%company name% – Cybersecurity Incident Response Plan

Revision 1.0

Date: January 1, 2021

Revision History

Version	Date:	Author:	Comments:
1.0	January 1, 2021	Tony Asher	Plan creation
1.2			Added GDPR breach requirements
1.3			Added Resource section
1.4			Added Communication escalation matrix
1.5			Added Clinical breach information & escalation requirements

Index:

Summary:

This incident response plan was written and developed specifically for _____ for the purpose of classifying, declaring, escalating, responding, and containing a cybersecurity events that could be considered harmful or impactful to the company, partners, vendors, patients, and employees.

Goal:

Proper response to cybersecurity events that are escalated beyond alert thresholds, so that we can reduce the impact of these events to the business.

Overview and Objectives:

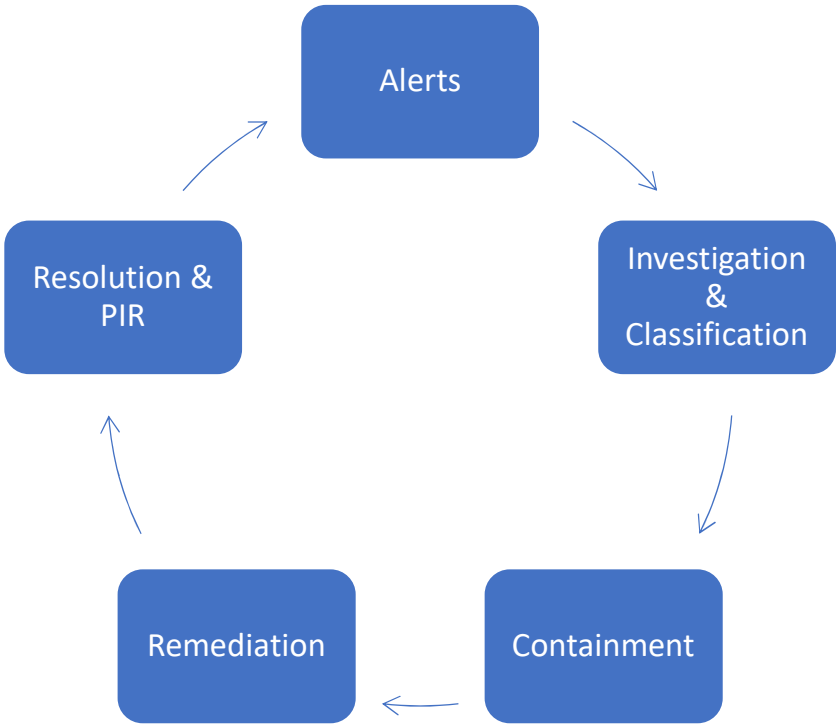
This incident response plan establishes the recommended organization, actions, and procedures needed to:

- Recognize and respond to an incident;

- Assess the situation quickly and effectively
- Notify the appropriate individuals and organizations about the incident
- Organize the company's response activities
- Escalate the company's response efforts based on the severity of the incident
- Support the business recovery efforts being made in the aftermath of the incident

This plan is designed to minimize operational and financial impacts of such an incident, and will be activated when a technology manager (or, in his/her absence, one of his/her alternates) determines that an incident has occurred.

Cybersecurity Incident Process Overview



Event Classification:

The incident process begins by receiving alerts and triaging them until closure or until review provides justification for the event classification to be upgraded. The event classifications are listed and defined below.

Level 1: Alert

Initial security notification is an *'Alert'.* It is a documented event that needs to be reviewed.

Cybersecurity events that could be harmful, violate security policies, justifies escalation based on security awareness and training material, or stands out from the unusual, is initially documented in the form of an 'Alert'.

Sources of Alerts:

1. End Users: Directly from employees, and users of systems. This can be brought to the attention of technology support and security in the form of an email, phone call, or direct walk up.
2. Security Management Consoles (such as endpoint protection or firewalls).
3. Managed Security Partners
4. Government & Law Enforcement

Level 2: Investigation

Reviewed alert that justifies further review before it can be confidently closed out as resolved.

An investigation is an effort to learn further information about alerts so that it can be determined if an incident has occurred or if there is no concern. This set of actions, and sources of additional information, will be determined by the security resource working the primary investigation.

During an investigation no formal communication escalation needs to take place.

A successful investigation will result in a closed alert, or escalation to an 'incident'.

Level 3: Incident

An investigation that cannot be closed out, or shows evidence of malicious activity, data loss, resource loss, or productivity outage.

The classification of an incident justifies reason for believing a violation of policy, or malicious activity has occurred.

The primary resource performing the incident handling should communicate an incident to the director of IT, and the lead cybersecurity resource.

Documentation should begin as part of the incident handling. Documentation should include;

- Source of alerts causing investigation
- Time and date of incident
- Resources supporting incident
- Time to detect: To the best of the ability at such time, the time and date that the origin of the incident began to the time the someone starting investigating the alerts (not the alert origination).
- Time to respond: Measurement of time between the incident actually began and the time of the formal incident declaration.
- Time to contain: Measurement of time between incident actually began and the time containment of incident was successful.
- Time to remediate: Measurement of time between incident actually began and the time to bring impacted assets back to operational status.
- All appliable evidence collected so that there is future ability to support a prosecution.
- Documented chain of custody of an evidence.

Level 4: Breach

An incident reveals evidence, or reason to believe, of data loss from _____.

A breach can be declared by the incident handling resource in coordination along with one other primary management resource.

The handling of a cybersecurity breach will be handlined according to the same guidelines as the incident.

The primary actions of a breach are focused on the escalation and communication of the cybersecurity event. The escalation and communication process should follow the 'Event Escalation' section below.

Event Declaration:

The level of the cybersecurity event should be declared by the designated cybersecurity resource. This can either be security staff, technology staff designated with security responsibilities by management, technology directory, or the managed security service partner.

Resources:

Upon the declaration of an incident, the security resource will communicate to Director of Technology the need for any staff resources. These human resources needed to contain, remediate, and recover from an incident or a breach are referred to as the 'Tiger Team'.

Tiger Team is a dynamically formed, specialized, cross-functional team brough together for incident resolution.

If you are asked to participate in the Tiger Team please communicate your work priorities to your leadership and get approval to shift your focus on the incident resolution.

Incident Documentation:

It is very important to document all the information relevant to cybersecurity incidents. As such, one an event is classified as a 'incident' it should be recorded and all evidence relevant to the event should be saved and archived to the best of the ability of the staff and support involved.

It is important that evidence of cyber attacks is documented and retained because in the event _____ decides to pursue legal action, evidence will be required as part of the case. Evidence collection should follow security best practice and have chain of custody log kept if and when evidence is moved, changes ownership, stored on external media, or transfer to other organizations.

Event Escalation:

The following escalation guidelines provide direction on when staff, partners, legal teams, and regulatory bodies should be notified as a part of _____ incident response plan.

> **Alerts & Investigations:** These events will be recorded within security consoles, and maybe documented separately for investigations justifying further documentation and tracking.

Incidents: The following groups should be notified that a cybersecurity incident has been opened and is being worked:

- IT Director

Breach: Immediate escalation should be communicated to:

- Executive leadership determined by IT Director
- Head of Compliance
- Head of Legal
- Head of Privacy

Please refer to the Roles and Responsibilities section below for contact information.

Specific Breach Protocols:

This section outlines specific requirements, other protocols and procedures that need to be followed when certain types of data are included in incidents or breaches.

GDPR Breach Notification Requirements:

_____ collects a limited amount of data considered in scope as part of GDPR. This regulation clearly states that in the event of a data breach containing GDPR data we must perform actions in compliance to these regulatory requirements. The requirement has been provided below, but can also be found in the most recent "General Data Protection Policy _____".

Requirement to Notify

(a) The GDPR imposes strict requirements to notify the Supervisory Authority in the event of a security breach of Personal Data (a **data breach**).

(b) A data breach occurs when there is an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. Under GDPR if a data breach occurs, controller must notify:

(i) the Supervisory Authority **without delay** and not later than within **72 hours of becoming aware** of the data breach, unless it is unlikely that the data breach will pose a risk to the rights and freedoms of individuals; and

(ii) affected individuals, unless any of the following applies:

(A) _____ has implemented security measures to ensure the Personal Data is unintelligible to anyone not authorized to access it (e.g. the Personal Data is encrypted);

(B) _____ has taken measures to ensure the high risk to individuals is no longer likely to materialize; or

(C) Notifying the individuals concerned would involve disproportionate effort. In this instance a public communication or similar would suffice, provided the individuals concerned are informed in an equally effective manner.

A failure to comply with the GDPR requirements concerning breach notification exposes _____ to significant fines.

(c) Data breaches will be managed in line with the **Security Incident Policy.**

Please refer to the General Data Protection Policy or Data Privacy Officer for specific steps that are required.

Clinical Data Breach Notification Requirements:

If the security breach involves, or might involve, clinical data it is required that we perform the following actions in parallel with the continued cybersecurity efforts:

1. Escalate notification to Clinical Quality Assurance
2. Follow the '***Suspected Serious Breach of GCP, Fraud or Misconduct'*** documentation located in _____.

Executive Breach Notification Requirements:

A cybersecurity breach requires escalation and communication to an executive leader resource. At such point the executive resource is made aware of the situation they will make the decision if further escalation and commination needs to take place.

This may include HR, Legal, Privacy, Compliance, Public Relations.

This effort should take place quickly enough so that proper escalation to law enforcement and regulatory agencies can take place within the required guidelines.

Post Incident Review (PIR):

A review of the cybersecurity incident should be performed within seven days of the incident. All team members involve din the triage, classification, investigation, containment, and resolution of the event should be involved.

The purpose of this review is to clarify lessons learned to:

- Prevent the same incident form happening again.
- Speed up the containment of the incident
- Improve escalation and team response and handling
- Decrease the time of resolution and recovery

Incident Response Playbooks:

As a result of ongoing security risks assessments, threat intelligence monitoring, and vulnerability assessments, the IT and cybersecurity teams have prepared incident response playbooks to supplement the cybersecurity incident handling and response procedures.

The purpose of these playbooks is to assist and speed up cybersecurity incident response so that the impact of the event is minimized.

Incident playbooks can be used as a valuable resource in the event of a cybersecurity incident, but do not have to be. They are information assets that have been premeditatedly planned to help and are optional to for teams to leverage.

Incident Response Playbooks can be found at: //

Roles and Responsibilities:

The Incident Response Lead is responsible for:

- Making sure that your Incident Response Plan and associated response 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 Incident Response Plan is up-to-date, reviewed and tested, at least once each year.
- Making sure that staff with Incident Response Plan responsibilities are properly trained.
- Leading the investigation of a suspected breach or reported security incident and initiating the Incident Response Plan, as and when needed.
- Reporting to and liaising with external parties.
- Authorizing on-site investigations by appropriate law enforcement or security/forensic personnel, as required during any security incident investigation. This includes authorizing access to/removal of evidence from site.

Security Incident Response Team (SIRT) members are responsible for:

- Making sure that all staff understand how to identify and report a suspected or actual security incident.
- Advising the Incident Response Lead 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 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 acquirer, third party service providers, business partners, customers, etc., as required.
- Assisting law enforcement and 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.
- Initiating follow-up actions to reduce 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 Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT).
- Complying with the security policies and procedures of _____.

Role*	Responsibility	Name	Email	Telephone
Information Security Officer	Incident Response Lead	[Insert Details]	[Insert Details]	[Insert Details]
Technology Directory	Incident Response Technical Lead	[Insert Details]	[Insert Details]	[Insert Details]
Senior Management	Executive Officer/Risk Owner	[Insert Details]	[Insert Details]	[Insert Details]
Communications / Public Relations	Handling of any external communications in relation to an incident	[Insert Details]	[Insert Details]	[Insert Details]
Compliance Contact	Handling of compliance and regulatory issues	[Insert Details]	[Insert Details]	[Insert Details]
Privacy Contact	Handing of Privacy issues and regulatory issues	[Insert Details]	[Insert Details]	[Insert Details]
HR Contact	Handling of any personnel and disciplinary issues relating to security incidents	[Insert Details]	[Insert Details]	[Insert Details]

Legal Issues	Handling of any legal questions/issues relating to security incidents	[Insert Details]	[Insert Details]	[Insert Details]
Managed Security Service	Incident Management Service	[Insert Details]		[Insert Details]