*Instructions:* This template is not a complete Incident Response Plan (IRP.) It serves as a guide to help you construct your own, tailored to the specific needs and resources of your business.

**What do you need to do?**

Carefully review each section of this template and update it with the appropriate details for your company. Because this Plan also serves as an active communications and contact document, make sure that you keep it up to date as people and 3rd-party providers join and leave the company. Be sure to:

* Include all current contact information (email, phone, other) for the key participants and stakeholders in the company’s Plan.
* Fill in all recommended slots, even if multiple roles are held by the same person.
* Replace, at minimum, all of the placeholders in this document, such as “<COMPANY NAME>”, with real-world values that apply to your company.

*--- Remove text above this line in the company’s final Plan ---*

Introduction

This document sets out the <COMPANY NAME> plan for reporting and resolving cybersecurity incidents. All security incidents must be managed in a time-effective manner to make sure that the impact of an incident is contained, and that the consequences for customers and other stakeholders are limited.

What is a Cybersecurity Incident?

A Cybersecurity Incident means any incident that occurs accidentally or deliberately, that impacts the company’s communications, data storage or information processing systems. An incident may be any event or set of circumstances that threatens the confidentiality, integrity or availability of information, data or services in <COMPANY NAME>.

This includes unauthorized access to, use, disclosure, modification, or destruction of data or services used or provided by <COMPANY NAME>.

How to Recognize a Security Incident

A security incident may not be recognized immediately; however, there may be indicators of a security breach, system compromise, unauthorized activity, or signs of misuse within the company’s IT systems, or that of the company’s 3rd-party service providers.

Everyone within the company must watch for, and be aware of possible indications that a security incident has occurred, or may be in progress, which might include:

* Excessive or unusual log-in attempts and system activity, in particular from any inactive user accounts.
* Excessive or unusual remote-access activity into the company’s IT systems. This could be from the company’s employees or the company’s 3rd-party providers.
* The appearance of any new wireless (Wi-Fi) networks visible or accessible from within the company’s offices or other locations.
* The presence of or unusual activity in relation to unknown software, ransomware, unusual advertising activities, suspicious files, or new/unapproved folders or other visible indications of unexpected activity on the company’s systems. This could be on the company’s networks, servers or PCs, including web-facing and email-related systems.
* Unexpected or unknown hardware or programs found connected to, or installed on, systems
* Suspicious or unusual activity or behaviors on web-facing or email-related systems, such as on the company’s ecommerce website, email hosting provider, or support provider.
* Point-of-Sale (POS) payment devices, payment terminals, chip & PIN/signature devices or dip/swipe card readers showing signs of tampering
* Any card-skimming devices found on company payment devices, or cameras or other data-capture activity found on or near the company’s payment devices.
* Lost, stolen, or misplaced merchant copy receipts or any other records that display the full payment card number or card security code (the 3- or 4-digit number printed on the card)
* Lost, stolen, or misplaced computers, laptops, hard drives, or other media devices that contain payment card data or other sensitive data

Roles and Responsibilities

This Incident Response Plan must be understood and followed by all personnel in the company, and must also be provided to, and acknowledged by, any involved 3rd-parties. This includes all employees, temporary staff, consultants, contractors, suppliers, and third parties operating on behalf of <COMPANY NAME>, or working with <COMPANY NAME>’s customers’ data, whether on-site or remotely. For simplicity, all of these personnel are referred to as ‘staff’ within this Plan.

Key Roles

The <COMPANY NAME> Cybersecurity Incident Response Team (CSIRT) is comprised of:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Role | Responsibilities | Name | Email | Phone | Notes |
| **Information Security Officer** | Primary lead for responding to an incident and ensuring that this IRP is followed. | <INSERT NAME> |  |  |  |
| **IT Manager or Primary IT Support Contact** | Technical response lead | <INSERT NAME> |  |  |  |
| **Senior Management Primary Contact** | Executive Officer / Business Risk Owner | <INSERT NAME> |  |  |  |
| **Person Responsible for each Key Business Operation** | <INSERT SPECIFIC ROLES> | <INSERT NAME> |  |  |  |
| **<NEXT KEY BUSINESS ROLE…>** |  |  |  |  |  |
| **Primary HR Contact** | Responsible for any personnel issues, disciplinary issues, or management of employee-data loss/compromise during an incident | <INSERT NAME> |  |  |  |
| **Primary Legal Contact** | Handling of any legal questions or issues that may arise as a result of an incident | <INSERT NAME> |  |  |  |
| **Primary Communications Contact** | Responsible for handling external communications to customers, vendors and other stakeholders during/after an incident | <INSERT NAME> |  |  |  |
| **[If Applicable]****External IT Support / On-call Response Specialist** | Responsible for providing on-demand IT support<INSERT ROLE> | <INSERT NAME> |  |  |  |
| **[If Applicable]****External Hosting Provider** | Responsible for managing the physical or logical infrastructure at an outsourced hosting facility | <INSERT NAME> |  |  |  |
| **[If Applicable]****E-Commerce Hosting Provider** | Responsible for managing the systems and/or software that oversee the customer experience and selling process for online/E-Commerce sales | <INSERT NAME> |  |  |  |
| **[If Applicable]****Application Developer** | Responsible for researching and resolving incidents associated with proprietary or in-house applications, not otherwise supported by a commercial application provider | <INSERT NAME> |  |  |  |

Responsibilities

The Information Security Officer is responsible for:

* Making sure that the company’s Cybersecurity Incident Response Plan and associated policies, responses and escalation procedures are defined and documented. This is to make sure that the handling of security incidents is timely and effective.
* Making sure that the Security Incident Response Plan is up-to-date, reviewed and tested, at least once each year.
* Making sure that staff with Cybersecurity Incident Response Plan responsibilities are properly trained, at least once each year.
* Leading the investigation of a suspected breach or reported security incident and initiating the Cybersecurity Incident Response Plan, as and when needed.
* Reporting to and liaising with external parties, including 3rd-party vendors or providers, legal representation, law enforcement, and others as required.
* Authorizing on-site investigations by appropriate law enforcement or cybersecurity/forensic personnel, as required during any incident investigation.
This includes authorizing access to/removal of evidence from site.

IT Managers and IT Team members (internal or external) are responsible for:

* Making sure that all staff understand how to identify and report a suspected or actual security incident.
* Advising the Information Security Officer of an incident when they receive a security incident report from staff.
* Investigating each reported incident.
* Taking action to limit the exposure of sensitive data, prevent further disclosure of information, and to reduce the risks that may be associated with any incident.
* Gathering, reviewing and analyzing logs and related information from various central and local safeguards, security measures and controls.
* Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
* Reporting each security incident and findings to the appropriate parties. This may include the customer, 3rd-party service providers, business partners, financial institutions or intermediaries, etc., as required.
* Assisting law enforcement and authorized security personnel during the investigation processes. This includes any forensic investigations and prosecutions.
* Resolving each incident to the satisfaction of all parties involved, including external parties and stakeholders.
* Initiating follow-up actions to reduce the likelihood of recurrence, as appropriate.
* Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

All staff members are responsible for:

* Making sure they understand how to identify and report a suspected or actual security incident.
* Reporting a suspected or actual security incident to the Information Security Officer (preferable) or to another named person on this Cybersecurity Incident Response Plan.
* Reporting any security related issues or concerns to line management, or to a named person on this Cybersecurity Incident Response Plan.
* Complying with the security policies and procedures of <COMPANY NAME>. This includes any updated or temporary measures introduced in response to a security incident, or for business continuity, incident recovery or to prevent recurrence of an incident.

Incident Response Plan Steps

There are a number of steps and stages that you must be taken to make sure that you protect the Company’s business by reacting to a security incident appropriately:

Report

Information security incidents must be reported, without delay, to the Information Security Officer (preferable) or to another named person on this Cybersecurity Incident Response Plan. The person receiving the report will advise the Information Security Officer of the incident.

In the event that a security incident or data breach is suspected to have occurred, we recommend the staff member discuss their concerns with their direct manager, who in turn may raise the issue with the Information Security Officer.

Investigate

After being notified of a security incident, the Information Security Officer will perform an initial investigation and determine the appropriate response, which may be to initiate the Cybersecurity Incident Response Plan.

If the Cybersecurity Incident Response Plan is initiated, the Information Security Officer will investigate the incident and initiate actions to limit the exposure of company data and in mitigating the risks associated with the incident.

Ensure that no one can access or alter compromised systems.

* Isolate compromised systems from the Company’s network and unplug any network cables – without turning the systems off.
* If using a wireless network, issue a new SSID (Service Set Identifier) on the wireless access point and transition un-affected systems that may be using this wireless network (but not any of the systems believed to be compromised).
* Preserve all logs and similar electronic evidence, e.g. logs from the Company’s firewall, anti-virus tools, access control systems, web servers, email servers, application server, database, etc.
* Perform a back-up of the Company’s systems to preserve their current state – this will also facilitate any subsequent investigations.
* Keep a record of all actions you and all involved parties take.
* Stay alert for further indications of compromise or suspicious activity in the Company’s environment, or that of the Company’s 3rd- parties.
* If the incident involved credit cards, other electronic payments, or integration with a financial institution, seek advice before you process any further payment or financial transactions.
* If possible, gather details of all compromised or potentially compromised payment customer accounts, credit cards, bank accounts, or other identifiable entities that may be impacted by the incident (the ‘accounts at risk’).

Inform

Once the Information Security Officer has carried out their initial investigation of the security incident:

* The Information Security Officer will alert the senior management primary contact.
* The Information Security Officer and / or the designated personnel responsible for communications / PR will inform all relevant parties. This includes the Company’s key stakeholders and (if related to financial or Personal Identifying Information protected by law or regulation) local law enforcement, and other parties that may be affected by the compromise such as the Company’s customers, business partners or suppliers. This also includes the personal data breach notification contacts, as applicable to the incident under investigation.

Maintain Business Continuity

The Information Security Officer will engage with operational teams in company to make sure that the company’s business can continue to operate while the security incident is being investigated.

Incident Response Plan Preparation

Plan Ahead

Be prepared – in advance of any security incident that may impact the company’s business, all participants in the Cybersecurity Incident Response Plan should make sure they have a written plan for how their areas of influence would operate if the Company’s systems and processes were unable to operate as normal.

For example:

* Does the company have a plan to activate backup systems, and are data backups available in the event of loss of data, system corruption/virus infection or hardware failure?
* With regard to financial transactions, consider what offline or alternative payment acceptance methods the company could use if it were unable to take card payments via an ecommerce website, in-store or over the telephone using the company’s usual methods.
* Determine risk mitigation and recovery services, such as Credit Monitoring or Identity Theft Protection that may be necessary to protect or indemnify employees, customers or other stakeholders from losses as a result of an incident. Ensure that current quotes and activation plans are in place, and up-to-date, with a chosen provider, vendor or other service, should they become necessary.

Resolve

The Information Security Officer will liaise with external parties, including the Company’s vendors, 3rd-party providers, financial/banking entities, law enforcement, etc., to ensure appropriate incident investigation (which may include on-site forensic investigation) and gathering of evidence, can be performed as rapidly as possible. This Cybersecurity Incident Response Plan will be kept up-to-date with regard to procedures those parties lay out to the Company, with regard to their own requirements for initiating or carrying out an investigation or mitigation activity on the Company’s behalf, should an incident occur.

The designated Role holders in this Plan will take action to investigate and resolve the problem to the satisfaction of all parties and stakeholders involved. This will include confirmation that the required controls and security measures are operational.

Recover

The Information Security Officer will authorize a return to normal operations once satisfactory resolution is confirmed.

The Communications Contact will notify the rest of the business that normal business operations can resume. Normal operations must adopt any updated processes, technologies or security measures identified and implemented during incident resolution.

Review

The engaged Role holders in this Plan will complete a post-incident review after every security incident. The review will consider how the incident occurred, what the root causes were and how well the incident was handled. This will help to identify recommendations for better future responses and to avoid a similar incident in the future.

Changes and updates that may be required include:

* Updates to the Cybersecurity Incident Response Plan and associated procedures.
* Updates to the Company’s business’ security or operational policies and procedures.
* Update or new implementation of appropriate Policies and Procedures for acceptable use and management of the company’s IT systems, and ensure that employees are trained and accountable for such.
* Updates to technologies, security measures or controls on networks, systems, or related devices (such as payment terminals, or POS systems).
* Introduction of additional safeguards in the environment where the incident occurred (for example, improved malware detection or restricted access based on revised Roles and policies).

The Senior management primary contact will ensure that the required updates and changes are adopted or implemented as necessary.

Specific Incident Response Types

<This Cybersecurity Incident Response Plan provides the generic steps that must be followed when dealing with a security incident. You must update the plan to include security incident types and responses that are specific to your business environment and operational activities.>

Malware (or Malicious Code)

1. Disconnect devices identified with malware from the network immediately.
2. Examine the malware to identify the type (e.g. rootkit, ransomware, etc.) and establish how it infected the device. This will help the company understand how to remove it from the device(s).
3. Once the malware has been removed a full system scan must be performed using the most up-to-date signatures available, to verify it has been removed from the device.
4. If the malware cannot be removed from the device (as is often the case with rootkit-type infections) it should be rebuilt using original installation media or images. Prior to restoration from back-up media/images the company must verify that the back-up media/images are not infected by the malware.
5. Protect the system(s) to prevent further infection by implementing fixes and/or patches to prevent further attack.
6. <ADDITIONAL STEPS AS APPROPRIATE TO YOUR COMPANY>

Tampering of POS systems, payment terminals, chip & PIN/signature devices or card readers detected, card-skimming devices found, or devices substituted:

1. Stop using the substituted/tampered devices
2. Report the substitution/tampering to the device provider and the company’s downstream financial services providers (Merchant account, bank, etc.)
3. Follow the device provider or merchant provider’s advice to ensure the security of all future card payments, inspect and confirm the integrity of the company’s remaining devices, deploy replacement devices, etc.
4. Follow the company’s device provider or merchant provider’s guidance to investigate the incident, possibly including sending the substitute/tampered devices to them, allowing on-site investigations, etc.
5. <ADDITIONAL STEPS AS APPROPRIATE TO YOUR COMPANY>

Unauthorized Wireless Access Points or other Network-Access Devices:

If unauthorized wireless or wired network access points are detected, or reported by staff, these must be recorded as a security incident.

1. Information Security Officer will investigate to identify the location of the unauthorized wireless access point/device.
2. The Information Security Officer will investigate as to whether or not the unauthorized wireless access point/device is being used for a legitimate business purpose/need. If a legitimate business reason is identified, then this wireless access point or device must be reviewed and go through the correct management approval process. This is to make sure that the business justification is documented and the wireless access point/device is securely configured (e.g. change default passwords and settings, enable strong authentication and encryption, etc.).
3. All other unauthorized wireless access points/devices must be located, shutdown and removed.
4. <ADDITIONAL STEPS AS APPROPRIATE TO YOUR COMPANY>

Loss of Equipment

1. The theft or loss of an asset, such as a PC, laptop or mobile device, must be reported immediately to a named member of this Cybersecurity Incident Response Plan, and if applicable, local law enforcement. This includes losses/thefts outside of business hours on weekends, and while traveling.
2. If the device that is lost or stolen contained sensitive customer, employee personal or financial data, and the device is not encrypted, the Information Security Officer will complete an analysis of the sensitivity, type and volume of data stolen, including any potentially exposed financial information, or personally-identifying information.
3. Where possible, the Information Security Officer will use available technology/software to lock down/disable lost or stolen mobile devices (e.g. smart phones, tablets, laptops, etc.) and initiate a remote wipe. Evidence should be captured to confirm this was successfully completed.
4. <ADDITIONAL STEPS AS APPROPRIATE TO YOUR COMPANY>

Non-Compliance with the Company’s Security Policies

This covers incidents resulting from deliberate or accidental actions that are in breach of the company’s security policy and which put sensitive data at risk. This includes any systems or data mis-use, unauthorized exposure of data to external parties, unauthorized changes to systems or data, or tactics used to gain access to information that the user is not properly authorized for.

1. The Information Security Officer will engage with the relevant business area to establish an audit trail of events and actions. They will determine who is involved in the policy violation and the extent of the violation.
2. The Information Security Officer and/or line managers will notify the Human Resources contact of the incident.
3. The Information Security Officer will liaise with Human Resources and managers to determine whether disciplinary action is needed.
4. The Information Security Officer will undertake an assessment of the impact and provide advice and guidance to the business area to prevent reoccurrence, for example re-training of staff.
5. <ADDITIONAL STEPS AS APPROPRIATE TO YOUR COMPANY>

Testing and Updates

Annual testing of the Cybersecurity Incident Response Plan using walkthroughs and practical simulations of potential incident scenarios is necessary to ensure named Roles in this Plan are aware of their obligations, unless real incidents occur which test the full functionality of the process.

1. The Incident Response Plan will be tested at least once annually.
2. The Incident Response Plan Testing will test the company’s business response to potential incident scenarios to identify process gaps and improvement areas.
3. The Information Security Officer will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.
4. The Incident Response Lead will ensure the Security Incident Response Plan is updated and distributed to SIRT members.
5. <ADDITIONAL STEPS AS APPROPRIATE TO YOUR COMPANY>

Cybersecurity Incident Response Plan – Version and notes

|  |  |  |  |
| --- | --- | --- | --- |
|  | Key Data | Last Changed On | Last Changed By |
| **Current Version** | 0.1-Draft |  |  |
| **Plan Owner:** | <Named Owner> |  |  |
| **Plan Approver:** | <Named Approver> |  |  |
| **Date of Last Review** |  | <Review Date> |  |
| **Notes** |  |  |  |