSIRT Incident Officer and/or CSIRT Strategic Team before implementation

Eradication

The objective of the eradication phase is to take steps to completely eradicate all signs and symptoms of the incident from the organization. After each problem or issue is successfully contained, the CSIRT Team will develop plans and the Incident Manager will assign appropriate resources to complete these plans. If any tasks have a significant chance of negatively impacting business operations, they must be approved by the Executive Team before implementation. Activities performed include:

- The CSIRT Team finalizes plans for eradicating the incident issues

© American International Group, Inc. All rights reserved.

- The Incident Manager assigns tasks to appropriate resources
- Plans with no substantial risk of business impact are implemented immediately following emergency change control procedures where appropriate
- Plans having significant risk of business impact require approval of the CSIRT Incident Officer and/or CSIRT Strategic Team before implementation

Recovery

The recovery phase includes restoring normal operations, investigating the incident's cause, and assessing its impact. The Incident Manager will create and assign CSIRT members to restore affected systems and services to their original state. Once production activities have been restored, the CSIRT schedules postmortem activities to identify and document the root cause and business impact of the incident. The postmortem should also include plans to remediate any identified issues and isolate specific preventive improvements to be further explored in the lessons learned phase and potentially implemented.

- The actions to recover affected resources as defined and determined during the containment phase are implemented
- Resources that do not require configuration changes are then returned to pre-incident state
- Resources that require configuration changes to prevent the incident's reoccurrence are updated, tested, and redeployed

Lessons Learned

The CSIRT Incident Manager is responsible for ensuring that following an incident, a formal lessons learned or review meeting is conducted to capture any recommendations, plan/process improvements, and technical considerations that have been encountered during the incident. These lessons learned should be documented in the incident tracking database or via another agreed upon form of record prior to the incident being formally closed out. Any lessons learned enhancements and any recommendations made may then be used in the cyclical preparation phase to improve protection, detection, and identification of future computer security incidents. The objective of the lessons learned phase is to:

- Identify resources needed to prevent incident reoccurrence
- Identify any policy or procedural changes that need to be implemented to prevent incident reoccurrence
- Identify any modifications to the Incident Response Plan that will allow a quicker and more effective response to similar incidents in the future
- Document the incident, findings, and lessons learned in a final incident report
- Feed lessons learned and resulting recommendations into the preparation phase as the incident response cycle repeats

The CSIRT Incident Manager will:

- Determine the time frame for the lessons learned to be performed
- Perform a formal postmortem review to identify the incident's root causes and areas for improvement for all Severity Level 1 through 3 incidents
- Report findings to the Incident Officer and CSIRT Strategic Team as appropriate
- Request necessary policy and procedural changes and/or controls related to the business and technology practices to address the specific root cause of the incident

© American International Group, Inc. All rights reserved.

Incident Documentation Requirements

As part of the incident response process, documentation must be maintained for various purposes:

- It may be required in incidents resulting in civil or administrative action
- It is required as part of the incident review process
- It is key to the incident review and lessons learned phase in order to identify elements of success and areas for improvement

Whatever the nature of the incident, documentation must be maintained accurately. There are several tools that should be used by the CSIRT as part of this process.

Incident Handler's Notes

Individual members of the incident response team may maintain handwritten notes as part of their documentation. Electronic systems may not be available during an incident, nor are they always appropriate for the information that is collected. A simple bound notebook with numbered pages (ensure that no pages are removed) is very effective. This should only be used for incident handling. Notes should be taken professionally, using sufficient detail so that they might be used to re-create the steps taken in chronological order months, or even years later. Since these notes may be required as part of legal or administrative action, it is imperative that they are professional and do not contain extraneous information (doodling, etc.). Notes should be limited to specific facts and should avoid interpretation or implication of fault or intent.

Reporting for Severity Level 4

Severity Level 4 incidents are handled by trained operations staff as part of day to day operations and within the guidelines of this plan. Although less severe in nature, appropriate details must still be recorded and reported to allow follow-up review to occur. This is important for ongoing improvement since metrics on the frequency and type of incident and other details in Severity Level 4 incidents may lead to better preventive measures. Data reported via these systems should include:

- The date the incident was reported and who reported it
- Date and time the incident occurred (may be different from when reported)
- Type of incident
- Name of the incident handler
- What events were reported (log entries, unusual system behavior, etc.)
- The extent of the incident
- What steps were performed to stop the incident from spreading
- What was done to eliminate the problem?
- How & when were normal operations restored?
- Date the incident was closed

© American International Group, Inc. All rights reserved.

Reporting for Severity Levels 1-3

Incidents of higher severity require a more formal process and wider participation by members of the CSIRT Team. Incidents of this severity should be reported and tracked with unique case numbers assigned and with appropriate level of detail. Careful attention should be paid to evidence gathering and tracking as advised by General Counsel for specific types of incidents. Information tracked should include the following:

- Identification and location of all affected systems
- Specific information on what events, logs, witness reports, etc. were correlated during the incident
- Date, time, and names of CSIRT Team members involved and their roles
- Description of steps taken to contain, eradicate and recover from the incident:
- Were systems taken offline? Which ones? For how long? What approval was obtained?
- Was data lost (or destroyed) and if so, was it recovered, when and how?
- What conclusion was arrived at as to the cause of the incident (e.g., specific malware or intrusion)?
- What was done to eradicate the incident? Were systems rebuilt or reimaged?
- What steps were implemented to prevent reoccurrence? Were any system configurations changed?
- What testing and corresponding approvals were required?
- How and when were services restored? Were build images modified and tested? What validation was done prior to returning to normal operations?
- What monitoring was implemented to watch for reoccurrence?
- Summary of the lessons learned phase including recommendations made, those implemented, and those not pursued.

AIG Claim Reporting

While managing the security incident, the Incident Manager should coordinate with the Corporate Risk Manager to ensure the appropriate amount of documentation that will assist in the reporting of a claim to AIG is captured. For further details refer to Appendix E: AIG Claims Support.

© American International Group, Inc. All rights reserved.

Appendix A: Definitions

The following table includes definitions for certain terms used throughout the Incident Response Plan

BCRS	Business continuity and recovery plan. In other words, documented process for recovering critical business systems and processes in the event of a disaster or cyber-attack. Business continuity plans should also include alternate methods for maintaining critical business processes.
CSIRP	Computer Security Incident Response Plan. In other words, a documented plan for responding specifically to a Cybersecurity incident.
CSIRT	Computer Security Incident Response Team
Incident Manager	Position responsible for coordinating and managing the IR Tactical Team's response to an incident
Executive Team	The management, business, and executive level personnel who decide on incident response actions that have any significant business impact
Critical Data	Any data, on premises or 3rd party hosted, that contains any client or employee data that is considered confidential, personally identifiable (PII), financial, or health related.
Critical Systems	Any device, on premises or 3rd party hosted, that stores, processes, or transmits critical data, or that is part of critical business processes, that if halted, would negatively affect services, revenue, and business reputation.
CSIRT Team	Refers to all personnel, tactical and strategic, responding to or assisting in the response to an incident
Customer Data	Customer data includes, but is not limited to, customer PII, PCI, and PHI, as well as customer financial, strategic marketing and confidential business information. The incident response plan requires notification of the executive team in incidents involving customer data.
Forensic Media Analysis	The use of repeatable analysis methods and techniques that employ tested procedures and tools to recover and analyze artifacts from a media device associated with a security incident.
Forensic Image	An exact bitstream (bit-by-bit) duplication of a media device into a file to be used for forensic media analysis.
GDPR	Europe's General Data Protection Regulation. Requirements for management of European citizen data, notification of breach within 72 hours, data protection officer, etc. (https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en)
HIPAA	Health Insurance Portability and Accountability Act
Incident	When used in the context of this incident response plan, see *Security Incident.*
Incident Indicators	Descriptive artifacts or observable characteristics with which to associate or describe incident activity. Often referred to as Indicators of Compromise (IOC).
Incident Management Cycle	Recommended IR Management procedures that the Incident Manager is required to manage and follow until incident resolution
IR	Incident Response
Non-Volatile Data	Data which is not subject to frequent change and is most likely recoverable when power is removed from a computer device.
PCI	Payment Card Industry information is any data regulated by the Payment Card Industry Security Standards Council (or similar foreign regulatory body) and commonly includes information related to credit cards, debit cards, ATM cards, prepaid cards, and other similar financial instruments. There is a legal obligation to report PCI-related incidents in the United States and most other countries. The incident response plan requires notification the executive team in incidents involving PCI.

© American International Group, Inc. All rights reserved.

PHI	Protected Health Information are individually identifiable data elements (e.g., names, telephone numbers, medical record numbers, serial numbers, etc.) explicitly linked to health information of a particular individual, or that could be reasonably expected to allow individual identification. PHI is protected under various laws, including HIPAA, HITECH, and other similar legislation in the United States and abroad. The CSIRP requires notification of the executive team in incidents involving PHI.
PII	PII is defined as Information that can be used, either alone or in combination with other information, to identify or trace a unique person. It includes, but is not limited to, national and state identifiers such as a Social Security number (SSN) or driver's license number, name, address, telephone number, email address, date of birth, place of birth, mother's maiden name, credit card number(s), financial accounts, passwords, medical information and biometric data. Anonymous and de-identified data are not considered PII. PII is protected under various laws both in the United States and abroad. There may be a legal obligation to report incidents involving PII to regulatory authorities. The CSIRP requires notification of the executive team in incidents involving PII.
Security Incident	Any event, actual or reasonably suspected to have occurred, which destroys or degrades the availability, integrity and/or confidentiality of information system resources, computer-based systems, computer-maintained data files, and electronically-based documents or procedures. Security incidents include the unauthorized disclosure, loss, or alteration of data, or the inappropriate use of network of computer systems.
Sensitive Data	Any data deemed sensitive by data classification policies, regulatory requirements, or information critical to the business. This may also include PII, PCI, HIPPA, GDPR or other forms of data.
Severity Level 1	Security incidents that may present an immediate or severe impact to the business operations, financial standing, brand reputation, or regulatory obligations. Incidents meeting the level 2 threshold of business impact but exhibiting widescale prevalence or impact throughout the enterprise fall under this category. Incidents involving the exposure, degradation, or loss of any sensitive or customer data.
Severity Level 2	Security incidents presenting a moderate potential impact to business operations, financial standing, brand reputation, or regulatory obligations. These may include incidents meeting lower thresholds of business impact but exhibiting wider scale prevalence throughout the organization.
Severity Level 3	Security incidents presenting a limited potential impact to business operations, financial standing, brand reputation, or regulatory obligations.
Severity Level 4	Security incidents that do not present any significant impact to business operations, financial standing, brand reputation, or regulatory obligations.
Volatile Data	Data which is subject to frequent change and is likely lost upon termination of the power source to a computer device. RFC3227 outlines the order of volatility.
Volatile Data Analysis	The use of repeatable analysis methods and techniques that employ tested procedures and tools to analyze and recover artifacts from volatile data which has been collected from live systems and preserved.

© American International Group, Inc. All rights reserved.

Appendix B: IR Team Contact List

IR Conference Bridges

Bridge Designation	Authorized Users	Numbers and Codes
CSIRT Team	Incident Manager Tactical Team Members	*Bridge:* <NUMBER> *Participant Code:* <Code> *Moderator Code:* <Code>
Executive Team	Executive Team Members	*Bridge:* <NUMBER> *Participant Code:* <Code> *Moderator Code:* <Code>

Incident Manager

The <POSITION> shall serve as the Incident Manager. An alternate has been designated in the event of his/her unavailability or need for rotations.

Role	Contact Name	Contact Info
Primary IM	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Alternate IM	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>

CSIRT Team

The Incident Manager shall assemble the appropriate members of the CSIRT Team as needed to appropriately manage the incident. The CSIRT team members have been organized by IT function in the contact list below. 3rd party support contacts are contained with Appendix C.

Role	Contact Name	Contact Info
IT Security (primary)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
IT Security (alternate)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Systems Administration (primary)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Systems Administration (alternate)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
IT Helpdesk (primary)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Network Administration (primary)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>

© American International Group, Inc. All rights reserved.

Network Administration (alternate)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Database Administration Team (primary)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Database Administration Team (alternate)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Application Development Team (primary)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Application Development Team (alternate)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Corporate Facilities Management (primary)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Corporate Facilities Management (alternate)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>

Executive Team

The designated executive focal for the incident shall assemble the appropriate members of the Executive Team on the basis of the following primary contacts:

Role	Contact Name	Contact Info
C-Level Executive (primary)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
C-Level Executive (alternate)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Business Unit VPs (primary)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Business Unit VPs (alternate)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
General Counsel (primary)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
General Counsel (alternate)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Risk Management (primary)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Risk Management (alternate)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE>

© American International Group, Inc. All rights reserved.

		E-mail: <email>
Human Resources (primary)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Human Resources (alternate)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Public Relations (primary)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Public Relations (alternate)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Accounting (primary)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email
Accounting (alternate)	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email

Appendix C: 3rd Party Vendor Contact List

The following table contains a list of contacts for all 3rd party services provided to the organization that may be called upon in the event of a security incident. These may include cloud hosting services, managed IT service providers, contracts for critical device maintenance, etc.

Vendor Name	Service or Product Provided	Contact Info
{Vendor Name}	{Service or Product Description}	*Name: <CONTACT NAME>* *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}	{Service or Product Description}	*Name: <CONTACT NAME>* *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}	{Service or Product Description}	*Name: <CONTACT NAME>* *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}	{Service or Product Description}	*Name: <CONTACT NAME>* *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}	{Service or Product Description}	*Name: <CONTACT NAME>* *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}	{Service or Product Description}	*Name: <CONTACT NAME>* *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}	{Service or Product Description}	*Name: <CONTACT NAME>* *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>

© American International Group, Inc. All rights reserved.

Appendix D: External Staffing Support

The information contained in this appendix refers to previously established contractual relationships with 3rd party vendors that may be called upon to assist in the event of a security incident.
{For North American clients, it is recommended that these firms are selected from the AIG Post-Incident Partners and Vendors List, to ensure claims coverage. Appendix F contains a link and current list of those firms that a client can select from to pro-actively establish contractual relationships in the event of an incident. Refer questions to cyberedge@aig.com or cyberriskconsulting@aig.com.}

Vendor Name	Contract Service Provided	Contact Info
{Vendor Name}	AIG Cyber Claims	*Name:* AIG Cyberedge claims Hotline *Office:* 1-800-CYBR-345(1-800-292-7345) *E-mail:* cyberedge@aig.com See Appendix E..
{Vendor Name}	External Legal Counsel	*Name:* <*CONTACT NAME*> *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}	Forensics and Incident Response Services	*Name:* <*CONTACT NAME*> *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}	Public Relations Counsel	*Name:* <*CONTACT NAME*> *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}	Local Law Enforcement	*Name:* <*CONTACT NAME*> *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}	Local FBI Office	*Name:* <*CONTACT NAME*> *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}	IT Staff Augmentation	*Name:* <*CONTACT NAME*> *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}	Forensics Accounting	*Name:* <*CONTACT NAME*> *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}	{Service Description}	*Name:* <*CONTACT NAME*> *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}	{Service Description}	*Name:* <*CONTACT NAME*> *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>

© American International Group, Inc. All rights reserved.

Appendix E: AIG Claims Support

To ensure a smooth and efficient claim handling process, and/or receive additional guidance and assistance in managing the incident, it is very important to contact AIG CyberEdge Claims as soon as you suspect or know a cyber incident has occurred.

AIG Claims Contact

If you suspect a cyber incident has occurred, or is in progress, call AIG's CyberEdge® Claims Hotline immediately ((24/7/365):

1-800-292-7345

Once a call is made, the AIG CyberEdge Claims Team will coordinate with your organization, if needed, to assist with your response plan by engaging any necessary vendors including breach counsel and forensics firms to identify immediate threats, and start the restoration and recovery process. The claims team will also assist you in processing your first notice of loss to AIG to begin the claims process. See Appendix F for a list of firms that are currently approved to work with by the AIG CyberEdge Claims team.

Contacting a CyberEdge partner or vendor prior to reporting the claim or event to AIG does not constitute formal notice of a claim. Services performed by any vendor prior to providing notice to AIG may not be covered under your policy.

Providing a detailed first notice of loss is very important to a smooth and efficient claim handling process. In particular, a first notice of loss should contain information such as:

- **A description of the nature of the event or claim** - For example, was it a computer or network security failure such as a data breach or ransomware event, or was it a privacy event resulting from the unauthorized/accidental disclosure of hard copy documents containing customer or employee confidential information (PII or PHI)); or was it a distributed denial of service attack, or a network interruption claim leading to possible lost profit or additional operational expenses.
- **When the event was first discovered**

After the incident has been handled, more detailed information can be submitted to AIG in a proof of loss. Utilizing a form, like the sample incident form in Appendix F, can help to gather the detailed information needed. Information and supporting documentation needed to complete the Proof of Loss will depend on the circumstances surrounding the security incident and the Loss being claimed. Information required for the proof of loss, that should be gathered during and after an incident includes:

- **Detailed information about the security incident**
- **What expenses were incurred as a result of the event (forensics, legal, identity protection coverage, etc.)**
- **Why the expenses were necessary and reasonable**

© American International Group, Inc. All rights reserved.

Appendix F: Sample Incident Summary Form

Form Use

Only one copy of this form is maintained per investigation. If multiple copies are developed as part of the investigation, the assigned incident manager for the specific incident must consolidate them into one form. All copies used to aggregate the summary form must be retained. Each form must include the identity of the person(s) completing it along with the employee's full name and contact information.

Investigative Incident Summary Form

PURPOSE

This document must be filled out completely during an incident investigation. Each field in this form is required in order to comply with the Computer Security Incident Response Plan.

INSTRUCTIONS

This form must be completed in ink. If corrections must be made, simply draw a single line through the item and correct the information. Initial and date any corrections on the form. Blue or black ink is preferred.

INVESTIGATION FORM	
CASE NUMBER	
INCIDENT DECLARATION (mm/dd/yyyy)	
DATE INCIDENT OCCURRED (mm/dd/yyyy)	
SEVERITY LEVEL	☐ SEVERITY 1 ☐ SEVERITY 2 ☐ SEVERITY 3 ☐ SEVERITY 4

INCIDENT MANAGER NAME (FIRST, MIDDLE INITIAL, LAST)			
OFFICE	**MOBILE NUMBER**	**PAGER NUMBER**	**HOME NUMBER**
NAME OF INVESTIGATION REQUESTOR			
NAME OF INVESTIGATOR APPROVER *(NOTE: ONLY THE GENERAL COUNSEL AND/OR HUMAN RESOURCES CAN APPROVE AN INVESTIGATION)*			
SIGNATURE OF REQUESTOR *(SEE NOTE ON DATE LINE BELOW)*			
DATE OF REQUEST *(NOTE: THE SIGNATURE AND DATE CAN BE EXECUTED AFTER THE FACT WITH SUPPORTING COMMUNICATIONS. THE DATE IS THE DATE OF THE REQUEST, NOT THE DATE OF THE SIGNATURE.)*			

PAGE _____ OF _____

© American International Group, Inc. All rights reserved.

DETECTION PROCESS (HOW WAS THE INCIDENT DISCOVERED?)

WAS THE INCIDENT REPORTED TO THE EXECUTIVE TEAM?	☐ YES ☐ NO
Who reported the incident?	
Date and time incident was reported.	
If No, explain why it was not reported.	

WAS THE INCIDENT PUBLICLY DISCLOSED?	☐ YES ☐ NO
NAME OF PERSON RELEASING INFORMATION	
NAME OF PERSON AUTHORIZING RELEASE	
DATE OF AUTHORIZATION	
DATE OF RELEASE	
COMPLETE TEXT OF RELEASED INFORMATION	

© American International Group, Inc. All rights reserved.

POLICY INFORMATION	
WAS THE INCIDENT A VIOLATION OF A CORPORATE POLICY? (I.E., ACCEPTABLE USE)	☐ YES ☐ NO
IF **YES**, STATE THE POLICY AND ATTACH A COPY OF THE POLICY TO THE BACK OF THIS FORM.	

SUMMARY OF ACTIONS TAKEN BY INVESTIGATIVE TEAM

PAGE _____ OF _____

© American International Group, Inc. All rights reserved.

EVIDENCE COLLECTION INFORMATION	
LOCATION WHERE EVIDENCE WAS FOUND	☐ SERVER ROOM ☐ CUBICLE / OFFICE ☐ DATA CENTER ☐ HOME OF SUSPECT ☐ OTHER _____
STREET	
CITY	
STATE	
COUNTRY/PROVINCE	

EVIDENCE CUSTODIAN INFORMATION	
Name	
TITLE	
COMPANY	
CONTACT NUMBER(S)	

IT ACTION ITEMS
REQUIRED ACTION ITEMS TO ENSURE NON-REPEATABILITY OF VIOLATION (E.G., RETRAIN XYZ DEPARTMENT IN USER POLICY, PRACTICES, AND PROCEDURES AND/OR ENSURE PASSWORDS ARE NOT SHARED)

CRIMINAL ACTION
WAS ANY CRIMINAL ACTION INVOLVED? IF SO, EXPLAIN WHAT DEPARTMENTS WERE CONTACTED AND THE OUTCOME OF THIS COMMUNICATION.

PAGE _____ OF _____

© American International Group, Inc. All rights reserved.

CIVIL ACTION
WAS ANY CIVIL ACTION TAKEN? IF SO, EXPLAIN WHO WAS CONTACTED AND A SUMMARY OF THE DECISION.

ADMINISTRATIVE ACTION
WAS ANY ADMINISTRATIVE ACTION TAKEN? IF SO, EXPLAIN WHO WAS CONTACTED AND A SUMMARY OF THE DECISION.

LIST INDIVIDUALS WHO WERE INTERVIEWED & CONTACTED			
NAME	BUSINESS UNIT/DEPT.	CONTACT NUMBER	EMAIL ADDRESS

PAGE _____ OF _____

© American International Group, Inc. All rights reserved.

FORENSIC INVESTIGATION ACTIVITY		
LOCATION	INDIVIDUAL(S)	ACTIVITY SUMMARY

INCIDENT CLOSED AUTHORITY		
NAME	TITLE/POSITION	BUSINESS UNIT/DEPARTMENT
REASON FOR CLOSING THE INCIDENT		

_____

Print Name

_____

Position and/or Title

_____

Signature and Date

© American International Group, Inc. All rights reserved.