CyberSecure Inc. Incident Response & Risk Management Plan

1. Introduction

1.1 Purpose of the Plan

The Incident Response Plan (IRP) is a structured framework designed to help CyberSecure Inc. effectively

1.2 Scope

This plan applies to all CyberSecure Inc. departments and employees, covering incidents that affect:

- Cloud and on-premise IT infrastructure
- Customer and employee data
- Sensitive intellectual property
- Third-party service providers

1.3 Plan Ownership and Maintenance

The Chief Information Security Officer (CISO) oversees and maintains this plan. The IRP is updated:

- Every six months
- After any major security incident
- To align with evolving threats and compliance requirements

1.4 Definitions

- Incident: An event that threatens data confidentiality, integrity, or availability.
- Threat Actor: An individual or group attempting unauthorized access or disruption.
- Risk Mitigation: Proactive strategies to reduce exposure to cyber threats.

2. Roles and Responsibilities

2.1 Incident Response Team (IRT)

Role | Responsibilities

------|----------

CISO | Oversees the IRP, ensures regulatory compliance.

Incident Response Lead | Directs response efforts and coordinates teams.

IT Security Team | Investigates, contains, and mitigates security incidents.

Legal & Compliance | Evaluates legal obligations and ensures compliance.

PR & Communications | Manages external and internal messaging.

2.2 External Support

CyberSecure Inc. engages with:

- Law enforcement agencies for criminal investigations.
- Cybersecurity consultants for forensic analysis.
- Regulatory bodies when necessary.

3. Incident Identification

3.1 Identifying Potential Incidents

Security incidents may be identified through:

- Intrusion Detection Systems (IDS) alerts
- Unusual network traffic monitoring
- Employee reports of suspicious activity
- Failed login attempts and account lockouts

3.2 Reporting Process

Employees must report potential incidents within 24 hours via:

- Internal security reporting tool
- Email alerts to IT Security Team
- Incident hotline for critical breaches

3.3 Initial Assessment

- Analyze severity based on affected systems and data.
- Determine if external parties need to be notified.
- Assign classification level (see Section 4).

4. Incident Classification

4.1 Classification Criteria

Incidents are classified based on:

- Impact on business operations
- Confidentiality of compromised data
- Potential financial loss or legal consequences

4.2 Classification Levels

Level | Impact | Response Action

------|--------|----------------

Low | Minimal security breach | Internal mitigation & documentation.

Medium | Unauthorized access detected | Investigation & containment.

High | Data breach or system compromise | Full incident response activation.

5. Incident Response Process

5.1 Preparation

- Implement proactive cybersecurity monitoring.
- Conduct regular employee security awareness training.
- Maintain an updated incident response playbook.

5.2 Identification

- Detect suspicious activities through logs and monitoring.
- Identify affected systems, data, and potential threat actors.

5.3 Containment

- Short-term containment: Isolate infected systems.
- Long-term containment: Apply security patches and updates.

5.4 Eradication

- Remove malware, malicious software, or unauthorized access.
- Conduct forensic analysis to determine the attack vector.

5.5 Recovery

- Restore systems from secure backups.

- Monitor for reinfection and ensure operational stability.

5.6 Lessons Learned

- Conduct a post-incident review.
- Update security policies based on findings.

6. Communication and Notification

6.1 Internal Communication

- Notify executive leadership, IT teams, and affected employees.

6.2 External Communication

- Notify clients, regulatory agencies, law enforcement if applicable.
- Issue public statements via the PR team.

7. Training and Testing

7.1 Training Plan

- Conduct quarterly security awareness programs.
- Implement hands-on security drills for IT personnel.

7.2 Testing Plan

- Simulated phishing tests.
- Annual penetration testing.
- Tabletop exercises for executive teams.

7.3 Schedule

- Training: Quarterly.
- Testing: Bi-annual.
- Unannounced security breach drills.

8. Review and Continuous Improvement

8.1 Plan Review Schedule

- Reviewed semi-annually.
- Updated post-major incidents.
- Reviewed by external auditors annually.

8.2 Plan Update Process

- Adapt based on emerging threats.
- Enhance security infrastructure.
- Ensure compliance with evolving industry regulations.

Conclusion

This Incident Response Plan (IRP) & Risk Management Plan (RMP) provides CyberSecure Inc. with a com