

# Incident Response Plan (IRP)

## Section 1: Policy Statement, Purpose, Scope, and Objectives

- **1.1 Policy Statement:** World Bank is committed to maintaining a robust and agile incident response capability to effectively prepare for, detect, analyze, contain, eradicate, and recover from cybersecurity incidents. This Incident Response Plan (IRP) provides the framework and procedures to ensure a coordinated and timely response to minimize operational, financial, reputational, and regulatory impacts resulting from such incidents.
- **1.2 Purpose:** The purpose of this IRP is to:
  - Provide a structured and documented approach for managing and responding to cybersecurity incidents affecting World Bank's information assets, systems, and services.
  - Ensure prompt and effective containment of incidents to limit their scope and severity.
  - Facilitate the efficient eradication of threats and the secure recovery of affected systems and services.
  - Minimize disruption to business operations and ensure the continuity of critical banking services.
  - Protect sensitive customer and bank data from unauthorized disclosure, modification, or destruction.
  - Meet legal, regulatory (e.g., FFIEC, FDIC, SOX, GDPR, SWIFT CSP), and contractual obligations for incident reporting and management.
  - Enable post-incident analysis to identify lessons learned and implement improvements to security controls and response capabilities.
- **1.3 Scope:**
  - This IRP applies to all cybersecurity incidents involving World Bank's information assets, including but not limited to data, systems, networks, applications, and facilities, whether on-premise or cloud-based.
  - This plan is applicable to all World Bank employees, contractors, consultants, and third-party vendors who have access to World Bank information assets or are involved in the incident response process.
  - Specific incident types covered by this plan and its associated playbooks include (but are not limited to): malware infections (including ransomware),

denial-of-service attacks, unauthorized access, data breaches, phishing and social engineering attacks, insider threats, and critical system outages due to cyber events.

- **1.4 Objectives of Incident Response:** The primary objectives during an incident response are to:
  - **Verify and Assess:** Quickly confirm if an incident has occurred and assess its nature, scope, and potential impact.
  - **Contain:** Limit the spread and impact of the incident, preventing further damage or unauthorized access.
  - **Eradicate:** Remove the root cause of the incident and any malicious artifacts from the environment.
  - **Recover:** Securely restore affected systems and services to normal operations within defined RTOs.
  - **Communicate:** Provide timely and accurate information to relevant internal and external stakeholders.
  - **Learn:** Conduct post-incident analysis to identify lessons learned and improve future preparedness and response.
  - The financial services sector is a prime target for cyberattacks. Therefore, this IRP is not a static document but a dynamic framework that must be continuously tested, refined, and adapted to the evolving threat landscape and the Bank's specific risk profile. The ability to respond swiftly and effectively can significantly reduce financial losses, maintain customer trust, and ensure regulatory compliance.

## Section 2: Incident Response Team (IRT) / Computer Security Incident Response Team (CSIRT)

- **2.1 IRT/CSIRT Mission and Authority:**
  - The World Bank Incident Response Team (IRT), also referred to as the Computer Security Incident Response Team (CSIRT), is formally chartered with the authority to take necessary actions to investigate, contain, eradicate, and recover from cybersecurity incidents.
  - The IRT operates under the direction of the Security Manager (or a designated Incident Commander during a major incident).
- **2.2 IRT/CSIRT Structure and Composition:** The World Bank IRT is a cross-functional team comprising core members and an extended team that can be activated based on the nature and severity of the incident.

- **Core IRT Members:**

- **Incident Response Manager/Commander (Typically Security Manager or delegate):** Overall coordination, decision-making, liaison with executive management.
- **Technical Lead/Security Analysts:** Technical investigation, forensic analysis, containment, and eradication efforts.
- **IT Operations Lead:** Coordinates restoration of systems, network connectivity, and infrastructure.
- **Network Security Engineer(s):** Firewall management, network traffic analysis, IDS/IPS operations.
- **System Administrator(s) (Server, Database, Application):** System-specific expertise, log analysis, system recovery.
- **Communications Coordinator:** Manages internal and external communications as per the Communication Plan.

- **Extended IRT Members (Activated as needed):**

- **Legal Counsel:** Advises on legal implications, regulatory reporting, evidence handling, and liaises with law enforcement.
- **Human Resources:** Involved in incidents related to employee misconduct or insider threats.
- **Public Relations/Corporate Communications:** Manages media inquiries and public statements.
- **Business Unit Representatives:** Provide impact assessment from a business perspective and assist with business process recovery.
- **Compliance Officer:** Ensures adherence to regulatory reporting requirements.
- **Physical Security:** Involved if the incident has a physical component or requires facility access control.
- **Third-Party Vendor Liaisons:** Coordinate with relevant service providers if their systems are involved or required for recovery.

- A clear definition of roles and responsibilities, along with pre-assigned backups for key roles, is crucial to avoid confusion and delays during a high-stress incident. Regular joint training and tabletop exercises are essential to ensure all team members understand their roles and can work cohesively.

- **2.3 Contact Information:**

- A maintained and regularly updated contact list (including out-of-band communication methods) for all IRT members, key stakeholders, and external entities (e.g., FS-ISAC, law enforcement, regulators, cyber insurance provider) is documented in Appendix B (Contact Directory – *Not detailed in this simulation output, but would be present*).

## Section 3: Incident Response Lifecycle (Based on NIST SP 800-61 and SANS )

### • 3.1 Preparation:

- **Policies and Procedures:** This IRP and associated playbooks are established, reviewed annually, and updated as needed.
- **Tools and Resources:** Necessary hardware, software (e.g., forensic tools, SIEM, EDR, PAM), and secure communication channels are identified, procured, and maintained.
- **Training and Awareness:** Regular training for IRT members on incident handling procedures, tools, and current threats. General cybersecurity awareness training for all employees on identifying and reporting potential incidents.
- **Asset Inventory and Network Diagrams:** Maintaining an accurate inventory of critical assets and up-to-date network diagrams to aid in incident scoping and containment.
- **Risk Assessments:** Regular risk assessments to identify potential threats and vulnerabilities that could lead to incidents.
- **Establishing Baselines:** Understanding normal system and network behavior to better detect anomalies.

### • 3.2 Identification (Detection and Analysis):

- **Incident Detection Sources:**
  - Alerts from SIEM, IDS/IPS, EDR, antivirus, firewalls, DLP, PAM systems.
  - Reports from employees, customers, or external parties (e.g., law enforcement, FS-ISAC ).
  - Anomalous activity detected through log reviews or UEBA.
  - Notifications from third-party service providers about incidents affecting World Bank.
- **Incident Validation and Initial Assessment:**
  - Verify the authenticity of reported incidents and filter out false positives.

- Conduct an initial assessment to understand the nature of the incident (e.g., malware, unauthorized access, DDoS).
    - Determine the initial scope and potential impact.
  - **Incident Classification and Prioritization:**
    - Incidents will be classified based on their type (e.g., data breach, system outage, malware infection) and severity (e.g., High, Medium, Low) using a defined Incident Classification and Prioritization Matrix (see Section 4).
    - Prioritization determines the urgency and level of response.
  - **Documentation:** All identified incidents, assessments, and actions taken will be logged in an incident tracking system from the point of detection.
- **3.3 Containment:**
    - **Strategy:** The primary goal is to limit the spread of the incident and prevent further damage or unauthorized access while preserving evidence. Containment strategies will depend on the incident type and severity.
    - **Short-term Containment:**
      - Isolating affected systems from the network (e.g., disconnecting network cables, VLAN segmentation, firewall ACLs).
      - Disabling compromised user or service accounts.
      - Blocking malicious IP addresses or domains at the firewall or proxy.
      - Redirecting network traffic (e.g., during a DDoS attack).
    - **Long-term Containment:**
      - Applying temporary fixes or workarounds to prevent immediate re-exploitation.
      - Enhanced monitoring of affected systems and network segments.
    - **Evidence Preservation:** During containment, all actions must be taken with consideration for preserving forensic evidence (see Section 6).
  - **3.4 Eradication:**
    - **Root Cause Analysis:** Identify the underlying cause of the incident (e.g., exploited vulnerability, compromised credential, misconfiguration).
    - **Removal of Malicious Artifacts:**

- Removing malware, backdoors, and other malicious tools from affected systems.
  - Deleting unauthorized user accounts or access mechanisms.
- **Vulnerability Remediation:**
  - Applying patches to exploited vulnerabilities.
  - Correcting misconfigurations that contributed to the incident.
  - Strengthening security controls (e.g., updating firewall rules, enhancing access controls).
- Systems may need to be rebuilt from trusted backups or clean installations if heavily compromised.
- **3.5 Recovery:**
  - **Restoration of Systems and Data:**
    - Restoring affected systems and data from clean, verified backups according to RTOs defined in the BDR Policy.
    - Validating the integrity and functionality of restored systems before bringing them back into production.
  - **Security Validation:**
    - Confirming that vulnerabilities have been addressed and systems are secure.
    - Performing vulnerability scans or penetration tests on recovered systems if deemed necessary.
  - **Monitoring:** Implementing enhanced monitoring on recovered systems to detect any residual threats or recurrence of the incident.
  - **Gradual Resumption of Services:** Phased rollout of services to ensure stability.
- **3.6 Post-Incident Activity (Lessons Learned):**
  - **Incident Review Meeting:** Conduct a formal review within two weeks of incident closure (or sooner for critical incidents) involving all relevant IRT members and stakeholders.
  - **Analysis:**
    - What happened, when, and why?
    - How well did staff and management perform during the incident?

- Were documented procedures followed? Were they adequate?
  - What information was needed sooner?
  - What corrective actions can prevent similar incidents in the future?
  - What could be done to improve incident detection and response tools or resources?
- **Documentation:** Update the incident log with all findings, lessons learned, and recommended actions.
  - **Action Plan:** Develop an action plan to implement recommendations for improving policies, procedures, controls, and training. Track action items to completion.
  - **Reporting:** Provide a final incident report to Senior Management and, if required, to regulatory bodies or other external parties.
  - The entire incident response lifecycle emphasizes a feedback loop. Lessons learned from one incident directly inform the preparation phase for future events, fostering a culture of continuous improvement and resilience. This iterative process is vital as threat actors constantly evolve their TTPs.

## Section 4: Incident Classification and Prioritization Matrix

- Incidents will be classified based on their functional impact, information impact, and recoverability effort. This matrix guides the level of response, resources allocated, and communication urgency.

**TABLE: World Bank Incident Severity and Priority Matrix (Illustrative)**

Impact Category	Severity Level	Criteria Example (Financial Services Context)	Initial Response Time SLA	Priority
Functional Impact	High (Critical)	Core Banking System outage; widespread inability to process transactions; Online/Mobile banking unavailable to all customers.	< 15 minutes	P1
	Medium (Major)	Degradation of a key service (e.g., slow online banking); outage of a non-critical but important system (e.g., internal reporting system).	< 1 hour	P2
	Low (Minor)	Localized issue affecting a small number of users/systems; minor feature malfunction with workaround available.	< 4 hours	P3
Information Impact	High (Critical)	Confirmed breach of sensitive customer PII/financial data (e.g., account numbers, SSNs); compromise of critical system credentials.	< 15 minutes	P1
	Medium (Major)	Suspected but unconfirmed breach of sensitive data; compromise of non-critical system credentials; unauthorized access to internal confidential data.	< 1 hour	P2

	Low (Minor)	Malware infection on isolated endpoint with no data loss; minor policy violation.	< 4 hours	P3
<b>Recoverability</b>	High (Difficult)	Complex recovery requiring extensive rebuild, external expertise, or significant downtime expected (e.g., major ransomware).	N/A (Impact drives P)	Adjusts P
	Medium (Moderate)	Recovery possible from backups but may take several hours; some data reconstruction needed.	N/A (Impact drives P)	Adjusts P
	Low (Easy)	Quick recovery from readily available backups or simple remediation steps.	N/A (Impact drives P)	Adjusts P

\* **\*Note:\*** The final Priority (P1, P2, P3, P4) is determined by the highest severity level across Functional and Information Impact, potentially adjusted by Recoverability. P1 incidents require immediate, all-hands response.

\* **\*This matrix provides a standardized framework for assessing incidents, ensuring that response efforts are commensurate with the actual or potential harm. For a bank, a P1 incident involving a Core Banking System outage or a major data breach demands an immediate and comprehensive response involving senior management and potentially external regulators.\***

## Section 5: Communication Plan

- **5.1 Internal Communication:**

- **IRT Communication:** Predefined secure communication channels for the IRT (e.g., dedicated encrypted chat, conference bridges, out-of-band email if primary is affected).
- **Management Updates:** Regular, concise updates to Senior Management and key stakeholders on incident status, impact, and actions taken. Frequency determined by incident severity.
- **Employee Notifications:** Communication to general employees regarding incidents that may affect them or require specific actions (e.g., password resets, phishing awareness alerts).
- A communication matrix detailing who communicates what to whom, and when, is maintained in Appendix C (Communication Matrix – *Not detailed here*).

- **5.2 External Communication:**

- **Customers:** If customer data or services are impacted, timely, clear, and accurate communication will be provided through approved channels (e.g., website banners, secure messages, email, call center scripts). Content must be approved by Legal and Corporate Communications.



- **Regulatory Bodies:** Incidents meeting defined thresholds (e.g., FFIEC notification incidents ) will be reported to the relevant regulatory agencies (FDIC, OCC, Federal Reserve, State Regulators) within the mandated timeframes (e.g., 36 hours for certain computer-security incidents).
- **Law Enforcement:** Incidents involving criminal activity will be reported to appropriate law enforcement agencies (e.g., FBI, Secret Service).
- **FS-ISAC and other Information Sharing Groups:** Relevant non-confidential threat information and IoCs may be shared with FS-ISAC and other trusted industry groups to help protect the broader financial sector.
- **Third-Party Vendors:** Communication with affected or involved vendors.
- **Media:** All media inquiries will be handled by Corporate Communications/Public Relations in coordination with Legal and Senior Management. Pre-drafted statement templates for common scenarios are maintained.

## Section 6: Evidence Handling and Forensics

- **6.1 Evidence Collection and Preservation:**

- Procedures for collecting and preserving digital evidence must maintain its integrity and admissibility for internal investigations and potential legal or disciplinary actions.
- This includes creating forensic images of affected systems, collecting volatile data (memory, network connections), preserving log files, and documenting all actions taken.
- Chain of custody will be maintained for all collected evidence.

- **6.2 Forensic Analysis:**

- Forensic analysis will be conducted by trained internal personnel or qualified third-party forensic specialists to determine the incident's root cause, scope, attack vectors, and extent of compromise.
- Findings from forensic analysis will feed into the eradication, recovery, and lessons learned phases.

## Section 7: Plan Testing, Training, and Maintenance

- **7.1 Testing:**

- The IRP and associated playbooks will be tested at least annually through various methods, including tabletop exercises, functional drills, and full-scale simulations.

- Tests will cover a range of incident scenarios relevant to World Bank.
- Test results will be documented, and any identified gaps or weaknesses will be addressed through plan updates and corrective actions.
- **7.2 Training:**
  - All IRT members will receive regular, specialized training on incident response techniques, tools, and procedures.
  - All employees will receive annual security awareness training that includes how to identify and report potential incidents.
- **7.3 Maintenance:**
  - This IRP will be reviewed and updated at least annually, or as needed based on test results, lessons learned from actual incidents, changes in the threat landscape, new technologies, or modifications to World Bank's business operations or regulatory environment.
  - Contact lists, tool inventories, and procedural documentation will be kept current.

## Section 8: Policy Review and Exceptions

- **8.1 Review Cycle:** This Incident Response Plan will be reviewed and formally approved by Senior Management and the Board of Directors at least annually.
  - **8.2 Exception Process:** Any exceptions to this IRP must be documented, justified with a risk assessment, and approved by the Security Manager and relevant executive leadership.
- 

## Appendix A: Incident Response Plan Simulation

### Items/Scenarios for World Bank

1. **Incident Declaration:** Based on SIEM alerts for widespread anomalous logins to the Online Banking Platform, the SOC Lead declares a P1 incident.
  - **Action:** Initiate the IRP and assemble the core IRT.
2. **Ransomware Attack Playbook Activation:** Evidence suggests a ransomware variant is encrypting files on multiple critical servers, including a database server for the Loan Origination System.
  - **Action:** Execute the "Ransomware Attack Response Playbook" (see Appendix D – *Not detailed here*). Key steps: Isolate affected servers, identify ransomware strain, assess backup integrity, decide on restoration vs. other options.

3. **DDoS Attack on Online Services:** Online Banking and Mobile Banking platforms are experiencing a significant degradation of service due to a volumetric DDoS attack.
  - **Action:** Execute the "DDoS Attack Mitigation Playbook" (see Appendix E – *Not detailed here*). Key steps: Engage DDoS mitigation service provider, analyze attack traffic, implement traffic scrubbing/blackholing.
4. **Phishing Campaign Leading to Credential Compromise:** Multiple employees report falling victim to a targeted phishing campaign. AD logs show suspicious logins using potentially compromised credentials.
  - **Action:** Execute the "Phishing Incident Response Playbook" (see Appendix F – *Not detailed here*). Key steps: Identify all affected users, force password resets, scan endpoints for malware, block malicious URLs/senders.
5. **Data Breach Notification Simulation (Internal):** Forensic investigation confirms that a database containing non-critical customer marketing preferences (no financial data) was accessed by an unauthorized external IP.
  - **Action:** IRT Lead, Communications Coordinator, and Legal Counsel to draft an internal notification to relevant department heads.
6. **Regulatory Reporting Decision:** A significant computer-security incident (e.g., Core Banking System encrypted by ransomware) has occurred, materially disrupting operations for over 4 hours.
  - **Action:** Incident Commander, Legal, and Compliance Officer to determine if the incident meets FFIEC criteria for a "notification incident" and prepare notification to primary federal regulator within 36 hours.
7. **Containment Strategy Decision:** Malware is spreading rapidly across a network segment containing teller workstations.
  - **Action:** Technical Lead to decide between network segmentation of the affected VLAN or shutting down all workstations in that segment. Document justification.
8. **Evidence Collection:** An insider threat is suspected of unauthorized data modification in the CRM.
  - **Action:** Forensic analyst to create a forensic image of the suspect's workstation and collect relevant server logs, maintaining chain of custody.
9. **Eradication Verification:** After cleaning malware from several servers, IT Operations believes the threat is eradicated.
  - **Action:** Security Analyst to perform secondary scans and review logs to confirm eradication before systems are approved for recovery.

10. **Recovery Prioritization:** Multiple systems are down after a major incident.
- **Action:** Incident Commander, using the BIA and RTOs, prioritizes the recovery sequence (e.g., Core Banking System first, then Payment Gateways, then Online Banking).
11. **Post-Incident Review (Tabletop):** Conduct a lessons learned session after a simulated phishing attack exercise.
- **Action:** Identify three areas for improvement in user training or technical controls. Assign action items.
12. **Communication with FS-ISAC:** Non-sensitive IoCs (malicious IPs, file hashes) from a confirmed malware campaign are identified.
- **Action:** Designated IRT member to prepare and (simulate) share this information with FS-ISAC.
13. **SWIFT CSP Incident Reporting:** A security incident impacts the local SWIFT infrastructure.
- **Action:** Follow SWIFT CSP guidelines for incident response and (simulate) reporting to SWIFT.
14. **Escalation to Extended IRT:** A P2 incident (e.g., website defacement) is identified. The core IRT manages it, but media inquiries begin.
- **Action:** Incident Commander to escalate and activate Public Relations from the extended IRT.
15. **Third-Party Incident Coordination:** A critical cloud service provider reports a security incident impacting World Bank data.
- **Action:** Vendor Liaison to establish communication with the provider, gather impact details, and coordinate World Bank's response based on the provider's actions.
16. **Incident Log Review:** During an ongoing incident, the Recorder provides an update on all actions taken, decisions made, and timelines.
- **Action:** Incident Commander reviews for completeness and accuracy.
17. **Testing Out-of-Band Communication:** Primary email system is "down" as part of a simulated attack.
- **Action:** IRT members to switch to the designated secure chat platform or conference bridge for communication.
18. **Impact Assessment Update:** Initial assessment of a malware incident was "Medium." New evidence shows it has spread to a critical database.

- **Action:** Technical Lead to re-classify the incident impact to "High" and adjust response priority.

19. **Legal Hold Notification:** A data breach involving customer PII is confirmed.

- **Action:** Legal Counsel to issue a legal hold notice for all relevant data, logs, and communications.

20. **Decision Not to Pay Ransom:** Following a ransomware attack where viable backups are confirmed to be available and restorable within RTO.

- **Action:** Incident Commander, with executive approval, makes the formal decision not to pay the ransom and proceeds with recovery from backups.