**Cyber Incident Response Plan (CIRP)**
**Prepared by Phenicie Business Management**
**For: [Client Name]**

**1. Purpose and Scope**

This plan establishes a structured framework for identifying, managing, mitigating, and recovering from cybersecurity incidents. It ensures business continuity, safeguards sensitive data, and maintains regulatory compliance.

**2. Incident Response Team (IRT)**

**Roles and Responsibilities:**

* **Incident Response Coordinator:** [Name/Contact] – Leads response efforts and stakeholder communication.
* **IT Security Lead:** [Name/Contact] – Manages technical response, containment, and forensic analysis.
* **Legal & Compliance Officer:** [Name/Contact] – Ensures adherence to legal and regulatory requirements.
* **Communications Lead:** [Name/Contact] – Handles internal and external communication.
* **Business Continuity Manager:** [Name/Contact] – Minimizes operational disruptions.

**3. Incident Classification and Severity Levels**

Cyber incidents are categorized to determine appropriate response actions:

* **Level 1 – Low Impact:** Minor disruptions, no data breach.
* **Level 2 – Medium Impact:** Unauthorized access, malware, service disruptions.
* **Level 3 – High Impact:** Ransomware, data breaches, critical system compromise.
* **Level 4 – Critical Impact:** Large-scale attacks affecting business continuity and sensitive data.

**4. Incident Response Phases**

**Phase 1: Preparation**

* Implement cybersecurity policies and best practices.
* Train employees on threat recognition (phishing, ransomware, etc.).
* Deploy endpoint detection and response (EDR) tools.
* Conduct regular backups and penetration testing.

**Phase 2: Identification**

* Detect threats using monitoring tools, logs, and user reports.
* Confirm incident scope, impact, and attack vector.
* Classify severity and document findings.

**Phase 3: Containment**

* **Short-Term:** Isolate affected systems to prevent spread.
* **Long-Term:** Block malicious IPs, segment networks.
* Preserve forensic evidence for investigation.

**Phase 4: Eradication**

* Remove malware and unauthorized access.
* Patch vulnerabilities and apply security updates.
* Conduct forensic analysis to identify root causes.

**Phase 5: Recovery**

* Restore systems from clean backups.
* Monitor for lingering threats or anomalies.
* Validate security measures before resuming operations.

**Phase 6: Lessons Learned**

* Conduct a post-incident review to assess response effectiveness.
* Update policies and procedures based on findings.
* Enhance employee training and threat awareness.

**5. Communication Plan**

* **Internal Reporting:** Employees report incidents to [IRT Contact].
* **Client Notification:** Notify affected clients within [X] hours of discovery.
* **Regulatory Compliance:** Report breaches per applicable regulations (e.g., GDPR, CCPA, HIPAA).
* **Public Relations:** Designate a spokesperson for media inquiries.

**6. Incident Documentation and Reporting**

* Maintain detailed logs of incidents, actions taken, and remediation steps.
* Submit an incident report to management within [X] hours post-recovery.
* Securely store reports for audit and compliance purposes.

**7. Testing and Maintenance**

* Conduct annual tabletop exercises and penetration tests.
* Update the CIRP regularly to address evolving threats.
* Ensure all employees and stakeholders understand their roles.

**8. Contact Information**

**Phenicie Business Management IT Security Team**

* **Email:** support@phenicie.com
* **Phone:** 406-382-9207
* **Website:** [www.phenicie.com](http://www.phenicie.com)

**Approval and Acknowledgment**

By signing below, the organization agrees to implement and adhere to this Cyber Incident Response Plan.

**Authorized Representative:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
**Title:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This document, provided by Phenicie Business Management, serves as a guideline to enhance cybersecurity resilience. Custom modifications may be necessary to align with industry-specific regulations and organizational needs.