SAMPLE
Cybersecurity Incident Response Plan

For
Small Businesses

AIG Cyber Risk Consulting
Cyberriskconsulting@aig.com

Revision Date: ***July 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 establish 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 small organizations, with limited resources, can simply add specific information, unique to their business, make slight adjustments where needed, and then finalize as their cyber incident response plan. You may use this document only for internal business purposes and 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.

Contents

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 Approver

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.

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 least annually.

In order to have an effective incident response plan with trained incident response team members, the Document Owner will schedule and test the plan with members of the incident response team, annually. Testing will include at least one significant mock scenario. All employees with defined responsibilities within this plan will participate.

Testing History

Test Date	Authority	Notes

Charter

Purpose of this Document

This Computer Security Incident Response Plan defines the process by which ***<company name>*** will manage and respond to any cybersecurity incident. The Incident Manager has the responsibility and authority to manage the incident and any actions to respond and recover during an incident.

Cybersecurity Incident Definition

For the purposes of this document, an incident is defined as any incident impacting the confidentiality, availability, or integrity of any ***<company name>*** IT asset or sensitive data. A cybersecurity incident may also involve business entities and third-parties that manage or provide product or support to IT assets, applications, or sensitive data. Incidents involving the unauthorized disclosure, loss, or alteration of data or the inappropriate use of computer systems constitute a cybersecurity incident.

Scope

This incident response plan applies to ***<company name>***'s network, systems, and any device that is owned and supported by employees or that may be managed by a third party, or that contain any ***<company name>*** owned data and outlines the process for all necessary actions to address any computer security incident affecting any such assets.

Statement of Authority

The Incident Manager maintains appropriate authority to request access to any and all systems within ***<company name>***'s infrastructure and to take preventive, reactive or other necessary actions to control, mitigate and remediate any incident.

Confidentiality

While responding to an incident, some employees may have temporary access to confidential or privileged materials that are not normally accessible. Individuals working on an incident will not disseminate, discuss, or otherwise disclose confidential material outside of the response to an incident.

Privileged Status

If determined by General Counsel that by nature of the cyber incident it be handled under privileged status, instructions from General Counsel should be closely adhered to in addition to steps followed within this documented plan for appropriate communications and evidence and document retention.

Plan Initiation

This plan shall be activated whenever any company employee or 3rd party service provider discovers and reports a potential cybersecurity 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 will be assessed and categorized as low or high severity. The table below provides a brief overview of how these levels may be determined based upon business impact or incident with more detailed definitions following.

Severity	Business Impact	Scope
Low	Limited to none	Isolated systems
High	Moderate to Severe	Widespread Sensitive Data Compromise Significant Business Interruption

Low Severity Incidents

Security incidents that do not present a significant impact to business operations, financial standing, brand reputation, or regulatory obligations will be classified as low incident severity and handled as part of normal day to day operations. Low severity incidents require only to be tracked for general reporting. 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 Low severity incident:

- Limited to one to two 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
- Can be resolved during normal business hours

Example Low Severity Incident Types

- An isolated malware infection
- A single malicious phishing email or other social engineering attempt against a non IT admin
- The identification of a system or software vulnerability

High Severity Level

Security incidents that impact business operations, financial standing, brand reputation, or regulatory obligations will be classified as high severity incidents. Incidents that have less impact but are determined to require increased handling may also be declared high severity. In addition, the potential for, or already determined, exposure of any confidential data must be reported to the Incident Manager immediately and the incident classified as high severity. Upon notification, the Incident Manager should proceed with required actions according to this documented plan. The Incident Manager should update the executive team throughout the process of managing the incident and proceed with obtaining external support for legal, public relations, reporting requirements, and other required elements for the incident, as deemed appropriate. 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 High severity 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, etc.)
- High risk of the problem spreading throughout the enterprise

Example High Severity Incident Types

- Active compromise of systems containing sensitive company or client data
- A cyber extortion event or any incident involving a ransom demand
- Detected internal or external penetration of systems
- Denial of service activity impacting business operations
- Widespread malware event requiring coordinated enterprise activity to control

Critical Systems and Business Processes

Security incidents involving critical systems or business processes, that if interrupted, would cause significant damage to revenue, costs, and/or business reputation, such as the ones below, require immediate notification of the Incident Manager and a classification of high Severity. Any system or process included in this section should have an alternative means for ensuring business continuity documented as part of this organizations business continuity and recovery plan.
{Note: whether 3rd party provided and supported or self-supported, it does not matter. All systems deemed critical should be identified in this section.}

Examples Include
Point of Sale Systems
Data Systems, in cloud or not, storing sensitive data (PCI, PII, HIPPA, company confidential, etc.)
Any external Website and/or applications
IoT devices maintaining appropriate temperatures on refrigeration units

Ransom Demands and Payment

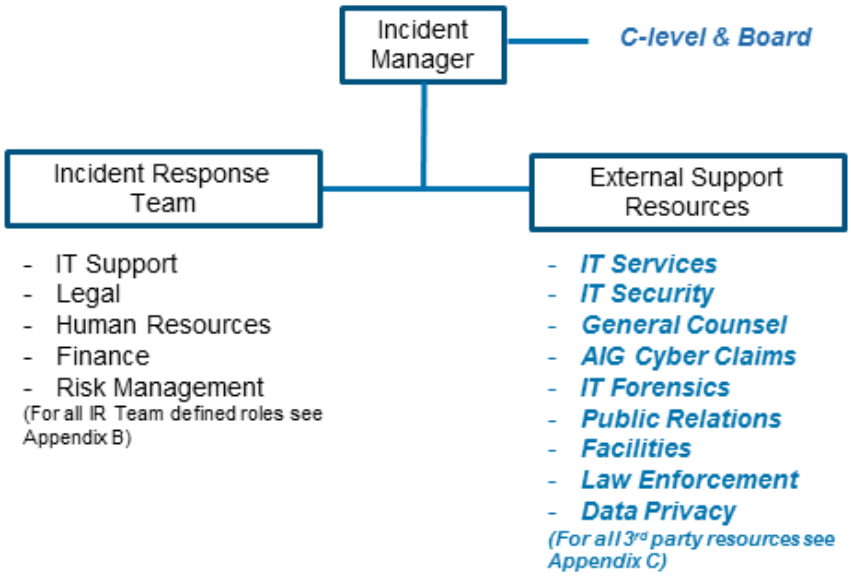
{This section should document corporate policy on paying ransom or not, or the process by which those decisions will be made in the event of an extortion or ransomware event. Resources for obtaining crypto currency, financial loans, or other to obtain necessary funds to make ransom payments, should also 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.}

{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, finance, and identified financial resources, as identified in Appendix C, to secure the necessary funds, bitcoin, etc. and proceed with payment towards business recovery.

Incident Response Team

The Incident Response Team (IR Team), for ***<company name>***, will be led and managed by the Incident Manager. The IR Team is composed of current employees as defined in Appendix B with defined responsibilities in this section of the document. Additional resources, as needed, will be relied upon by external 3rd party organizations as deemed necessary during the incident and listed in Appendix C. The following diagram shows the described IR Team structure.



Incident Response Team

The IR Team includes all roles, internal and external, required to appropriately manage, respond, and recover from a security incident. The IR Team will be activated for all high severity incidents with necessary external support functions required. The IR Team 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 support analysis of affected systems
- Return all systems to secure, operational status in accordance with appropriate procedures (i.e., change control, business continuity/disaster recovery)

{Note: The size of your organization may dictate that some of these roles are done via 3rd party, or that multiple roles may be filled by the same person. For example, the CFO may be your incident manager and also act as risk manager. Or, you may only have external general counsel. Review each role definition carefully, alter titles as necessary, and ensure responsibilities for each role remain, whether as currently constituted or combined. Remove this text.}

Incident Manager

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

- Directing all tasks and assignments to team members
- Coordinate necessary logistics for meetings (i.e., conference room, teleconference bridges, times)

- Coordinating and directing any external support teams
- Ensuring that all appropriate incident specific response procedures are followed
- Ensuring that incidents are fully documented including lessons learned and recommendations for improvement upon closeout of the incident
- Providing appropriate status updates to the C-Level and Board Members
- Designates an alternate Incident Manager to handle incident management responsibilities as appropriate

IT Support

Any employee of <***company name***>, with job responsibilities related to IT support, administration or security may be activated by the incident manager as deemed necessary. Those with IT related job functions that are involved in a security incident:

- Provides guidance and support to the Incident Manager
- Assesses the impact of an incident on IT systems, assets, and data, as appropriate
- Assist with activities involving any IT system in the environment
- Coordinates the acquisition of appropriate system and network logs for 3rd party forensics analysis
- Assists with acquisition of data (i.e., volatile/non-volatile data from servers, etc.) for 3rd party forensics analysis
- Helps to assess the impact/scope of any level of compromised sensitive data
- Works with 3rd party vendors (i.e., "3rd party IT Support or IT security support or IT forensics"), as directed by the Incident manager
- Assist with recovery and/or replacement of systems affected by an incident
- If appropriate, and directed to do so, work internally or through 3rd party support to create a 'greeting message' to notify clients that may call in reporting issues or to post a message on external facing website.

{Note: review this last bullet point carefully and reword as appropriate or remove depending on business requirements for dealing with client support. This may be a function of public relations or other vs. IT, for example. Then remove this highlighted text.}

Legal

Legal acts as an advisor to provide guidance in ensuring any necessary legal requirements concerning the incident are met in accordance with any federal and state legislation, and pursuant to any other applicable regulatory rules and protocols (e.g., PCI). It is the responsibility of legal to advise the incident response team on regulatory requirements and act as liaison to any external general counsel, breach coach, law enforcement, and external entities/regulatory bodies, as deemed appropriate, during an incident. Responsibilities may also involve handling any post incident legal requirements or possible litigation.

Human Resources

The role of human resources is activated by the incident manager during a cyber incident where personnel related issues are involved or incidents involving employee PII data. For example, an incident involving malicious actions of an employee resulting in exposed sensitive data. Any resulting disciplinary actions resulting from a violation of business policy will be handled by the guidance of legal and by human resources. Human resources may also be involved in any internal communications, to employees, concerning a cyber incident.

Finance

The role of Finance is to 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 3rd party accounting contacts for securing loans or crypto currency. See Appendix C for a list of identified financial resources to use. Finance will also provide appropriate insight to financial matters during an incident including tracking of related expenditures, costs, etc.

Risk Management

Risk Management is responsible for cyber insurance coverage and the relationship with AIG cyber claims. The Risk Manager provides the necessary evaluation and determination of insurance claim requirements resulting from certain types of security incidents. If necessary, the Risk Manager will report incidents to AIG for purposes of securing 3rd party resources for assistance with the current incident. The Risk Manager will provide appropriate insight to the Incident Manager for claims information gathering requirements and coverage applicability, throughout the incident management cycle. When required, Risk Management will work with AIG Cyber Claims to secure breach coach, forensics, or other external services needed. See Appendix D for AIG claims notification process and information.

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. This may involve working with Human Resources, executives, legal, marketing, and a 3rd party Public Relations firm, as necessary, to ensure appropriate communications during and after the incident. No external communication will be made without the prior approval of legal and any involved 3rd party general counsel firm. Any calls from external media, or other, are to be referred to legal. Communications templates should be prepared ahead of time and pre-approved by legal and executive leadership, especially for any external communications.

C-Level Executives and Board Members

Any C-level executive will be regularly updated during management of a high severity incident, by the Incident Manager, or may be involved with specific responsibilities as designated by this plan. Some critical decisions may require input before proceeding. For example, whether to pay a ransom demand or attempt to recover key systems through alternative means. If not already involved, C-level executives may be asked to step in and fill responsibilities for a defined role where primary resources are not available, or as needed.

External Support Resources

IT/IT Security Services

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

- Alert to any incidents on the systems managed by them on behalf of ***<company name>***
- Provide tactical support for systems and applications under their purview
- Advises the Incident Manager regarding the potential effects of an incident on those systems
- Collect 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: External Support Resources for a list of third party vendors and contacts for ***<company name>***.

Additional External Incident Staffing Support Resources

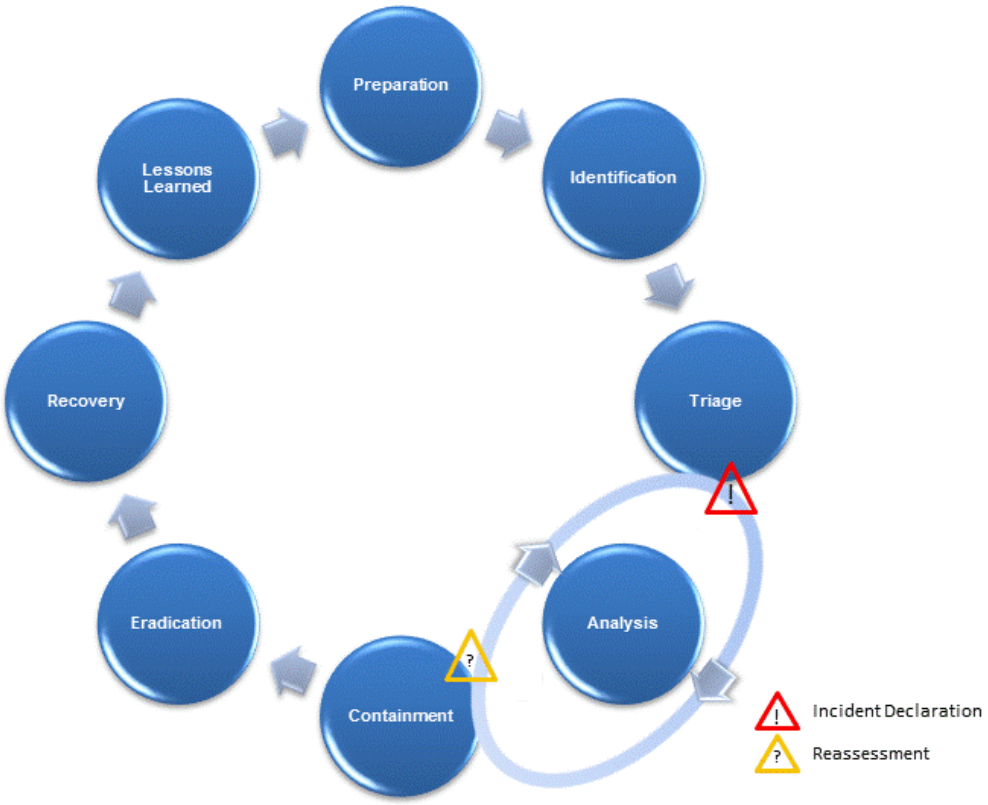
External resources may be required to assist with investigation and management of a high severity cyber incident such as IT Forensics, General Counsel, Forensics Accounting, Public Relations, etc. If no prior relationship exists for these types of services, the Risk Manager may be authorized to work through AIG Cyber Claims to secure appropriate resources. If relationships already exist, via retainer or otherwise, then the Incident Manager may, directly or through the appropriate assigned resource, engage the needed services. Relationships with external firms, already existing, are listed in Appendix C: External Support Resources.

Facilities

The appropriate member of the IR Team manages the relationship with the facilities support or ownership where ***<company name>*****'s,** office reside. Familiarity with the process for providing access to physical facilities for vendors and contractors, if applicable, during incident response engagements, is necessary. In the event an incident involves a potential physical security breach, facilities management should be engaged to assist with security efforts to identify and mitigate the breach and implement any temporary defensive measures.

Incident Response Process Overview

This plan does not provide specific steps for handling different types of security incidents, but instead defines ***<company name>***'s general process for handling all cybersecurity 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

Preparation

The preparation phase defines those actions taken to prepare for cybersecurity incidents, including maintenance of this incident response plan and the establishment of the IR team. Actions taken in this step should be completed and documented prior to a cybersecurity incident. To prepare for a cybersecurity incident ***<company name>*** will:

- Inventory all company assets on the network and develop diagrams showing logical locations and relationships
- Identify critical systems 3rd party managed or self-managed, that store and/or process sensitive data and document them within this plan
- Ensure regular IT system hardening is performed in accordance with documented guidance
- Deploy cybersecurity monitoring services wither self or 3rd party managed systems and document
- Ensure appropriate logging at key locations is active and that the resulting logs are retained according to current retention policies
- Ensure critical data is backed up and that regular restoration testing has occurred
- Document any 3rd party vendor IT and cybersecurity service providers and review existing contract agreements for SLAs pertaining to support during a cybersecurity incident.
- Conduct cybersecurity awareness training of all employees including how to report a cybersecurity incident. Conduct mock incident drills with IR Team members.

Identification

The identification phase begins with the notification of a potential cybersecurity incident. Any received notification of a potential incident is assessed by the appropriate member of the IT team. If it is determined to be low severity, it is handled by the IT team in accordance with standard process and low severity incident recording requirements as defined previously in this document. If the incident is anything but a low severity incident, the Incident Manager is notified immediately and the process moves forward with triage. Possible notifications may include, but are not limited to:

- Communication to the IT team 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

During triage the Incident Manager works with appropriate internal and external IT Support resources to assess the details of the reported incident and to determine the validity and scope. IR Team members are notified and organized by the Incident Manager to collect data and conduct initial analysis of the incident. Actions may include, but are not limited to:

- Initial assessment and classification of the incident
- Determination of the scope and type of compromise
- Collection of volatile and non-volatile data collection

- Assessment of the possibility of sensitive information disclosure
- Official declaration of the incident

The result of the triage phase is a decision regarding ***incident declaration*** and the initiation of the remainder of this plan. Formal declaration by the Incident Manager activates the appropriate oversight for decisions which may lead to significant expenditure of corporate resources and/or finances and other considerations such as legal requirements for notification. Once an incident declaration has taken place, consideration should be given to notifying AIG Cyber Claims, see appendix D, for reporting First Notice of Loss and receiving additional resource assistance as needed.

Analysis

The analysis phase continues actions taken during the triage phase. 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:

- Activation of required external support services such as: Breach Counsel, IT Forensics, etc.
- Additional data collection and forensic imaging as necessary
- Analysis of system and network logs, volatile data, etc. for indicators of compromise
- Basic root cause analysis

Containment

Containment may be accomplished in conjunction with Analysis, depending on the nature of the incident and information determined while conducting analysis. Some containment actions may be required prior to analysis, depending on the nature of the incident. For example, a fast spreading ransomware attack taking down multiple systems. The Incident Manager will identify resources necessary to implement the containment plan and assign tasks to appropriate resources.

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 steps to achieve containment of the incident
- The Incident Manager assigns tasks to appropriate personnel, including any 3rd party support, and tracks completion
- 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 may require approval of other executives before the 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 IR 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 other executives before implementation. Activities performed include:

- The IR Team finalizes plans for eradicating any malware, other foreign software, etc.

- Patching or remediating any source vulnerability allowing continued penetration or spread within the environment
- 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 {*insert required approval source}*
- The Incident Manager assigns tasks to appropriate resources and tracks completion

Recovery

Once it is clear that full eradication has completed, plans are made for restoring normal business operations. The Incident Manager will assign appropriate IT staff or 3rd party support to restore affected systems and services to their original state. Once production activities have been restored, the IR Team 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 further identified weaknesses that contributed to the incident. Actions include:

- Implementing identified steps to restore affected systems
- Resources that do not require configuration changes are returned to pre-incident state
- Resources that require configuration changes to prevent the incident's reoccurrence are updated, tested, and redeployed
- When recovery is complete, the Incident Manager notifies executives, IR Team members, etc.
- Review any remaining tasks required by legal requirements related to the incident, if applicable

Lessons Learned

The Incident Manager is responsible for ensuring that following a severity medium or high incident, 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 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

Incident Documentation Requirements

Documentation is mandatory for each incident and must be accurately reported in the required form. In addition to the standard incident report form, documentation may also include the storing of any incident artifacts such as:

- Any communications and notes
- Any other related notes or materials, as deemed required, by legal and general counsel

IR Team members should be aware of any requirements to retain any artifacts, documentation, etc. as part of standard training prior to an incident. Legal is responsible for communicating any requirements for records retention.

Documentation for Low Severity Incidents

Low severity incidents are handled by trained IT staff as part of day to day operations and within the guidelines of this plan. Although less severe in nature, appropriate details are still recorded, using the designated IT ticketing system, and reported to allow for follow-up review and analysis for trends, potential improvements, and better preventative 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 IT staff member that resolved the issue
- 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

Documentation for High Severity Incidents

Incidents of higher severity require a more formal process and wider participation by members of the IR 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 IR 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 Claims Reporting

While managing the security incident, the Risk Manager has responsibility to report the incident to AIG claims and coordinate with the Incident Manager, on the appropriate amount of documentation and what items should be tracked, during the incident investigation, to appropriately report the full extent of the claim to AIG. For further details refer to Appendix D: AIG Claims Support.

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.
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.
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, 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.

Appendix B: IR Team Contact List

IR Conference Bridges

Bridge Designation	Vendor	Numbers and Codes
IR Team	*{Webex, AT&T, ….}*	*Bridge:* <NUMBER> *Participant Code:* <Code> *Moderator Code:* <Code>

Incident Manager

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>

IR Team Members

The Incident Manager shall assemble the appropriate members of the IR Team as needed to appropriately manage the incident. 3rd party support contacts are contained with Appendix C.

Role	Name	Contact Info	Alternate	Contact Info
IT Support	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Legal	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Human Resources	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Finance	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
Risk Management	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
<Job Role>	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
<Job Role>	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
<Job Role>	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>	<Name and Title>	*Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>

Appendix C: External Support Resources

3rd Party Vendors

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>

External Support

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. Some of these may be on retainer, others may be secured through AIG Cyber Claims support.

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}	General 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	*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}	Facilities Management	*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>

Financial Support

The following table contains a list of contacts for all financial resources that have been identified to assist with loans or securing of crypto currency in the event a decision is made to pay a ransom. Maintenance of this list and relationships is owned by finance.

Vendor Name	Financial Services Provided	Contact Info
{Vendor Name}		*Name:* <*CONTACT NAME*> *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}		*Name:* <*CONTACT NAME*> *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>
{Vendor Name}		*Name:* <*CONTACT NAME*> *Office:* <OFFICE PHONE> *Mobile:* <CELL PHONE> *E-mail:* <email>

Appendix D: 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**

Appendix G: 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)	

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 _____

DETECTION PROCESS (HOW WAS THE INCIDENT DISCOVERED?)

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	

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

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)	

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)

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

_____

Print Name

_____

Position and/or Title

_____

Signature and Date