Incident Response Policy

[Company Name / Department Name]

Document Version: 2.5
Effective Date: April 8, 2025

Policy Contributors:

Bryan Lim
Casey Sharp
Grzegorz Rudnicki
Jacob Garcia
Raquel Lugo

(Representing Security, IT Operations, Legal, Risk Management, and Executive Leadership)

Document ID: SEC-IRP-001 Rev. 2.5

Contents

1. Policy Overview

1.1. Purpose and Objectives

This Incident Response Policy (IRP) establishes the official framework, roles, responsibilities, communication channels, and systematic procedures for responding effectively to cybersecurity Incidents within [Company Name]. The primary objectives driving this policy are to:

- Ensure the rapid and efficient detection, analysis, and response to suspected or confirmed Incidents.
- Minimize adverse impacts resulting from Incidents, including operational disruption, financial loss, reputational damage, and legal liability.
- Facilitate the secure and timely restoration of affected services, systems, and data Assets to a known-good operational state.
- Guarantee compliance with all applicable legal, regulatory (e.g., GDPR, CCPA, HIPAA), and contractual obligations concerning incident handling, data protection, and breach notification. Reference specific compliance documentation [Ref: COMPLIANCE-REGISTER-001].
- Foster a culture of continuous improvement by systematically analyzing Incidents and integrating lessons learned into security controls, policies, and procedures.

Policy Statement

[Company Name] is fundamentally committed to maintaining a proactive and effective incident response capability as a cornerstone of its cybersecurity strategy and risk management framework. This policy mandates the establishment, training, and regular exercising of a formal Incident Response Team (IRT). It outlines the required phases of the incident response lifecycle, defines clear communication protocols for internal and external Stakeholders, and requires diligent adherence by all personnel. Failure to comply with this policy, including neglecting to report suspected Incidents or hindering response efforts, may constitute grounds for disciplinary action, up to and including termination of employment or contract, as stipulated in the Employee Code of Conduct [Ref: HR-POL-005] and relevant third-party agreements. This IRP operates in conjunction with, and does not supersede, other critical policies such as the Data Privacy Policy [Ref: DP-POL-001], Acceptable Use Policy (AUP) [Ref: IT-AUP-001], and the Business Continuity / Disaster Recovery Plan [Ref: BCDR-PLAN-001].

1.2. Policy Governance

This IRP is formally owned and maintained by the [Specify Department, e.g., Office of the Chief Information Security Officer (CISO)]. It is subject to review and approval by the [Specify Body, e.g., Information Security Steering Committee] on at least an annual basis, or more frequently if significant changes occur in the threat environment, organizational structure, critical technologies, regulatory landscape, or following major Incidents. Proposed exceptions to this policy must undergo a formal risk assessment process and require documented approval from the CISO or a designated equivalent authority [Ref: POLICY-EXCEPTION-PROC-001].

2. Audience

This policy applies universally to all individuals and entities granted access to [Company Name]'s information systems, network resources, or data assets, regardless of employment status, location, or relationship. This encompasses, but is not limited to:

- **All Employees:** Includes full-time, part-time, temporary, and contract employees across all departments and levels. All employees have a baseline responsibility to adhere to security practices, recognize potential threats, report suspected Incidents promptly via designated channels, and cooperate fully with response efforts when requested.
- **Information Technology (IT) and Security Personnel:** Staff within IT operations, network engineering, system administration, cloud engineering, application development, and cybersecurity departments (including the Security Operations Center (SOC) and core IRT) have specific operational duties related to implementing preventative controls, monitoring for threats, performing technical analysis, and executing response actions as defined in this policy and supporting procedures/Playbooks.
- **Management and Leadership:** Individuals in supervisory roles up to executive leadership are responsible for championing security culture, ensuring their teams understand and comply with this policy, allocating necessary resources and budget for preparedness and response capabilities, participating decisively in escalation procedures, and managing business implications during major Incidents.
- **Third-Party Vendors, Partners, and Contractors:** All external entities, consultants, service providers, or contractors granted logical or physical access to company systems, networks, or data are contractually obligated to comply with the principles of this policy, maintain appropriate security controls, and report any suspected Incidents affecting company Assets immediately according to the terms specified in their agreements and the Vendor Security Requirements [Ref: VENDOR-SECURITY-REQ-001].
- **Specific Response Roles:** Individuals formally designated with specific roles within the incident response structure (detailed in Section 5, e.g., Incident Commander, Legal Counsel, Privacy Officer, Communications Lead) must thoroughly understand and execute their explicit responsibilities as defined within this policy, associated Playbooks, and related documentation (e.g., Communication Matrix [Ref: IR-COMM-MATRIX-001]).

Ignorance of this policy does not excuse non-compliance. All personnel are required to complete relevant security awareness training, including incident reporting procedures, upon onboarding and annually thereafter [Ref: SECURITY-AWARENESS-TRAINING-PROG].

3. Scope

3.1. In Scope

This policy governs the response process for all confirmed or suspected cybersecurity Incidents impacting any organizational Asset, irrespective of location (on-premise, cloud, remote endpoint) or management model. Assets covered include, but are not limited to:

- **Information Systems:** All servers (physical/virtual), endpoints (desktops, laptops, mobile devices, IoT devices), network infrastructure (routers, switches, firewalls, VPNs), cloud services (IaaS, PaaS, SaaS accounts and configurations), and operational technology (OT) / industrial control systems (ICS) where applicable and integrated.

- **Data Assets:** All forms of organizational data, including customer databases, employee records (Personally Identifiable Information (PII)), financial information, intellectual property, source code, research data, operational logs, strategic plans, and third-party confidential information entrusted to the organization. Data handling must align with the Data Classification Standard [Ref: DATA-CLASS-STD-001].
- **Services & Applications:** Critical business applications (ERP, CRM), communication platforms (email, messaging, video conferencing), authentication systems (Active Directory, SSO), public-facing websites, APIs, and internally developed software.
- **Physical Security Intersections:** Events where a physical security breach (e.g., unauthorized facility access) directly leads to, or enables, a compromise of digital Assets.

The scope encompasses the entire incident lifecycle: Preparation, Detection & Analysis, Containment, Eradication, Recovery, and Post-Incident Activity.

3.2. Out of Scope

This policy does not directly govern the procedures for:

- **Business Continuity / Disaster Recovery (BC/DR):** While closely linked and often invoked concurrently, BC/DR focuses on restoring overall business functions following major disruptions (natural disasters, extended power outages, etc.). Refer to the corporate BC/DR Plan [Ref: BCDR-PLAN-001] for detailed procedures. IR focuses on the security aspects of an event.
- **Standard IT Support:** Routine technical assistance, hardware malfunctions (without security cause), software installation requests, or standard operational maintenance activities handled via the IT Help Desk ticketing system [Ref: HELPDESK-PORTAL-URL].
- **Physical Safety Emergencies:** Response to fire, medical emergencies, workplace violence, or environmental hazards are managed under separate Emergency Response Plans [Ref: EHS-EMERGENCY-PLAN-001].
- **Minor Operational Glitches:** Transient performance issues or minor bugs without evidence of malicious activity or significant security/business impact may be handled through standard operational procedures.

All activities under this policy must be conducted in accordance with the organization's AUP and any relevant data handling or privacy policies.

4. Definitions

To ensure unambiguous understanding, key terms employed throughout this policy are defined below. Consistent use of these terms, often referenced via glossary commands like `\gls{term}` or `\gls{ACRO}`, is crucial for clarity. The comprehensive glossary is provided in Appendix A. **Note:** If glossary terms appear as '?¿ in the final PDF, it indicates the document was not compiled correctly; see the critical compilation note in the LaTeX source code preamble.

5. Roles and Responsibilities

A successful incident response relies on coordinated action from multiple individuals and teams. The specific composition of the active IRT for any given Incident will depend on its nature and severity.

Table 1: Incident Response Roles and Responsibilities (Continued on next page if necessary)

Role / Group	Primary Responsibilities in Incident Response
Incident Commander (IC) / IRT Lead	Assumes overall tactical command during a declared Incident. Coordinates all response activities, facilitates communication, directs resource allocation according to the plan, makes critical time-sensitive decisions, ensures adherence to procedures, and serves as the primary interface between technical responders and management/other Stakeholders.
Security Operations Center (SOC) / Core IRT	Typically the first line of defense. Responsible for 24/7 monitoring of security alerts (Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), etc.), initial triage and validation of potential Incidents, performing preliminary analysis, executing initial Containment steps as defined in Playbooks, and maintaining detailed incident logs in the designated tracking system.
Technical Specialists (Extended IRT)	Subject Matter Experts (SMEs) integrated into the IRT based on the specific systems or technologies involved (e.g., Network Engineers, Cloud Architects, Database Administrators, Application Developers, OT Engineers). Provide in-depth technical expertise, perform advanced analysis, and execute complex remediation and Recovery tasks under the IC's direction.
Forensic Investigators (Internal/External)	Responsible for conducting deep-dive forensic analysis of compromised systems to precisely determine the timeline, scope, Root Cause, data accessed/exfiltrated, and Threat Actor TTPs. Critically important for preserving evidence in a legally defensible manner [Ref: FORENSIC-PROC-001] and supporting potential litigation or law enforcement action.
Threat Intelligence Analysts	Analyze internal and external threat data to provide actionable intelligence regarding active threats, attacker methodologies, relevant Indicator of Compromises (IoCs)/Indicator of Attacks (IoAs), and potential motivations. Helps the IRT understand the adversary and anticipate next steps. May involve analysis of malware or attacker infrastructure.
Management (IT / Security)	Provide strategic oversight, necessary resources (personnel, budget, tools), and organizational authority to support the IRT. Serve as key escalation points for critical decisions (e.g., service shutdowns, significant expenditures). Includes roles like Security Manager, Director of IT, up to the CISO.

Continued on next page...

Table 1 continued from previous page

Role / Group	Primary Responsibilities in Incident Response
Legal Department	Advises on all legal aspects of the Incident, including potential liabilities, regulatory compliance (breach notification laws under GDPR, CCPA, etc.), contractual obligations, evidence preservation standards, engagement with law enforcement, and maintaining attorney-client privilege over sensitive communications and investigative findings where applicable. Reviews and approves all external communications.
Privacy Officer / Team	Leads the assessment of impact on PII and other regulated data types. Ensures compliance with global data protection regulations and internal privacy policies [Ref: DP-POL-001]. Develops and executes the data breach notification strategy for affected individuals in coordination with Legal and Communications.
Human Resources (HR)	Manages Incidents involving potential employee misconduct, insider threats, or policy violations. Coordinates internal communications affecting employees. Plays a key role if employee PII is compromised. Ensures disciplinary actions align with corporate policy [Ref: HR-POL-015].
Communications / Public Relations (PR)	Develops and executes the approved internal and external communication strategy. Manages media inquiries, drafts public statements, customer notifications (content approved by Legal/Privacy), and ensures consistent messaging across all channels to protect corporate reputation.
Business Unit Leaders / System Owners	Provide critical context on the business impact of the Incident within their specific operational areas. Assist in identifying critical systems/data, participate in Recovery prioritization decisions, and lead the validation and sign-off process for restored systems/applications.
All Employees / Users	Have a fundamental responsibility to remain vigilant for suspicious activity, report potential Incidents immediately using established channels (e.g., [Specify Channel: Phishing Report Button, Help Desk Portal/Hotline]), adhere to security policies (the AUP), and fully cooperate with IRT requests during an investigation.

6. Incident Response Lifecycle

[Company Name] adheres to a structured incident response lifecycle, generally aligned with NIST SP 800-61 Rev. 2, encompassing the following phases:

6.1. Phase 1: Preparation

This ongoing phase ensures the organization is equipped to handle Incidents effectively. Activities include:

- **Policy, Plan, and Playbook Development & Maintenance:** Regular (at least annual) review and updating of this IRP, supporting procedures, and detailed, scenario-specific Playbooks. Version control is critical [Ref: DOC-CONTROL-PROC-001].
- **Asset Management Integration:** Maintaining a comprehensive and current inventory of critical hardware, software, and data Assets, including ownership and classification, to inform

response priorities [Ref: ASSET-MGMT-DB-LINK].

- **Tool Deployment, Configuration, and Tuning:** Implementing, configuring, and continuously optimizing security technologies (SIEM, EDR, Network Security Monitoring, Threat Intel Platforms, Security Orchestration, Automation, and Response (SOAR), Forensic Suites). Ensure adequate logging is enabled and logs are retained per policy [Ref: LOG-RETENTION-STD-001].
- **IRT Formation, Training, and Skill Assessment:** Establishing core and extended IRT rosters, defining roles, providing regular technical and procedural training, maintaining a skills matrix, and ensuring backup personnel are identified.
- **Exercises, Drills, and Testing:** Conducting periodic IR exercises (tabletop, functional, simulation) to test plans, tools, procedures, and team readiness. Document results and track remediation actions.
- **Threat Intelligence Integration:** Establishing processes to acquire, analyze, and integrate relevant threat intelligence (open source, commercial feeds, ISACs) into detection mechanisms (SIEM rules, EDR watchlists) and preparedness planning.
- **Secure Baseline Establishment:** Defining and monitoring expected normal behavior for networks, systems, and applications to facilitate anomaly detection.
- **Communication Channels:** Pre-establishing secure primary and backup communication methods (e.g., dedicated encrypted chat, conference bridges) for the IRT and Stakeholders.

6.2. Phase 2: Detection and Analysis

Identifying potential malicious activity, analyzing available evidence to confirm an Incident, and determining its initial scope and severity.

- **Monitoring & Alerting:** Continuous monitoring of diverse data sources: SIEM correlation alerts, EDR detections (IoCs and IoAs), IDS/IPS signatures, firewall/proxy logs, DNS queries, user-submitted reports (phishing emails, help desk tickets), threat intelligence feeds, cloud service logs, application-level logs.
- **Initial Triage & Validation:** SOC analysts perform rapid assessment of incoming alerts/reports. Filter false positives, correlate related events, enrich alerts with context (Asset criticality, user roles), and determine if further investigation is warranted based on predefined criteria [Ref: SOC-TRIAGE-PROC-001]. Document initial findings in the incident management system [Ref: INCIDENT-TRACKING-SYSTEM-URL].
- **In-Depth Analysis & Data Correlation:** Gather and analyze relevant forensic data (logs from multiple sources, network traffic captures, endpoint artifacts using EDR, memory dumps if necessary). Correlate findings to understand the sequence of events, identify potential IoCs/IoAs, and determine affected systems/data. Utilize threat intelligence (e.g., STIX/TAXII feeds) where applicable.
- **Incident Declaration & Classification:** Based on confirmed malicious activity or significant policy violation, the designated authority (e.g., SOC Shift Lead, IR Lead) formally declares an Incident, assigns a unique tracking identifier, and classifies its initial type and severity level (Section 7). This formally invokes this IRP.

- **Scope Determination (Initial):** Identify initially known affected systems, user accounts, data sets, and potential business impacts. Recognize that the full scope may evolve as the investigation progresses.
- **Documentation Initiation:** Immediately begin detailed, timestamped logging of all findings, actions taken, decisions made, and communications related to the Incident in the official record [Ref: INCIDENT-TRACKING-SYSTEM-URL].
- **Notification & Escalation Initiation:** Trigger internal notifications and the formal escalation process (Section 6.2.1) based on the initial classification and potential impact.

6.2.1. Escalation Path

Timely and appropriate escalation is critical for mobilizing necessary resources and ensuring management awareness and decision-making authority. The Incident Commander (IC) is responsible for initiating escalation according to these triggers:

- **Severity Level Trigger:**
  - *Low (4):* Managed primarily by Core IRT/SOC. Requires notification to Security Manager.
  - *Medium (3):* Requires engagement of relevant Extended IRT SMEs. Requires notification to Security Director/CISO. Legal/Privacy notification considered based on potential data sensitivity.
  - *High (2) / Critical (1):* Mandates immediate escalation notification to CISO, IT Leadership, Legal Counsel, Privacy Officer, HR Business Partner, Corporate Communications lead, and relevant Executive Leadership according to the pre-defined critical incident Communication Matrix [Ref: IR-COMM-MATRIX-001]. Activation of external resources (retained forensics firm, breach counsel) is typically considered at this level.
- **Incident Type Trigger:** Certain incident types automatically trigger a higher severity escalation, regardless of initial perceived scope. These include: confirmed breach involving regulated data (PII, PHI, CPNI, financial), successful ransomware deployment on critical systems, confirmed compromise of executive or highly privileged accounts, events posing immediate physical safety risk, or actions indicating nation-state Threat Actor involvement.
- **Time-Based Trigger:** Failure to achieve Containment or make significant progress within predefined time objectives for a given severity level (e.g., 4 hours for Medium, 1 hour for High) automatically triggers escalation to the next management tier.
- **Resource / Authority Trigger:** If the responding team determines they lack the necessary technical resources, personnel, budget, or organizational authority to effectively manage the Incident, they must immediately escalate to obtain support.

Detailed escalation contacts and procedures are documented within internal Playbooks [Ref: IR-PLAYBOOKS-DIR] and the Communication Matrix [Ref: IR-COMM-MATRIX-001].

6.3. Phase 3: Containment

Implementing actions to limit the spread of the Incident and prevent further damage while preserving necessary evidence.

- **Strategy Development & Selection:** The IC, in consultation with technical SMEs, threat intelligence, and potentially Legal/Management (depending on impact), rapidly develops and selects the most appropriate Containment strategy. Considerations include the type of threat, speed of propagation, affected environment (cloud, on-premise, OT), potential for tipping off the adversary, and the operational impact of the containment itself. Common strategies include network segmentation, host isolation via EDR or manual disconnect, firewall rule changes, disabling compromised accounts, DNS sinkholing/redirection, or temporary service shutdowns.
- **Short-Term (Tactical) Containment:** Execute immediate actions designed to quickly stop the bleeding (e.g., isolate the initially identified infected machines, block known malicious IP addresses).
- **Long-Term (Strategic) Containment:** Implement more durable measures as the investigation progresses and eradication plans form (e.g., re-architecting network segments with stricter controls, deploying temporary monitoring solutions on adjacent systems, implementing application-level blocks).
- **Evidence Preservation Considerations:** Ensure all Containment actions are documented and, where feasible, implemented in a way that preserves volatile data (memory) and system artifacts critical for forensic analysis and Root Cause determination. Follow established evidence handling procedures [Ref: FORENSIC-PROC-001].

6.4. Phase 4: Eradication

Methodically identifying and removing the Root Cause and all malicious artifacts associated with the Incident.

- **Comprehensive Root Cause Analysis (RCA):** Conduct thorough investigation leveraging forensic data, threat intelligence, and system analysis to pinpoint the initial entry vector, vulnerabilities exploited, lateral movement techniques, persistence mechanisms, and ultimate goals of the Threat Actor.
- **Systematic Threat Removal:** Execute procedures to eliminate all identified malicious elements: remove malware files and processes, delete attacker-created accounts or backdoors, revert unauthorized configuration changes, revoke compromised credentials, and patch exploited vulnerabilities across all affected systems.
- **Post-Eradication Validation Scanning:** After removal actions, perform thorough scans (vulnerability scans, malware scans, integrity checks) on affected systems to confirm successful Eradication and identify any missed artifacts.
- **Preventative Hardening:** Implement necessary security enhancements on affected and similar systems to prevent recurrence (e.g., apply security patches, strengthen password policies, implement stricter access controls, deploy compensating controls).

6.5. Phase 5: Recovery

Carefully restoring affected systems, data, and business services to a secure and fully operational state.

- **Recovery Strategy & Planning:** Based on the Incident and Eradication outcomes, determine the optimal recovery method(s). Options include: restoring systems from known-good, verified

backups taken before the compromise; rebuilding systems from scratch using hardened baseline images and reinstalling applications; or a hybrid approach. Plan for dependencies and sequence of restoration for critical services.

- **Secure System Restoration:** Execute the planned recovery actions, ensuring systems are brought back online in a secure configuration. Apply necessary patches and security updates during the restoration process. Validate data integrity after restoration from backups.
- **Rigorous Validation & Functional Testing:** Conduct comprehensive testing involving technical teams and business unit owners/users to confirm that restored systems and applications are fully functional, meet performance expectations, and are free from residual compromise. Obtain formal sign-off from business owners.
- **Post-Recovery Monitoring:** Implement a period of heightened monitoring on recovered systems (e.g., increased log scrutiny, network traffic analysis, EDR monitoring) to ensure stability and quickly detect any signs of recurrence or unforeseen issues.
- **Formal Declaration of Recovery:** Once validation is complete and systems are stable under normal load, the Incident Commander, with concurrence from key Stakeholders (including business owners and IT management), formally declares the affected systems/services as fully recovered.

6.6. Phase 6: Post-Incident Activity

Analyzing the Incident and the response effort to identify lessons learned and drive improvements.

- **Structured Post-Mortem Meeting:** Convene a formal lessons learned meeting within a defined timeframe (e.g., 5-10 business days post-recovery) involving all key participants (IRT, SMEs, Management, Legal, Privacy, Communications, affected Business Units). Utilize a structured agenda covering timeline review, impact assessment, effectiveness of tools and procedures, communication successes/failures, Root Cause confirmation, and identification of improvement opportunities. Ensure a blame-free environment focused on process improvement.
- **Comprehensive Incident Report Generation:** Produce a detailed final incident report tailored for different audiences (e.g., technical deep-dive for IR/IT teams, executive summary for leadership). The report must include: executive summary, detailed timeline, scope and impact analysis, investigative findings (Root Cause, TTPs), response actions taken (per phase), evaluation of response effectiveness, key metrics (Mean Time To Detect (MTTD), Mean Time To Respond/Resolve/Recover (MTTR), estimated costs), lessons learned, and specific, actionable recommendations for improvement [Ref: IR-REPORT-TEMPLATE-001].
- **Metrics Analysis & Reporting:** Analyze collected metrics (MTTD, MTTR variants, number of systems/users affected, estimated financial impact, recovery time objective (RTO) achievement) to measure response performance against benchmarks and identify areas needing investment or process change. Report trends to management.
- **Action Item Tracking & Implementation:** Assign ownership and deadlines for implementing all approved recommendations from the post-mortem. Track progress through a formal system [Ref: ACTION-ITEM-TRACKER-URL] until completion.
- **Documentation Updates:** Update this IRP, relevant Playbooks, checklists, technical procedures, system configurations, or training materials based on implemented improvements and lessons learned. Ensure proper version control.

- **Knowledge Management & Sharing:** Sanitize and archive incident reports and findings in a central knowledge base [Ref: IR-KNOWLEDGE-BASE-URL] to inform future responses and training. Share relevant, anonymized threat information or TTPs with trusted industry partners (e.g., ISACs) or peers where appropriate and approved by Legal/Management.
- **Final Legal/Compliance Closure:** Confirm all required regulatory notifications, legal actions, and internal compliance checks related to the Incident are fully completed and documented.

7. Incident Classification and Severity

Timely and accurate classification and severity assessment are crucial for prioritizing resources and triggering appropriate response protocols, including escalations.

7.1. Classification Categories (Examples)

Incidents are initially categorized based on the primary type of activity observed. Categories include, but are not limited to:

- **Unauthorized Access:** Includes account compromise (user, privileged, service), system intrusion, unauthorized elevation of privilege, successful access attempts bypassing controls.
- **Malicious Code:** Infection or execution of viruses, worms, Trojans, ransomware, spyware, rootkits, crypto-miners, potentially unwanted programs (PUPs).
- **Denial of Service (DoS/DDoS):** Attacks intended to overwhelm system resources or network bandwidth, rendering services unavailable to legitimate users. Includes volumetric, protocol, and application-layer attacks.
- **Improper Usage:** Violations of the organizational AUP [Ref: IT-AUP-001] by employees or authorized users, potentially creating security risks (e.g., unauthorized software installation, sharing credentials, misuse of resources).
- **Data Breach / Leakage / Exposure:** Confirmed or highly suspected unauthorized access to, acquisition, exfiltration, or public exposure of sensitive or regulated data (e.g., PII, PHI, financial data, intellectual property).
- **Scanning / Reconnaissance:** Probing networks or systems to identify vulnerabilities, open ports, or gather intelligence for a future attack (may be precursor activity).
- **Phishing / Social Engineering:** Attempts to deceive users into revealing sensitive information (credentials, financial details) or executing malicious code, via email, phone, messaging, or other means.
- **Loss / Theft of Equipment:** Unaccounted for or stolen laptops, mobile devices, storage media, or other hardware containing organizational data.
- **Web Application Attack:** Exploitation of vulnerabilities in web applications (e.g., SQL Injection, Cross-Site Scripting (XSS), Path Traversal, Remote Code Execution).

7.2. Severity Levels

Severity is assigned based on a holistic assessment of technical impact, business impact, data sensitivity, recovery effort, and potential legal/reputational consequences.

Severity Level Definitions

Level	Description	Example Indicators
4 - Low	Minimal operational impact, typically localized to a single user or non-critical system. No sensitive data exposure. Threat is easily contained and remediated using standard procedures with minimal effort. No significant business or reputational risk.	Single endpoint malware detection automatically quarantined by EDR; Minor violation of AUP with no compromise; Unsuccessful targeted phishing attempt; Brief interruption of a non-essential internal service.
3 - Medium	Moderate operational impact, potentially affecting a department, multiple users, or a non-critical business service. May involve limited exposure of non-sensitive company data. Requires coordinated IRT effort for Containment and Recovery. Potential for minor reputational damage if public-facing systems are involved.	Successful phishing leading to standard user account compromise requiring password reset and system scan; Malware outbreak contained to a single network segment; Temporary unavailability of a departmental application; Defacement of an informational website.
2 - High	Significant operational impact, disrupting critical business functions, affecting multiple critical systems or large user groups. High likelihood or confirmation of sensitive data exposure (PII, financial, IP). Recovery is complex, costly, and/or time-consuming. Poses substantial operational, financial, or reputational risk. Regulatory notifications likely required.	Confirmed ransomware encryption of critical servers or production databases; Confirmed data breach involving customer PII or regulated data; Sustained DDoS attack impacting primary revenue-generating services; Widespread compromise involving privileged credentials (e.g., Domain Admin).
1 - Critical	Severe, potentially catastrophic impact threatening organizational viability. Widespread disruption of essential business operations across multiple sites or functions. Confirmed major breach of highly sensitive data with significant legal/regulatory/reputational consequences. May pose a threat to physical safety or environmental stability. Requires immediate executive leadership involvement and potentially external crisis management support.	Large-scale ransomware event paralyzing core business operations; Major compromise of critical infrastructure (e.g., Active Directory forest, core network routers); Confirmed theft or public release of significant intellectual property or strategic plans; Attack attributed to sophisticated nation-state Threat Actor targeting critical systems.

Note: The Incident Commander holds the authority to adjust the severity level during the Incident lifecycle as more information becomes available and the impact is better understood.

8. Communication

Effective, accurate, and timely communication is paramount throughout the incident response lifecycle.

8.1. Internal Communication Protocols

- **IRT Coordination & Secure Channels:** Primary communication for active IRT members must occur over pre-defined, secure, and out-of-band channels (e.g., dedicated encrypted messaging platform, secure conference bridges) to avoid compromise via the affected network. The Incident Management System [Ref: INCIDENT-TRACKING-SYSTEM-URL] serves as the official log.
- **Stakeholder Communication Matrix:** A detailed matrix [Ref: IR-COMM-MATRIX-001] defines who needs to be informed, about what aspects of the Incident, at what frequency, through which channel, based on incident severity and type. This ensures consistent and appropriate updates to Management, Legal, PR, HR, Business Units, etc. Updates should focus on status, impact, actions taken, and expected timelines, avoiding excessive technical jargon for non-technical audiences.
- **Incident Command Post / War Room:** For High/Critical severity Incidents, a dedicated physical or virtual 'War Room' will be established to serve as the central hub for coordination, decision-making, and status tracking, facilitated by the Incident Commander.
- **Documentation Access:** Ensure all relevant IRT members and Stakeholders have appropriate access to the central incident documentation repository [Ref: INCIDENT-DOC-REPO-URL] for logs, reports, and evidence (access controlled based on role).

8.2. External Communication Protocols

- **Strict Approval Mandate:** Absolutely NO external communication regarding an active or potential security Incident shall be made without the explicit prior review and written approval of BOTH the Legal Department and the Corporate Communications/PR Department. This includes statements to media, customers, partners, regulators, law enforcement, or posts on social media. Unauthorized communication can have severe legal and reputational consequences.
- **Data Breach Notifications:** In the event of a confirmed data breach, particularly involving PII or other regulated data, notifications to affected individuals and regulatory authorities will be conducted strictly according to legal requirements and the established Data Breach Response Procedure [Ref: DATA-BREACH-PROC-001], managed by the Legal and Privacy teams.
- **Law Enforcement Interaction:** All interactions and information sharing with law enforcement agencies related to an Incident must be coordinated and managed through the Legal Department and designated Security Leadership liaisons.
- **Third-Party / Vendor Communication:** Communication with external partners, suppliers, or cloud providers potentially involved in or affected by the Incident will be managed centrally, typically by designated IRT members or relationship managers, with messaging approved by Legal/Comms as appropriate.

9. Policy Enforcement and Compliance

9.1. Enforcement

Adherence to this Incident Response Policy is mandatory for all individuals identified within its scope (Section 2). Violations of this policy, including but not limited to: failure to report a suspected Incident in a timely manner, unauthorized disclosure of incident information, interference with or obstruction of authorized response activities, or failure to cooperate with the IRT, will be subject to investigation and may result in disciplinary action, up to and including termination of employment or contract, in line with the procedures outlined in the Employee Code of Conduct [Ref: HR-POL-005] and applicable contractual agreements.

9.2. Compliance Assurance

All incident response activities must be executed in strict compliance with applicable international, federal, state, and local laws and regulations (e.g., GDPR, CCPA, HIPAA, PCI-DSS, SOX), relevant industry standards, contractual commitments, and other pertinent internal corporate policies (e.g., Data Privacy Policy [Ref: DP-POL-001], Data Classification Standard [Ref: DATA-CLASS-STD-001], AUP [Ref: IT-AUP-001]). The Legal Department, Privacy Office, and Internal Audit/Compliance teams provide guidance and oversight to ensure these obligations are met throughout the response process. Evidence handling must adhere to forensic best practices to maintain legal admissibility [Ref: FORENSIC-PROC-001].

10. Policy Review and Maintenance

- **Review Cadence & Approval:** This IRP will undergo a formal review, update (if necessary), and re-approval process coordinated by the [Specify Owner, e.g., Information Security Department] and approved by the [Specify Approving Body, e.g., Information Security Steering Committee or CISO] on at least an annual basis.
- **Triggered Updates:** Significant updates may also be triggered outside the annual cycle by factors such as: major lessons learned from post-incident reviews, significant changes in the organizational structure or technology landscape (e.g., major cloud migration), emergence of new significant threats or attack vectors, changes in regulatory requirements, or findings from IR exercises and tests.
- **Maintenance Responsibility:** The [Specify Owner] is responsible for ensuring the policy remains current, reflects best practices, aligns with organizational strategy, and is effectively communicated to all relevant personnel.
- **Version Control & Accessibility:** All revisions to this policy will be meticulously documented in the Revision History section (Section 11). The official, current version of this policy will be published and maintained on the [Specify Location, e.g., Centralized Corporate Policy Portal at URL] and made accessible to all personnel defined in the Audience section. Superseded versions will be archived according to the Document Retention Policy [Ref: DOC-RETENTION-POL-001].

11. Revision History

Version	Date	Summary of Changes	Approver/Editor
1.0	YYYY-MM-DD	Initial Policy Draft	[Name/Dept]
2.0	2025-04-08	Major revision: Added detailed roles, escalation path, corporate focus, UTPB color accents, enhanced definitions based on NIST SP 800-61 R2 alignment.	[Name/Dept]
2.1	2025-04-08	Corrected LaTeX errors (glossaries options/defs, & usage, textbf typo); Adjusted Roles table column width; Refined corporate language.	[AI Assisted]
2.2	2025-04-08	Final Review: Added author names; Enhanced detail in definitions & sections; Added `microtype` & `tcolorbox` for style; Added Playbook, Threat Actor, Zero Day, IoA definitions; Ensured consistency; Corrected page numbering and title page display.	[AI Assisted]
2.3	2025-04-08	Replaced Roles table `tabularx` with `longtable` to fix page break cutoff issue. Added `longtable` package. Emphasized glossary compilation steps.	[AI Assisted]
2.4	**2025-04-08**	**Thorough Review Pass: Refined Audience section detail; Corrected all identified placeholder formatting (`[Ref:..]`); Fixed `CCPA/HIPAA` typo; Removed `$` from `24/7`; Corrected minor punctuation/grammar; Added caption to Roles table; Re-emphasized glossary compilation steps.**	**[AI Assisted]**
2.5	**2025-04-08**	**Final Pass: Corrected remaining `&` vs `\&` errors in `\textbf`; Corrected escaped `$` in Revision History; Cleaned potential invisible space characters; Added detailed glossary compilation warning.**	**[AI Assisted]**

A. Appendix A: Glossary

Glossary

Asset Any tangible or intangible resource of value to the organization that requires protection. This includes, but is not limited to: data (PII, intellectual property, financial, customer, operational), information systems (servers, endpoints, networks, cloud infrastructure), applications, physical facilities, personnel, and corporate reputation.

Containment The phase involving actions to prevent an Incident from spreading further and causing additional damage. Effective Containment requires timely decision-making based on the nature of the threat and potential business impact of the containment actions themselves. Strategies are tailored to the environment (e.g., cloud vs. on-premise vs. OT).

Eradication The systematic process of identifying and eliminating the Root Cause and all remnants of the Incident (e.g., malware, attacker tools, persistence mechanisms, compromised accounts) from the affected environment. This phase often requires deep technical analysis and validation scanning.

Incident An adverse event, or the imminent threat thereof, that violates security policies, jeopardizes the Confidentiality, Integrity, or Availability (CIA) of organizational Assets, disrupts critical business operations, or results in unauthorized access, disclosure, modification, or destruction of information. This policy is invoked upon suspicion or confirmation of such an event.

Playbook A detailed, step-by-step checklist or procedure designed to guide the response to specific types of common or high-impact Incidents (e.g., Ransomware Playbook, Data Breach Playbook). Playbooks operationalize this IRP for specific scenarios.

Recovery The coordinated process of restoring systems, data, and services affected by an Incident to a fully functional, secure, and trusted operational state. This includes thorough validation, testing, and potentially phased rollouts before declaring full recovery.

Root Cause The fundamental underlying vulnerability, misconfiguration, process flaw, or condition that enabled an Incident to occur. Identifying the Root Cause through Root Cause Analysis (RCA) is paramount for effective Eradication and implementing long-term preventative measures.

Stakeholder Any individual, group, or entity, internal or external, with a vested interest in, or potential impact from, an Incident and the organization's response. Communication with Stakeholders must be carefully managed according to the Communication Plan (Section 8).

Threat Actor An individual, group, or entity responsible for actions that negatively impact the security of an organization's Assets. Actors can range from insiders and hacktivists to organized crime groups and nation-states, each with different motivations and capabilities.

Acronyms

AUP Acceptable Use Policy. The organizational policy defining permissible and prohibited uses of company IT Assets, network resources, and data. Referenced as [Ref: IT-AUP-001].

EDR Endpoint Detection and Response. Integrated endpoint security solutions combining real-time continuous monitoring, endpoint data collection, and automated response capabilities (e.g., host isolation, process termination). Key tool for detecting IoAs.

IoA Indicator of Attack. Evidence suggesting an attack is in progress, often focusing on attacker behaviors and TTPs rather than specific artifacts like IoCs. Examples include unusual PowerShell commands, lateral movement patterns, or credential dumping attempts. Detected primarily by EDR and behavioral analysis tools.

IoC Indicator of Compromise. Forensic artifact or evidence indicating, with high confidence, that a system or network intrusion has occurred. Examples include specific malware file hashes, C2 server IP addresses, or unique registry keys. Often used by SIEM and EDR tools.

IRT Incident Response Team. The designated group of individuals responsible for implementing the Incident Response Plan. Comprises Core members (e.g., SOC) and Extended members (SMEs, Legal, HR, etc.) activated based on incident needs.

MTTD Mean Time To Detect. An average measure of the time elapsed between the occurrence of an Incident and its discovery by the security team. A key performance indicator (KPI) for detection capabilities.

MTTR Mean Time To Respond/Resolve/Recover. A collective term for metrics measuring the average time taken to contain ($MTTC$), eradicate ($MTTE$), or fully recover ($MTTR$) from an Incident after detection. Specific definitions may vary.

PII Personally Identifiable Information. Any information relating to an identified or identifiable natural person, as defined by applicable regulations (e.g., GDPR, CCPA) and internal Data Privacy Policy [Ref: DP-POL-001]. Incidents involving potential PII exposure trigger specific legal and notification requirements.

SIEM Security Information and Event Management. Technology platform providing real-time analysis of security alerts generated by network hardware and applications. Centralizes log collection and correlation to support threat detection and compliance.

SOAR Security Orchestration, Automation, and Response. Technologies integrating various security tools and automating incident response workflows (e.g., enriching alerts, executing containment actions via Playbooks), aiming to improve response speed and efficiency.

SOC Security Operations Center. The dedicated facility and team responsible for continuous monitoring, detection, analysis, and response to cybersecurity threats and Incidents.