Cyber & Data Security Incident Response Plan (CSIRP) for

[Organization Name]

Designed according to the NIST SP 800-61 guidelines, this document aims to minimize service disruptions and ensure the continuity of legal and operational activities during security breaches. The plan also emphasizes best practices for rapid containment, eradication, and recovery from incidents, providing clear procedures and roles for the Incident Response Team (IRT) to follow.

Goals for Cyber Incident Response

When a cyber security incident occurs, timely and thorough action to manage the impact of the incident is a critical to an effective response process. The response should limit the potential for damage by ensuring that actions are well known and coordinated. Specifically, the response goals are:

Purpose & Scope

Purpose

This document provides a framework for detecting, responding to, and mitigating security incidents that may compromise the integrity, confidentiality, and availability of [Organization Name]'s systems and data. Given that our workforce operates remotely, with no physical office locations, and all data resides in [Vendor] Office 365 and Azure, this plan heavily relies on cloud-based tools, especially [Vendor] Defender for Endpoint (MDE) P2, for incident detection and response.

Scope

This IRP applies to all employees, contractors, and third-party vendors who access our cloud-based systems and services. It specifically covers incidents involving:

[Vendor] Office 365 (O365)

Azure services

Remote endpoints protected by [Vendor] Defender for Endpoint (MDE) P2

Incident Response Team (IRT)

Roles & Responsibilities:

Incident Response Coordinator: Oversees the incident management process and ensures timely communication.

Security Analyst: Investigates and analyzes security alerts from MDE and determines the incident's scope.

System Administrator: Responsible for technical containment, eradication, and recovery tasks in Azure and O365.

Legal/Compliance Officer: Ensures compliance with regulatory frameworks, including breach notification.

Public Relations: Handles external communications with clients, partners, and the media (if necessary).

The IRT Contact Information for key team members can be found in Appendix A, which provides detailed contact information to ensure quick communication and coordination during a security incident.

For any escalation or direct communication needs, please refer to Appendix A for the contact details of:

[CISO]

[Engineering Lead], Engineering Lead

[Security Operations Lead], Information Security Operations Lead

[Security Operations Analyst], Information Security Operations Analyst

Incident Response Life Cycle Process

For a structured response designed to mitigate security threats IRM works on-going with a cyclical pattern, IR Life Cycle Response:

Incident Detection

The detection methods implemented are designed to ensure minimal impact on business operations. By utilizing advanced tools such as [Vendor] Defender for Endpoint (MDE) P2, Office 365 Security & Compliance Center, and Azure Security Center, real-time monitoring and automated responses are performed without interrupting regular services.

Detection Methods:

How Proposed Methods Support Minimal Disruption?

Non-Intrusive Detection: These tools operate in the background, continuously scanning for threats like malware or unauthorized access without impacting system performance. This ensures that business activities proceed without interruptions, even during active threat detection.

Real-Time Alerts: Automated alerts from MDE P2 trigger responses instantly, allowing the Incident Response Team to address potential security risks before they escalate. These alerts are processed without causing downtime or affecting user accessibility, ensuring ongoing system availability.

Cloud-Based Logging and Monitoring: By centralizing all logs and real-time alerts in [Vendor] Sentinel and other cloud-based monitoring solutions, incident data is managed remotely. This approach allows investigations and mitigations to be performed without disrupting local system operations or user workflows.

User-Reported Incidents: When employees report suspicious activities, the system isolates and addresses potential threats in a way that does not affect the broader network or business functions. The response is contained, targeted, and minimally invasive to ensure continuous service delivery.

Logging and Monitoring:

All incidents are logged and monitored using [Vendor] 365 Defender and Azure Security Center.

Real-time alerts and incident data are stored centrally in [Vendor] Sentinel (if available).

Toolkit

Identification & Classification

Initial Incident Assessment:

Upon receiving an alert from MDE or other monitoring tools, the following steps are taken to assess and classify the incident:

Review the Nature of the Alert: Determine what type of incident is being reported, such as malware detection, suspicious login attempts, or unusual network activity.

Confirm the Scope: Identify how many endpoints, cloud services, or user accounts have been affected by the incident. Assess whether the threat is localized or widespread across the network.

Classify the Incident: Based on the initial findings, the incident is classified as low, medium, or high impact, which dictates the urgency and level of response required.

Incident Categories:

COMMON CATEGORIES OF CYBER INCIDENTS

Containment

The Containment phase focuses on preventing the spread of the security incident while ensuring that critical systems remain operational. The goal is to isolate and mitigate the threat without causing unnecessary disruptions to business continuity.

Short-Term Containment:

Isolate Devices: Using MDE, compromised devices are immediately isolated from the network. This prevents the threat from spreading to other systems while allowing remote access for continued investigation and remediation. By isolating rather than shutting down, the disruption is limited to affected devices, keeping the broader system operational.

Revoke Access: Disable user accounts that have been compromised in Azure Active Directory or O365. This ensures that no unauthorized actions can be taken from compromised credentials, protecting the integrity of the system without disrupting other users. The action targets specific accounts, ensuring the rest of the system remains functional.

Block Malicious IPs: Blocking known malicious IP addresses using MDE prevents further unauthorized access attempts from external sources. This approach isolates the threat externally, minimizing any further breach attempts without interrupting legitimate network traffic.

Long-Term Containment:

Patch Vulnerabilities: Apply necessary patches or updates to both endpoints and cloud environments. By addressing known vulnerabilities, this step prevents the same threat from reoccurring, while ensuring minimal downtime as systems remain operational during non-intrusive patching processes.

Harden Configurations: Strengthen security settings across Azure, O365, and endpoints based on recommendations from MDE. This step reduces the attack surface, preventing future incidents while keeping core systems active during configuration adjustments.

Eradication

The Eradication step, aligned with the NIST SP 800-61 framework, is critical for removing the threat entirely and ensuring no further disruptions occur. This phase focuses on eliminating the root cause of the incident while safeguarding against future breaches, all while minimizing the impact on ongoing business operations.

Removing Threats:

Automated Response: Use MDE's Automated Investigation and Response (AIR) to automatically remediate threats across compromised endpoints. This automated approach, following the NIST SP 800-61 recommendation for prompt response actions, ensures that threats such as malware are swiftly neutralized by deleting malicious files, cleaning registry entries, and restoring compromised system configurations. By automating the response, system recovery time is shortened, ensuring minimal disruption.

Manual Cleanup: In cases where automated tools cannot fully remediate the threat, perform manual checks to thoroughly remove all traces of the incident. According to NIST SP 800-61, a thorough manual review is essential when dealing with more complex incidents, ensuring that no residual threats remain on critical endpoints or systems. This step helps avoid the risk of unnoticed elements of the breach leading to further compromise.

Scan and Investigate: Conduct advanced threat hunting using [Vendor] 365 Defender and Azure tools to ensure no hidden or dormant threats remain in the system. Following NIST SP 800-61's best practice of continuous monitoring, this additional layer of investigation confirms that the system is entirely secure before declaring the eradication phase complete.

Root Cause Analysis:

In line with NIST SP 800-61's emphasis on post-incident analysis, perform a root cause analysis to identify how the incident occurred, whether due to unpatched vulnerabilities, configuration errors, or social engineering. By understanding the root cause, you can take proactive measures, such as patching software or enhancing user training, to avoid future security breaches. Root cause analysis also informs improvements to the overall incident response process, reinforcing the security framework to prevent similar incidents.

Recovery

Following the Containment, Eradication, Recovery clause of the NIST SP 800-61 framework, focuses on restoring affected systems to their operational state after a security incident while ensuring no residual threats remain. This phase is critical to minimize business disruptions and restore normal services securely.

Restoration of Systems:

Endpoint Recovery: In cases where endpoints were compromised, use tools such as [Vendor] Intune or a cloud backup solution to wipe and restore them. This aligns with the NIST SP 800-61 guidance for recovering systems in a secure and structured manner, ensuring that the endpoints are restored to a clean state without residual vulnerabilities. By utilizing cloud backups, recovery is faster and ensures minimal downtime.

Cloud Services Recovery: If the incident impacted services like Azure or O365, restore these systems from backups stored in Azure Backup or OneDrive/SharePoint. The NIST SP 800-61 framework emphasizes restoring services from secure, verified backups to ensure that no compromised data or configurations persist, allowing systems to resume operations with confidence.

Verification

As per NIST SP 800-61, it's essential to verify that the incident is fully resolved before declaring the recovery complete. This involves:

Running additional scans using MDE to ensure all threats have been eradicated from the system.

Checking the logs in Azure Security Center and O365 Security & Compliance for any lingering suspicious activity, ensuring that no further compromise is present. This step aligns with the framework’s focus on thorough validation after recovery.

Monitoring:

Following recovery, continue enhanced monitoring on affected accounts and endpoints for at least 30 days. For Hight Incident Categories monitoring post-recovery shall be extended to detect any residual or secondary threats, ensuring the system remains secure and that recovery actions have been fully effective.

Communication & Compliance

Internal Communication:

Incident Response Coordinator: The Incident Response Coordinator is responsible for notifying the IRT and other relevant stakeholders, including the executive team and IT teams, regarding the incident’s progress. This ensures timely coordination and decision-making at all levels.

Regular Updates: During medium and high-severity incidents, the management team will receive regular updates to stay informed about the status and actions being taken. The primary methods of communication will include email and secure communication platforms such as [Vendor] Teams or other approved collaboration software, ensuring that updates are shared efficiently and securely across all stakeholders.

External Communication:

Client Notification: In the event that sensitive client data is compromised, the organization will notify affected parties in compliance with GDPR, HIPAA, or other applicable legal frameworks. This ensures that external obligations are met in a timely and transparent manner, while protecting the organization’s legal standing.

Public Relations: For significant breaches, the PR/Communications team will manage all external media inquiries. This approach ensures consistent, clear messaging to the public and helps protect the organization’s reputation during and after the incident.

Incident Report:

A formal incident report will be prepared at the conclusion of the incident. This report will detail:

The nature and scope of the incident.

The actions taken during the phases of detection, containment, eradication, and recovery.

Steps to prevent recurrence of similar incidents.

This report will be shared with executive management and legal counsel for review. Reporting templates are provided in Appendix B to standardize and facilitate the documentation process.

Effective information recording during an incident is essential not only for successful containment and eradication but also for post-incident analysis and potential legal action. Each IRT member is required to chronologically document their actions and findings using the IRT Incident Record Form found in Appendix B. This documentation is critical for drawing lessons learned and for use in legal proceedings if necessary.

While no incident will follow a perfectly scripted sequence, this plan serves as a robust framework for managing cybersecurity and data breach incidents.

Legal and Compliance

In the event of a data breach, the IRT must comply with applicable breach notification laws such as GDPR, CCPA, HIPAA, and other relevant frameworks. Following the guidelines set forth by the NIST SP 800-61 framework, the breach notification process must be timely, transparent, and follow strict legal protocols.

Compliance Methods:

Notification of Affected Parties:

Under GDPR Article 33, any data breach must be reported to the relevant supervisory authority within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. If personal data is at risk, affected individuals must also be notified “without undue delay.”

CCPA (California Consumer Privacy Act) mandates that businesses notify California residents “in the most expedient time possible” if their unencrypted or unredacted personal information has been compromised.

HIPAA (Health Insurance Portability and Accountability Act) requires covered entities to notify affected individuals within 60 days of a breach affecting protected health information (PHI). If the breach affects more than 500 individuals, media outlets and the U.S. Department of Health and Human Services must also be notified.

Use of [Vendor] Compliance Manager:

[Vendor] Compliance Manager streamlines the management and documentation of regulatory requirements. This tool ensures the organization remains compliant by automating the tracking of legal obligations such as breach notification timelines under GDPR, CCPA, and HIPAA. The system maintains an audit trail for each action taken, helping to verify that notification obligations are met within legal timeframes.

Regulatory Authority Notification:

Under GDPR, organizations must notify the Data Protection Authority (DPA) within the prescribed 72-hour timeframe, providing details of the breach, including its nature, the number of records affected, and the steps taken to mitigate the impact.

CCPA requires documentation of notifications made to the California Attorney General for breaches involving sensitive personal information.

For HIPAA, breaches must be reported to the Office for Civil Rights (OCR), either immediately for larger breaches (500+ records) or annually for smaller incidents.

Risk Assessment and Documentation:

Following NIST SP 800-61's incident handling guidelines, organizations should conduct a post-breach risk assessment to evaluate the potential harm caused to individuals whose data was compromised. This assessment should include whether the breach is likely to result in physical, material, or non-material damage to individuals.

Encryption and Data Minimization:

To comply with GDPR and CCPA, organizations should demonstrate that appropriate encryption and pseudonymization measures were in place at the time of the breach. If the data was encrypted, breach notification requirements may be waived or reduced. Following NIST SP 800-61, strong encryption mechanisms should be integrated into all sensitive data storage systems to mitigate the impact of breaches.

Training and Awareness:

HIPAA and NIST SP 800-61 both emphasize the importance of ongoing security awareness training. Employees should be trained to understand their role in detecting and reporting potential breaches, and the organization should maintain training logs to prove compliance during a breach investigation.

Third-Party Vendor Breach Notification:

If a breach occurs through a third-party service provider, both GDPR (Article 28) and CCPA require that the provider notify the data controller or business "without undue delay." This notification triggers the organization's obligation to inform the affected individuals and regulatory authorities, ensuring swift compliance with legal frameworks.

Lessons Learned & Continuous Improvement

Post-Incident Review:

After a major incident, the IRT will conduct a post-mortem to discuss what went well and what needs improvement. The review will include:

Detection and containment effectiveness.

Communication efficiency.

Incident documentation and reporting.

Policy Updates: Update this IRP based on lessons learned. Also, update security policies, training programs, and tools as needed.

Training and Testing:

Simulations: Conduct regular incident response drills and simulations using MDE’s capabilities to ensure the team is familiar with the process.

Education: Train employees regularly on recognizing phishing emails, social engineering, and other threats.

Incident Response Process Timeline

The response process, at a detail level, for an incident includes 5 of the 6 life cycle phases, as it excludes the Preparation phase. The detailed steps and general timing of an incident response are outlined below. The IT function is specifically called out as an involved party, separate from other SME’s.

Appendix A - Cyber Incident Response Team (IRT)

[CISO], CISO, Phone: , Email:

[Engineering Lead], Engineering Lead, Phone , Email:

[Security Operations Lead], Information Security Operations Lead, Phone , Email:

[Security Operations Analyst], Information Security Operations Analyst, Phone:, Email:

Appendix B - Cyber Incident Response Team (IRT)

IRT Incident Record Form

Recorded Information and Events

Document Version History

Appendix C - Cyber Incident Response Team (IRT)

Links to [Vendor] documentation and resources:

Appendix D - Incident Impact Definitions