[redacted]'s Incident Response Plan

Table of Contents:

1. General Information

1. Date: 02/11/2025
2. Policy owner (Student Name): Christian Stevens
3. Client company name: [redacted]
4. Version: 1.0

2. Purpose

This incident Response Plan (IRP) establishes clear protocols and procedures for effectively managing and responding to cybersecurity incidents within the [redacted] organization. It is designed to safeguard individuals, ensure compliance with regulatory standards, protect sensitive information, and minimize operational disruptions.

This IRP defines the roles and responsibilities of [redacted] personnel in addressing cybersecurity threats, technical failures, and other unexpected incidents. By implementing a structured response framework, [redacted] aims to enhance preparedness, enable rapid decision-making, and uphold legal and security requirements.

This plan fosters a secure and resilient cyber environment through ongoing training, communication, and coordination. It strengthens public trust in the organization's services while prioritizing the integrity and safety of all stakeholders.

3. Scope

This [redacted] Incident Response Plan (IRP) applies to all cybersecurity incidents that may impact the [redacted] organization, including its networks, systems, data, and digital assets. It covers threats such as data breaches, malware infections, denial-of-service attacks, unauthorized access, phishing attempts, insider threats, and other security incidents that could compromise confidentiality, integrity, or availability.

The IRP applies to all employees, contractors, third-party vendors, and anyone with access to [redacted] IT infrastructure. It outlines procedures for identifying, containing, mitigating, recovering from, and reporting cybersecurity incidents to minimize operational disruptions and protect sensitive information.

This plan ensures compliance with legal, regulatory, and industry security standards while integrating with broader business continuity and disaster recovery efforts. It is designed to be adaptable, evolving with emerging threats, technological advancements, and organizational changes.

4. Incident and Event Definitions

1. Data Breach Definition

A data breach is an incident in which unauthorized individuals gain access to, acquire, disclose, or compromise sensitive, confidential, or protected data. This may involve personal, financial, legal, or proprietary information being exposed, stolen, or altered accidentally or through malicious actions.

Common Causes of Data Breaches:

- Cyberattacks – Hacking, malware, ransomware, phishing, or other unauthorized intrusions.
- Insider Threats – Intentional or accidental exposure of sensitive data by employees or contractors.
- Lost or Stolen Devices – Unsecured laptops, smartphones, or external storage devices containing sensitive data.
- System Vulnerabilities – Exploitation of software, networks, or applications security weaknesses.
- Misconfiguration & Human Error – Accidental exposure due to improper system settings or unauthorized data sharing.

Potential Consequences of a Data Breach:

- Financial losses due to fraud, fines, or lawsuits.
- Reputational damage leading to loss of trust and business.
- Regulatory penalties for non-compliance with data protection laws.

- Operational disruptions affecting business continuity.

Response to a Data Breach:

Upon detection, [redacted] will activate its Cyber Incident Response Plan (IRP) to contain the breach, assess the impact, notify affected parties as required by law, and implement corrective measures to prevent future occurrences.

2. Malware Malfunctions Definition

A malware malfunction occurs when malicious software (malware) disrupts, damages, or compromises the regular operation of an IT system, network, or device. Malware can infiltrate systems through various attack vectors, leading to data corruption, unauthorized access, performance degradation, or total system failure.

Types of Malware Malfunctions:

- Viruses – Self-replicating programs that attach to legitimate files and spread across systems.
- Worms – Standalone programs that spread automatically through networks, consuming resources.
- Trojans – Malicious programs disguised as legitimate software to deceive users into executing them.
- Ransomware – Encrypts files or systems, demanding payment for decryption.
- Spyware – Secretly gathers user information, including passwords and sensitive data.
- Adware – Displays intrusive advertisements and may collect user data without consent.
- Rootkits – Grants attackers deep system access while remaining hidden from detection tools.

Causes of Malware Malfunctions:

- Phishing emails and malicious attachments
- Infected software downloads or updates
- Exploitation of unpatched vulnerabilities
- Compromised USB drives or external devices
- Drive-by downloads from malicious websites

Impact of Malware Malfunctions:

- System slowdowns, crashes, or complete failures

- Unauthorized access and data breaches
- Financial losses due to fraud, ransom demands, or operational downtime
- Legal and compliance violations if sensitive data is exposed

Response to Malware Malfunctions:

[redacted] will follow its Cyber Incident Response Plan (IRP) to detect, contain, eradicate, and recover from malware infections. This includes isolating affected systems, conducting forensic analysis, updating security protocols, and implementing preventive measures to reduce future risks.

3. Denial-of-Service (DoS) Attacks Definition

A Denial-of-Service (DoS) attack is a cyberattack that aims to overwhelm a system, network, or service, rendering it slow or completely unavailable to legitimate users. Attackers achieve this by flooding the target with excessive traffic, exploiting vulnerabilities, consuming system resources, and disrupting normal operations.

Types of Denial-of-Service (DoS) Attacks:

- Volumetric Attacks – Overload bandwidth by flooding the network with excessive traffic (e.g., UDP floods, ICMP floods).
- Protocol Attacks – Exploit vulnerabilities in network protocols to consume server resources (e.g., SYN flood, Ping of Death).
- Application Layer Attacks – Target specific applications or services to exhaust server resources (e.g., HTTP floods, Slowloris attacks).
- Distributed Denial-of-Service (DDoS) Attacks – A more severe DoS attack where multiple compromised devices (botnets) coordinate to attack a target.

Causes of DoS Attacks:

- Exploitation of network or software vulnerabilities
- Use of botnets or compromised systems to generate attack traffic
- Inadequate security configurations or lack of traffic filtering
- Malicious intent from cybercriminals, competitors, or hacktivist groups

Impact of DoS Attacks:

- Service downtime, preventing access to critical applications or websites
- Loss of productivity and operational disruptions
- Financial losses due to downtime or mitigation costs
- Potential reputational damage and loss of customer trust

Response to DoS Attacks:

[redacted] will activate its Cyber Incident Response Plan (IRP) to detect, mitigate, and recover from DoS attacks. This includes implementing traffic filtering, rate limiting, deploying anti-DDoS solutions, isolating affected systems, and strengthening network defenses to prevent future occurrences.

4. Unauthorized Access Definition

Unauthorized access is any instance where an individual, system, or process gains entry to a network, system, application, or data without proper authorization or permission. This can occur due to cyberattacks, insider threats, weak security controls, or accidental exposure of credentials.

Common Causes of Unauthorized Access:

- Weak or stolen credentials – Use of compromised passwords or lack of multi-factor authentication (MFA).
- Phishing attacks – Social engineering tactics to trick users into revealing login credentials.
- Exploiting software vulnerabilities – Using security flaws to bypass authentication controls.
- Insider threats – Employees or contractors misusing access privileges.
- Misconfigured security settings – Open databases, unrestricted administrative access, or poor access control policies.
- Lost or stolen devices – Unauthorized use of unattended or stolen laptops, smartphones, or storage devices.

Impact of Unauthorized Access:

- Data breaches – Exposure, theft, or modification of sensitive information.
- System compromise – Attackers gaining control over IT infrastructure.
- Financial losses – Fraud, regulatory fines, and recovery costs.
- Reputational damage – Loss of trust from customers, partners, or stakeholders.
- Legal consequences – Non-compliance with data protection laws and industry regulations.

Response to Unauthorized Access:

[redacted] will follow its Incident Response Plan (IRP) to detect, contain, and remediate unauthorized access incidents. This includes identifying the breach, revoking unauthorized privileges, conducting forensic analysis, notifying affected parties if necessary, and strengthening security measures such as implementing MFA, access logs, and least-privilege principles.

5. Phishing Attacks Definition

A phishing attack is a type of cyberattack where an attacker impersonates a trusted entity to deceive individuals into revealing sensitive information, such as login credentials, financial details, or personal data. These attacks typically occur through fraudulent emails, messages, websites, or phone calls designed to manipulate victims into taking harmful actions.

Common Types of Phishing Attacks:

- Email Phishing – Fake emails pretending to be from legitimate organizations, often containing malicious links or attachments.
- Spear Phishing – Targeted phishing attacks customized for specific individuals or organizations to increase credibility.
- Whaling – A specialized form of spear phishing aimed at high-ranking executives or key decision-makers.
- Smishing (SMS Phishing) – Fraudulent text messages attempting to trick users into clicking malicious links.
- Vishing (Voice Phishing) – Attackers use phone calls to impersonate authorities or service providers to extract sensitive information.
- Clone Phishing – A legitimate email is copied and resent with altered links or attachments containing malware.

Common Indicators of Phishing Attacks:

- Urgent or threatening language prompting immediate action.
- Suspicious sender addresses or domain names.
- Unexpected attachments or links requesting sensitive information.
- Poor grammar, formatting errors, or inconsistencies.
- Requests for personal, financial, or login details.

Impact of Phishing Attacks:

- Credential theft – Unauthorized access to accounts and systems.
- Financial fraud – Loss of funds due to fraudulent transactions.
- Data breaches – Exposure of sensitive company or customer information.
- Malware infections – Phishing emails often distribute ransomware, spyware, or trojans.
- Reputational damage – Loss of customer trust and potential regulatory penalties.

Response to Phishing Attacks:

[redacted] will follow its Incident Response Plan (IRP) to identify, contain, and mitigate phishing incidents. This includes reporting and blocking phishing emails, alerting affected users, revoking compromised credentials, conducting security awareness training, and implementing email filtering, multi-factor authentication (MFA), and other preventive security measures.

6. Insider Threats Definition

Insider threats refer to security risks posed by individuals within an organization who have authorized access to systems, networks, or data, but misuse this access either maliciously or unintentionally. These individuals may include employees, contractors, vendors, or anyone with privileged access to the organization's critical resources.

Types of Insider Threats:

- Malicious Insiders – Employees or individuals who intentionally exploit their access to harm the organization, such as stealing data, committing fraud, or sabotaging systems.
- Negligent Insiders – Employees who unintentionally cause security breaches or disruptions due to carelessness, lack of awareness, or failure to follow security protocols (e.g., mishandling sensitive data or falling for phishing attacks).
- Compromised Insiders – Individuals whose accounts or access credentials are taken over by external attackers through social engineering, phishing, or other means, making them unwitting participants in an attack.

Common Causes of Insider Threats:

- Lack of security awareness – Employees unaware of security best practices or proper data handling procedures.
- Uncontrolled access – Over-permissioned users with access to sensitive data or systems they don't need for their job.
- Job dissatisfaction or disgruntlement – Employees with personal grievances may intentionally cause harm to the organization.
- Weak access controls – Failure to enforce role-based access control or implement least-privilege access principles.
- Unmonitored activity – Lack of proper monitoring, auditing, or logging to detect suspicious behavior.

Impact of Insider Threats:

- Data breaches – Unauthorized access to or theft of sensitive company, customer, or employee data.
- Financial losses – Fraud, theft of intellectual property, or regulatory fines.
- Reputational damage – Loss of public trust, customer confidence, and potential loss of business.
- Operational disruption – Deliberate sabotage of systems, leading to downtime or loss of critical data.
- Legal and compliance risks – Violation of data protection regulations, leading to legal action or penalties.

Response to Insider Threats:

[redacted] will follow its Incident Response Plan (IRP) to detect, contain, and investigate insider threats. This includes monitoring user activity, enforcing strict access controls, conducting regular security audits, providing security training to employees, and implementing data loss prevention (DLP) tools to safeguard against unauthorized access or data exfiltration.

7. Cybersecurity Event

A cybersecurity event is any observable occurrence within [redacted] IT environment that may affect the confidentiality, integrity, or availability of its systems, data, or networks. Events may be routine activities, anomalies, or security-related activities that do not necessarily indicate a security breach but require monitoring and analysis. Examples of cybersecurity events include:

- Unusual network traffic patterns
- Failed login attempts exceeding normal thresholds
- Detection of malware by security tools
- Unexpected system behavior or performance degradation

8. Cybersecurity Incident

A cybersecurity incident is any confirmed or suspected event that threatens [redacted] IT systems, data, or digital assets by violating security policies, regulations, or expected operations. Incidents require an active response to mitigate risks and minimize potential damage. Examples of cybersecurity incidents include:

- Unauthorized access or system intrusion
- Data breaches resulting in unauthorized data exposure or theft
- Ransomware, malware, or other malicious software infections
- Phishing attacks leading to credential compromise
- Denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks
- Insider threats involving deliberate or accidental data leaks
- Exploitation of vulnerabilities leading to unauthorized system control

5. Incident Reporting & Documentation

1. Reporting

If any [redacted] employee, contractor, user, or customer becomes aware of an information security event, incident, potential incident, unauthorized access, policy violation, security vulnerability, or suspicious activity, they must promptly report the information using one of the following communication channels:

Email: help@[redacted].com with details or reports regarding the event or incident.

Reporters should act as responsible witnesses, treating the situation as if reporting a crime. Reports should include specific, accurate details about what has been observed or discovered.

2. Severity

The IT Manager is responsible for monitoring reports of security incidents or events. For example, [redacted] Support Teams shall monitor incident and event tickets and assign tickets based on the following categories.

1. P3 Low Severity

A low-severity cybersecurity incident is a security event that has minimal impact on an organization’s operations, data, or users. These incidents do not immediately threaten critical systems, sensitive information, or business continuity. They typically require monitoring and minor corrective actions but do not necessitate an urgent response.

2. P2 Medium Severity

A medium-severity cybersecurity incident is a security event that moderately impacts an organization's operations, data, or users. While it does not immediately threaten critical systems or sensitive data, it requires timely intervention to prevent escalation into a high-severity incident.

3. P1 - High Severity

A high-severity cybersecurity incident is a critical security event that significantly threatens an organization's operations, data integrity, or user safety. These incidents often require immediate action and can lead to substantial financial loss, reputational damage, or legal repercussions if not addressed swiftly.

4. **P0 - Critical Severity**

   A critical-severity cybersecurity incident is an extremely serious security event that poses an immediate and severe threat to an organization’s operations, data integrity, and overall security posture. These incidents can result in catastrophic consequences, including significant financial loss, major operational disruption, and long-lasting damage to reputation and trust.

3. Escalation and Internal Reporting

The incident escalation contacts can be found below in Appendix A.

P0 - Critical Severity: Internal Stakeholders, Legal and Compliance, External Stakeholders, Public Relations and Communications, Affected Customers and Partners, and Insurance Providers.

P1 - High Severity: Internal Stakeholders, Legal and Compliance, External Stakeholders, Affected Customers and Partners, Public Relations and Communications, and Insurance Providers.

P2/P3 - Medium and Low Severity: Internal Stakeholders, Department Heads or Managers, Employees Involved, and the Incident Response Records.

4. Documentation

All reported security events, incidents, and response activities shall be documented and adequately protected in Amazon Web Services (AWS).

A root cause analysis may be performed on all verified <P0> security incidents. The incident ticket shall document and reference a root cause analysis report. The IT Manager shall review the root cause analysis and determine if a post-mortem meeting will be called.

6. Incident Response Process

For critical issues, the response team will follow an iterative response process designed to investigate, contain exploitation, eradicate the threat, recover system and services, remediate vulnerabilities, and document a post-mortem report including the lessons learned from the incident.

a. Summary

- Event reported
- Triage and analysis
- Investigation

- Containment & neutralization (short-term/triage)
- Recovery & vulnerability remediation
- Hardening & Detection improvements (lessons learned, long-term response)

b. Detailed

- The IT Manager or Chief Executive Officer will manage the incident response effort
- If necessary, a central “War Room” will be designated, which may be a physical or virtual location (i.e. Slack channel)
- A recurring Incident Response Meeting will occur at regular intervals until the incident is resolved
- Legal and executive staff will be informed as required

c. Incident Response Meeting Agenda

- See the Incident Response Meeting Agenda link below:
- https://docs.google.com/document/d/1FS4tUijN63Nz-Ki2rWq359_IoQ1KuDvG/edit?usp=drive_link&ouid=100811395158769932063&rtpof=true&sd=true

7. Detection Tools

This section provides an overview of the types of solutions and tools used to detect and manage security incidents within the organization.

Types of Solutions and Tools

1. Splunk

Splunk is a powerful Security Information and Event Management (SIEM) and log management tool that collects, analyzes, and visualizes machine-generated data in real-time. It is widely used for security monitoring, threat detection, IT operations, and business analytics.

2. Snort

Snort is an open-source Intrusion Detection and Prevention System (IDPS) that monitors network traffic in real-time to detect and prevent security threats. Developed by Cisco, Snort is widely used for network security monitoring and threat detection.

3. Amazon Web Services (AWS)

AWS (Amazon Web Services) is a cloud computing platform provided by Amazon. It offers a wide range of cloud-based services, including computing power, storage, databases, networking, security, and machine learning, allowing businesses and individuals to build, deploy, and scale applications efficiently.

8. Special Considerations

1. Internal Issues

The Incident Response Plan (IRP) addresses internal issues that may arise during or after an incident.

1. Employee Misconduct or Negligence

- Unauthorized Access or Data Handling – Employees accessing, sharing, or mishandling sensitive data.
- Failure to Follow Protocols – Non-compliance with IRP procedures, delaying response efforts.
- Insider Threats – Intentional harm caused by malicious insiders, requiring monitoring and risk assessments.

2. Lack of Awareness or Training

- Inadequate Security Knowledge – Employees falling victim to phishing or social engineering attacks.
- Unclear Reporting Procedures – Delays in identifying and escalating security incidents.
- Limited Technical Skills – Insufficient expertise among staff to respond to advanced cyber threats.

3. Resource Constraints

- Insufficient Personnel – Lack of dedicated security staff to handle complex incidents.
- Limited Budget or Tools – Inadequate investment in cybersecurity technologies and response mechanisms.
- Overworked Teams – Burnout and inefficiencies due to excessive workload during prolonged incidents.

4. Policy or Compliance Gaps

- Outdated Incident Response Plan – Failure to update the IRP to address evolving threats.
- Regulatory Non-Compliance – Lack of adherence to industry standards and legal requirements.
- Weak Access Controls – Poor implementation of security policies, increasing vulnerability to attacks.

5. Conflict of Interest or Leadership Challenges

- Disagreements on Response Actions – Conflicts among leadership or security teams delaying decision-making.
- Lack of Executive Support – Insufficient backing from leadership to enforce security measures and allocate resources.
- Conflicting Business Priorities – Balancing security needs with operational and financial concerns.

Mitigation Strategies

- Regular Training and Awareness Programs – Strengthen employee security knowledge and reporting procedures.
- Clear Communication Protocols – Establish structured internal messaging and escalation pathways.
- Adequate Resource Allocation – Ensure dedicated personnel, tools, and budget for incident response.
- Frequent Policy Reviews – Update security policies and response plans based on emerging threats.
- Strong Leadership and Accountability – Define clear roles and responsibilities to enhance coordination

2. Compromised Communications

Communication channels may be compromised in a security incident, posing risks to internal coordination and external disclosures. The Incident Response Plan (IRP) establishes protocols to detect, mitigate, and recover from compromised communication channels.

Identify compromised communication by reviewing emails and phishing attacks and checking for unauthorized access. Once identified, the Incident Response Team must isolate all affected channels to prevent further security risks. Switch to secure alternatives and identify the causes.

3. Root Account Compromise

This document provides a structured response plan for incidents involving Amazon Web Services (AWS) resource compromise. Please see the playbook in Appendix D.

4. Additional Requirements

- Suspected and reported events and incidents shall be documented

- Suspected incidents shall be assessed and classified as either an event or an incident
- Incident response shall follow this plan and any associated procedures.
- All incidents shall be formally documented, and a documented root cause analysis shall be performed
- Incident responders shall collect, store, and preserve incident-related evidence in accordance with industry guidance and best practices, such as NIST SP 800-86's Guide to Integrating Forensic Techniques into Incident Response.
- The incident response team shall review suspected and confirmed unauthorized access events. The Chief Executive Officer and Legal Team shall only make breaching determinations.
- [redacted] shall promptly and properly notify customers, partners, users, affected parties, and regulatory agencies of relevant incidents or breaches in accordance with [redacted] policies, contractual commitments, and regulatory requirements, as determined by the Chief Executive Officer and Legal Department.
- This Incident Response Plan shall be reviewed and formally tested at least annually. Results of IR plan testing activities, including findings and lessons learned, will be formally documented and maintained to support security, compliance, and audit requirements

9. External Communications and Breach Reporting

Clear and timely communication is essential during a security incident to maintain transparency, comply with regulations, and protect the organization's reputation. The Incident Response Plan (IRP) establishes protocols for external communications and breach reporting to ensure consistency and compliance.

1. External Communications

- Designated Spokesperson – Only authorized personnel, such as the Public Relations (PR) Team, Legal Team, or Incident Response Manager, may communicate with external parties.
- Consistent Messaging—To prevent misinformation, all public statements must align with legal, regulatory, and business considerations.
- Media and Public Relations – If necessary, issue press releases or official statements to address public concerns and mitigate reputational risks.
- Customer Notifications – Provide clear, concise, and actionable information to affected customers while safeguarding sensitive details.

2. Breach Reporting

- Regulatory Compliance – Report security breaches to regulatory bodies within required timeframes (e.g., GDPR, CCPA, HIPAA).
- Law Enforcement Notification – Engage with law enforcement agencies when incidents involve criminal activity, such as data theft or fraud.
- Data Controller and Partner Reporting – Inform third-party data controllers, vendors, or partners in accordance with contractual obligations.
- Incident Documentation – Maintain detailed records of the breach, including its scope, impact, response actions, and communication efforts.

3. Timelines and Escalation

- Immediate Assessment – Determine if a breach meets reporting thresholds based on regulatory requirements.
- Notification Deadlines – Follow legal timelines for breach disclosure (e.g., 72 hours under GDPR).
- Ongoing Updates – Provide follow-up communications as new information becomes available.

By implementing structured external communication and breach reporting processes, the organization ensures regulatory compliance, preserves trust, and mitigates reputational damage.

10. Mitigation and Remediation

Mitigation measures are essential to minimizing the impact of security incidents and preventing recurrence. The Incident Response Plan (IRP) outlines structured actions to contain threats, reduce risks, and restore normal operations efficiently.

1. Immediate Containment
   - Isolate Affected Systems – Disconnect compromised devices or networks to prevent further spread.
   - Limit Access – Temporarily revoke user privileges or enforce stricter access controls.
   - Deploy Security Controls – Activate firewalls, intrusion prevention systems, and endpoint protections as necessary.

2. Threat Eradication
   - Identify and Remove Malicious Elements – Scan for and eliminate malware, unauthorized access points, or exploited vulnerabilities.
   - Patch and Update Systems – Apply security updates to prevent re-exploitation.
   - Reset Credentials – Change passwords and enforce multi-factor authentication (MFA) if needed.

3. Impact Assessment and Recovery
    - Analyze Affected Data and Systems – Determine the extent of data loss or corruption.
    - Restore from Backups – Ensure systems are recovered using clean, verified backups.
    - Validate System Integrity – Conduct security testing to confirm successful mitigation before resuming full operations.

4. Preventative Measures
    - Enhance security policies by updating protocols based on lessons learned from the incident.
    - Increase Employee Awareness – Conduct security training and phishing simulations.
    - Strengthen Monitoring and Detection – Improve logging, anomaly detection, and automated response capabilities.

5. Continuous Improvement
    - Post-Incident Review – Conduct a formal analysis to identify gaps and recommend improvements.
    - Update Incident Response Plan – Modify procedures to address emerging threats and organizational changes.
    - Implement Long-Term Security Enhancements – Invest in new technologies, threat intelligence, and proactive risk assessments.

By following these mitigation steps, the organization can reduce downtime, protect sensitive data, and strengthen overall cybersecurity resilience.

11. Cooperation with Customers, Data Controllers and Authorities

Effective incident response requires transparent and coordinated cooperation with customers, data controllers, and authorities to ensure compliance, trust, and efficient resolution of security incidents. The Incident Response Plan (IRP) outlines the following principles for engagement:

1. Cooperation with Customers

- Timely Notification – Inform affected customers of security incidents, following regulatory and contractual obligations.
- Clear Communication – Provide accurate and transparent updates on incident status, impact, and remediation efforts.

- Support and Guidance – Offer recommendations on mitigating potential risks, such as password changes or fraud monitoring.
- Privacy Protection – Ensure customer data is handled securely and complies with applicable data protection laws.

2. Cooperation with Data Controllers (for Organizations Processing Third-Party Data)

- Incident Reporting – Notify data controllers promptly in accordance with data processing agreements (DPAs).
- Compliance with Contractual Obligations – Follow established protocols for investigating and mitigating data breaches.
- Joint Investigation and Resolution – Collaborate with data controllers to determine root causes, containment strategies, and corrective actions.
- Documentation and Reporting – Provide detailed reports on incident findings, response measures, and lessons learned.

3. Cooperation with Authorities

- Regulatory Compliance – Adhere to legal requirements for reporting security breaches to relevant authorities (e.g., GDPR, CCPA, industry-specific regulations).
- Law Enforcement Engagement – Work with law enforcement agencies when incidents involve cybercrime, fraud, or data theft.
- Incident Disclosure and Investigation – Provide necessary evidence and assistance to authorities while maintaining confidentiality.
- Audit and Compliance Support – Facilitate regulatory audits and inquiries by supplying requested documentation and incident details.

By fostering proactive cooperation with these stakeholders, the organization ensures legal compliance, minimizes reputational damage, and strengthens cybersecurity resilience.

12. Roles & Responsibilities

An effective response requires clearly defined roles and responsibilities to ensure a coordinated and efficient approach. The following outlines key roles within the Incident Response Plan (IRP) and their respective responsibilities.

13. Response Team Members

Role	Responsibility
Incident Manager	• Oversees and directs the IRT during an incident. • Ensures compliance with the IRP and regulatory requirements.

	• Coordinates with executive leadership and external entities as necessary. • Approves major decisions related to containment, mitigation, and recovery.
Incident Response Team (IRT)	• Leads and coordinates incident response efforts. • Assesses the severity and impact of security incidents. • Implement response and containment measures. • Communicates with stakeholders and escalates incidents as needed. • Documents incident details and response actions for future analysis.
Legal & Compliance Team	• Ensures incident response aligns with legal and regulatory requirements. • Advises on privacy, data protection, and breach notification obligations. • Coordinates with law enforcement and regulatory agencies if required.
Communication & Public Relations Team	• Manages internal and external communication related to incidents. • Prepares statements for affected parties, customers, and the public. • Ensures messaging aligns with legal, compliance, and leadership directives.
Executive Leadership Team	• Provides strategic oversight and approves high-impact response actions. • Allocates resources to support incident response and recovery efforts. • Engages with external stakeholders, such as regulators and business partners.
Human Resources	• Assists in addressing security incidents involving employees. • Ensures compliance with workplace policies and disciplinary actions. • Supports employee awareness and security training initiatives.
IT Security Team	• Investigate, analyze, and mitigate security threats. • Implement technical controls to contain and remediate incidents. • Provides forensic analysis and threat intelligence. • Maintains and updates security tools and incident detection mechanisms.
External Customers/Suppliers	• Collaborate with the IRT to minimize operational disruption. • Provide insights into affected systems, data, and processes. • Support recovery efforts and implement business continuity measures.

14. Management Commitment

[redacted] management has approved this policy and is committed to providing the necessary resources, tools, and training to effectively respond to security events and incidents that may impact the company or its customers.

15. Exceptions

While the Incident Response Plan (IRP) establishes standardized procedures for managing security incidents, certain exceptions may apply based on an incident's nature, severity, or circumstances. Exceptions to this plan must be documented, justified, and approved by designated management or security personnel. The following are key scenarios where exceptions may be considered:

Unforeseen Threats or Zero-Day Attacks – If an incident involves a novel or unknown threat with no predefined response, deviations from standard procedures may be necessary to contain and mitigate risks effectively.

Legal or Regulatory Compliance Conflicts – If compliance with the IRP contradicts legal or regulatory requirements, necessary adjustments must be made to align with applicable laws while maintaining security integrity.

- Resource Constraints – In cases where personnel, technology, or budget limitations prevent full adherence to the IRP, alternative measures must be implemented to ensure an adequate response.
- Business Continuity Prioritization – If responding strictly according to the IRP could severely impact critical business operations, leadership may authorize modified response actions to balance security and operational continuity.
- Third-Party Involvement – When incidents involve external vendors, partners, or service providers, response procedures may be adjusted to align with contractual agreements and third-party policies.
- Force Majeure Events – Natural disasters, large-scale cyberattacks, or other uncontrollable events may necessitate a flexible approach to incident response outside the standard framework.

Any exceptions must be reviewed, documented, and approved by the Incident Response Team (IRT) or designated management to ensure accountability and continuous improvement of the IRP.

16. Violations & Enforcement

All employees, contractors, and stakeholders must adhere to the established protocols to maintain the integrity and effectiveness of the incident response plan (IRP). Whether intentional or accidental, violations of the IRP can compromise security and response efforts, leading to disciplinary actions or legal consequences.

1. Types of Violations

Violations of the IRP may include, but are not limited to:

- Failure to Report Incidents – Not reporting a suspected or confirmed security incident in a timely manner.
- Unauthorized Access or Disclosure – Accessing, sharing, or modifying sensitive information related to an incident without proper authorization.
- Non-compliance with Response Procedures—Failure to follow established incident response protocols can lead to delays or ineffective handling of an incident.
- Tampering with Evidence – Altering, destroying, or misrepresenting information relevant to an investigation.
- Lack of Cooperation – Refusing to collaborate with the Incident Response Team (IRT) or other designated personnel.

2. Enforcement and Disciplinary Actions

Violations will be assessed based on severity, intent, and impact. Enforcement measures may include:

- Verbal or Written Warning – For minor or first-time infractions.
- Mandatory Security Training – Required for individuals demonstrating negligence or lack of awareness.
- Access Restrictions or Revocation – Limiting or removing access to systems or data for security reasons.
- Employment Disciplinary Actions – Suspension, demotion, or termination for serious or repeated violations.
- Legal Consequences—Legal action may be pursued in cases of criminal misconduct, regulatory breaches, or contractual violations.

3. Reporting and Accountability

All employees and stakeholders are responsible for reporting potential violations to the Incident Response Manager, IT Security Team, or Compliance Department. The organization is committed to enforcing the IRP fairly and consistently to protect business operations, customer data, and regulatory compliance.

Version	Date	Description	Author	Approved by

1.0	2/19/2025	Version 1	Christian Stevens	Courtroom5

17. Appendix A – Contact Information

Contacts for IT and Engineering Management, as well as executive staff and, can be found: [redacted]

18. Appendix B – Incident Response Meeting

Incident Response Meeting Agenda
Date: [Insert Date]
Time: [Insert Time]
Location: [Insert Location] / Virtual Meeting Link: [Insert Link]
Facilitator: [Name]

1. Welcome and Introductions
- Brief introduction of participants (if necessary)
- Review meeting objectives

2. Incident Summary
- Overview of the incident (timeline, impact, affected systems, root cause analysis)
- Reports from key team members (IT, Security, Operations, etc.)

3. Response Actions Taken
- Steps taken to mitigate and contain the incident
- Current status of the response effort
- Identification of remaining risks or gaps

4. Lessons Learned and Improvements
- Review of challenges encountered during the response
- Discussion on what worked well and what did not
- Identification of areas for improvement
- Documentation of action items for future preparedness

5. Next Steps and Action Items
- Assign responsibilities for follow-up tasks
- Establish deadlines for implementation of improvements

- Plan for a follow-up meeting, if necessary

6. Q&A and Open Discussion

- Address any outstanding concerns
- Gather additional feedback from participants

7. Closing Remarks

- Summary of key takeaways
- Confirm action items and responsibilities
- Thank participants for their time and contributions

19. Appendix C – Incident Type

Here are the main types of **Cybersecurity Incidents**:

1. Unauthorized Access

- Gaining access to systems, accounts, or data without permission.
- Examples: Stolen credentials, brute-force attacks, insider threats.

2. Malware Infections

- Malicious software that disrupts, damages, or gains unauthorized access.
- Examples: Viruses, ransomware, trojans, spyware.

3. Phishing & Social Engineering

- Deceptive tactics to manipulate individuals into revealing sensitive information.
- Examples: Email phishing, spear-phishing, business email compromise (BEC).

4. Denial-of-Service (DoS) & Distributed Denial-of-Service (DDoS) Attacks

- Overwhelming systems to make them unavailable to users.
- Examples: Network flooding and application-layer attacks.

5. Data Breaches & Exfiltration

- Unauthorized access, exposure, or theft of sensitive data.
- Examples: Database leaks, cloud misconfigurations, insider threats.

6. Insider Threats

- Current or former employees, contractors, or partners misusing access.
- Examples: Data theft, sabotage, unauthorized access.

7. Credential Compromise

- Theft or leakage of authentication credentials.
- Examples: Password dumps, credential stuffing, keylogging malware.

8. Supply Chain Attacks

- Exploiting vulnerabilities in third-party vendors or software providers.
- Examples: Software backdoors, compromised updates, vendor breaches.

9. Advanced Persistent Threats (APTs)

- Long-term, targeted cyberattacks by sophisticated adversaries.
- Examples: Nation-state attacks, cyber espionage.

10. Misconfigurations & Vulnerabilities

- Security weaknesses due to improper configurations or outdated software.
- Examples: Open cloud storage, unpatched systems, exposed APIs.

20. Appendix D - Incident Response Playbook – Root Usage

Amazon Web Services Compromise Summary for Incident Response Plan

In the event of a security compromise in AWS, the **Incident Response Plan (IRP)** outlines a structured approach to effectively detect, respond to, contain, and recover from security breaches.

1. Detection & Identification

- Utilize AWS security tools like **GuardDuty, CloudTrail, Security Hub, and Macie** to detect anomalies, unauthorized access, or data exfiltration.
- Monitor AWS logs, IAM activity, and network traffic for signs of compromise.
- Classify the severity of the incident (low, medium, high, critical).

2. Containment

- Isolate compromised AWS resources (e.g., EC2 instances, IAM accounts) using Security Groups, VPC, or IAM role adjustments.
- Temporarily revoke access, rotate credentials, and enable MFA for affected users.
- Implement AWS WAF and Shield to mitigate potential ongoing attacks.

3. Eradication

- Investigate root causes using AWS Detective and CloudTrail logs.
- Patch vulnerabilities, remove malicious software, and apply security updates.
- Review IAM permissions and enforce least privilege access.

4. Recovery

- Restore affected workloads from S3, EBS, or RDS backups.
- Validate system integrity before resuming full operations.
- Perform post-incident monitoring using AWS security tools.

5. Lessons Learned & Prevention

- Conduct a post-mortem analysis to document the incident, response actions, and resolution.

- Implement security enhancements such as AWS Config rules, automated security baselines, and real-time monitoring.
- Update the Incident Response Plan based on insights from the breach.

By following this structured response plan, organizations can minimize the impact of Amazon Web Services (AWS) compromise and improve their overall cloud security posture.