Computer Security Incident Response Plan (CSIRP) Template

1. Introduction & Purpose

The purpose of this Computer Security Incident Response Plan (CSIRP) is to have a standardized approach for identifying, responding to, and recovering from security incidents. This plan follows NIST 800-61 guidelines and that incidents are handled efficiently to minimize risk and impact.

2. Scope

This plan applies to all security incidents involving the organization's IT infrastructure, applications, and data. It covers cyber threats such as malware infections, unauthorized access, denial-of-service attacks, insider threats, and data breaches.

3. Incident Response Phases

3.1 Preparation

- Establish an incident response team (IRT).
- Define roles and responsibilities.
- Conduct security awareness training.
- Implement monitoring tools and log management.
- Develop and test incident response playbooks.
- Maintain an inventory of critical assets and their associated risks.

3.2 Detection & Analysis

- Identify security events using intrusion detection systems (IDS), security information and event management (SIEM), and endpoint detection response (EDR) tools.

- Categorize incidents based on severity and impact.
- Perform initial triage and analysis.
- Analyze logs from firewalls, IDS, and antivirus software to confirm incidents.
- Distinguish between false positives and confirmed security incidents.

3.3 Containment, Eradication & Recovery

- Short-term containment (e.g., isolating affected systems).
- Long-term containment (e.g., applying patches, reconfiguring firewalls).
- Eradication (e.g., removing malware, closing vulnerabilities).
- Recovery (e.g., restoring data from backups, monitoring for reoccurrence).
- Define expected recovery times based on incident severity.
- Document lessons learned and update response strategies accordingly.

3.4 Post-Incident Activity

- Conduct a post-mortem review.
- Update security controls and policies.
- Maintain an incident knowledge base.
- Implement security improvements based on lessons learned.
- Schedule follow-up reviews to ensure no lingering security gaps.

4. Escalation Procedures

Severity Level	Description	Escalation Contact
Critical	Ransomware attack leading to data encryption and system-wide lockout	Incident Response Team (IRT) Lead
High	Unauthorized root access detected on a critical server	Security Operations Center (SOC)
Medium	Unusual outbound traffic from an employee's workstation	IT Security Analyst

Low	Phishing email reported with no successful credential compromise	Help Desk

5. Communication & Reporting

- **Internal Reporting:** All incidents must be reported to the SOC within 30 minutes of detection.
- **External Reporting:** Notify regulatory bodies, customers, and law enforcement as required.
- **Documentation:** Maintain an incident log detailing response actions and lessons learned.
- **Incident Response Timelines:**
    - *Critical incidents:* Acknowledged within 15 minutes, containment in 1 hour, full remediation within 24 hours.
    - *High-severity incidents:* Containment in 4 hours, full remediation within 48 hours.
    - *Medium-severity incidents:* Containment in 1 business day, remediation in 3 days.
    - *Low-severity incidents:* Reviewed within 2 business days.

6. RACI Matrix

Task	Responsible	Accountable	Consulted	Informed
Identify & categorize incident	SOC Analyst	SOC Manager	IT Security	Executive Team
Containment strategy execution	IRT	SOC Manager	IT Infrastructure	Affected Teams
Communication & escalation	Incident Coordinator	CISO	Legal, PR	Employees
Post-incident review	Security Team	CISO	IT, Compliance	Executive Team

Approving external communication	CISO	Executive Team	Legal, PR	Employees
Conducting forensic analysis	Incident Response Team	SOC Manager	IT Security	Executive Team

7. Appendix

- **Incident Report Template**
  - Standardized form to document incident details, response actions, and resolution status.
  - Includes sections for date/time of detection, affected systems, impact assessment, and final resolution.
- **Checklist for Incident Triage**
  - Step-by-step guide for assessing and categorizing incidents.
  - Ensures uniform handling and prioritization of threats.
- **Escalation Contact List**
  - Up-to-date contact details for all relevant SOC, IT, and executive personnel.
  - Emergency response numbers and escalation procedures.
- **Forensic Analysis Guide**
  - Procedures for gathering and analyzing digital evidence.
  - Guidelines for maintaining chain-of-custody and ensuring data integrity.
- **Incident Response Playbooks**
  - Predefined response actions for common attack scenarios such as ransomware, phishing, and insider threats.
  - Step-by-step containment and mitigation strategies.
- **Regulatory Compliance References**
  - Overview of relevant compliance requirements (e.g., GDPR, HIPAA, NIST) for incident handling.
  - Ensures alignment with legal and industry standards.