**Cyber Intrusion Remediation Document**

**Document ID:** [Unique Identifier, e.g., INC-YYYY-MM-DD-001]  
**Date Created:** [Insert Date]  
**Prepared By:** [Your Name/Team Name]  
**Incident Date:** [Date of Intrusion]  
**Last Updated:** [Date of Last Update]

**1. Incident Overview**

**Purpose:** Summarize the intrusion for context.  
**Details:**

* **Incident Type:** [e.g., Malware, Phishing, Unauthorized Access]
* **Date/Time Detected:** [Insert Date/Time]
* **Affected Systems/Assets:** [e.g., Servers, Endpoints, Applications]
* **Impact Summary:** [e.g., Data Breach, Service Disruption]
* **Initial Detection Method:** [e.g., IDS Alert, User Report]

**2. Intrusion Specifics**

**Purpose:** Provide detailed information about the intrusion to inform remediation.  
**Details:**

* **Attack Vector:** [e.g., Exploited Vulnerability, Stolen Credentials]
* **Indicators of Compromise (IoCs):** [e.g., Malicious IPs, Hashes, File Names]
* **Scope of Compromise:** [e.g., Number of Affected Devices, Data Accessed]
* **Root Cause (if known):** [e.g., Unpatched Software, Misconfiguration]
* **Threat Actor (if identified):** [e.g., Known Group, Unknown]
* **Evidence Collected:** [e.g., Logs, Memory Dumps, Network Captures]

**3. Remediation Plan**

**Purpose:** Outline specific actions to contain, eradicate, and recover from the intrusion based on its specifics.

**3.1 Containment Actions**

* Short-Term Containment: [e.g., Isolate affected systems, Block malicious IPs]
* Long-Term Containment: [e.g., Deploy network segmentation, Restrict user access]

**3.2 Eradication Actions**

* Remove Malicious Artifacts: [e.g., Delete malware, Reimage compromised systems]
* Patch Vulnerabilities: [e.g., Apply software updates, Fix configurations]
* Credential Reset: [e.g., Reset compromised accounts, Enforce MFA]

**3.3 Recovery Actions**

* Restore Systems/Services: [e.g., Rebuild servers, Restore from backups]
* Validate Integrity: [e.g., Verify no residual threats, Test functionality]
* User Communication: [e.g., Notify affected users, Provide guidance]

**3.4 Preventive Measures**

* Based on Intrusion Specifics: [e.g., If phishing, enhance email filters; If unpatched software, automate patch management]
* General Hardening: [e.g., Update firewall rules, Conduct security training]
* Monitoring Enhancements: [e.g., Add new IoCs to SIEM, Increase log retention]

**Notes:**

* Tailor this section to the intrusion’s root cause and attack vector. For example, a ransomware incident may prioritize backup restoration, while a credential theft incident may focus on MFA enforcement.
* Include timelines or priorities for each action where applicable.

**4. Post-Incident Actions**

**Purpose:** Ensure lessons learned and compliance.  
**Details:**

* **Incident Review Date:** [Schedule Date]
* **Lessons Learned:** [e.g., Identified gaps in monitoring, Training needs]
* **Policy Updates:** [e.g., Revise incident response plan, Update access controls]
* **Reporting Requirements:** [e.g., Notify regulators, Inform stakeholders]
* **Documentation Status:** [e.g., Final report archived, Evidence preserved]

**5. Stakeholders**

**Purpose:** Identify key contacts for accountability.

| **Role** | **Details** |
| --- | --- |
| Incident Lead | [Name, Role, Contact] |
| IT/Security Team | [Name(s), Role(s)] |
| External Partners | [e.g., Forensics Firm, Law Enforcement] |
| Approver | [Name, Role] |

**6. Appendices**

* **Logs/Reports:** [Reference attached evidence or logs]
* **Timeline of Events:** [Detailed chronology of incident and response]
* **Additional Notes:** [Any other relevant information]