IOWA™ | Department of Management

STATE OF IOWA

KIM REYNOLDS, GOVERNOR

CHRIS COURNOYER, LT GOVERNOR

Disclaimer: This document is a sample provided for informational purposes only. The Iowa Department of Management cannot guarantee that the content will meet all federal program requirements or be suitable for every situation. The Grantee is responsible for reviewing the text, ensuring its compliance with applicable laws, and seeking legal counsel if needed.

Sample Cybersecurity Risk Management Plan

Utilizing NIST Framework for Improving Critical Infrastructure Cybersecurity (Version 2.0)

Introduction

ABC Telecom is committed to safeguarding its infrastructure, data, and stakeholders from the growing threats in the cyber domain. This cybersecurity plan leverages the NIST Framework for Improving Critical Infrastructure Cybersecurity, version 2.0, to create a comprehensive, risk-based approach tailored to the specific needs of the company. The five core functions of the NIST framework—Identify, Protect, Detect, Respond, and Recover—serve as the foundation of this plan.

---

1. Identify

Objective: Develop a deep understanding of the business environment, critical assets, risks, and cybersecurity roles to manage cybersecurity risk effectively.

Key Activities:

- **Asset Management:** Maintain an up-to-date inventory of ABC Telecom's hardware, software, data, and networks. This includes critical communication infrastructure and customer databases.
- **Business Environment:** Define roles and responsibilities for cybersecurity across departments, ensuring integration of cybersecurity within business strategies.
- **Governance:** Establish and enforce security policies, procedures, and compliance with regulatory requirements (e.g., telecommunications and privacy laws).
- **Risk Assessment:** Conduct regular assessments to identify vulnerabilities, threats, and impacts on ABC Telecom's infrastructure.
- **Supply Chain Risk Management:** Collaborate with vendors and third parties to evaluate and manage cybersecurity risks within the supply chain.

Deliverables:

- Updated asset inventory
- Risk assessment reports
- Cybersecurity roles and responsibilities matrix
- Vendor security compliance documentation

2. Protect

Objective: Implement safeguards to ensure the secure delivery of services and limit the impact of potential cyber incidents.

Key Activities:

- **Access Control:** Use role-based access controls, multi-factor authentication (MFA), and least-privilege principles to manage access to critical systems and data.
- **Data Security:** Encrypt sensitive data at rest and in transit, both internally and externally. Implement data loss prevention (DLP) solutions to monitor and control data flows.
- **Awareness and Training:** Conduct mandatory cybersecurity awareness training for all employees to recognize phishing, social engineering, and other cyber threats.
- **Information Protection Processes:** Implement patch management procedures to ensure timely updates of software and hardware. Conduct regular vulnerability scanning.
- **Maintenance and Protective Technology:** Install firewalls, intrusion detection/prevention systems (IDS/IPS), and endpoint protection to prevent unauthorized access and malicious activity.

Deliverables:

- Access control policy
- Data encryption guidelines
- Employee cybersecurity training records
- Patch management and vulnerability scanning reports
- Intrusion detection logs

3. Detect

Objective: Enable timely detection of cybersecurity events to ensure swift response.

Key Activities:

- **Anomalies and Events:** Set up network monitoring and security information and event management (SIEM) systems to detect unusual activity.
- **Continuous Security Monitoring:** Implement real-time monitoring solutions to track security events across ABC Telecom's infrastructure and applications.
- **Detection Processes:** Develop incident detection protocols, including thresholds for alerts and defined escalation paths.

Deliverables:

- SIEM monitoring dashboard
- Incident detection protocols
- Real-time event logs and anomaly reports
- Escalation and notification procedures

---

4. Respond

Objective: Establish an incident response process to mitigate the impact of cybersecurity incidents.

Key Activities:

- **Response Planning:** Develop an incident response plan that includes predefined actions for various types of incidents, such as DDoS attacks, data breaches, and malware infections.
- **Communication:** Establish internal and external communication protocols to inform key stakeholders, including customers, regulators, and law enforcement, about cybersecurity incidents.
- **Analysis:** Perform post-incident analysis to determine the root cause, scope, and impact of the incident.
- **Mitigation:** Execute containment strategies, such as isolating affected systems, and remediation actions to minimize further damage.
- **Improvements:** Update incident response strategies based on lessons learned from each incident.

Deliverables:

- Incident response plan
- Communication protocol documentation
- Post-incident analysis reports
- Remediation actions logs
- Incident response playbook

5. Recover

Objective: Ensure timely restoration of services and learn from incidents to prevent future occurrences.

Key Activities:

- **Recovery Planning:** Establish recovery procedures to restore ABC Telecom's critical services and systems after a cybersecurity event.
- **Improvements:** Implement continuous improvements to recovery strategies based on lessons learned from incidents and evolving threats.
- **Communications:** Ensure transparent communication with all stakeholders during recovery efforts to maintain trust and provide updates on service restoration.

Deliverables:

- Recovery plan and testing documentation
- Post-recovery analysis and improvement logs
- Stakeholder communication records

6. Governance and Continuous Improvement

ABC Telecom will regularly review and update this cybersecurity plan to ensure alignment with the latest regulatory requirements, business objectives, and emerging threats. The plan will be subject to periodic audits to measure its effectiveness and compliance with the NIST framework.

Key Activities:

- Conduct annual audits and assessments
- Establish a cybersecurity steering committee
- Monitor regulatory changes and incorporate updates into the cybersecurity plan

Conclusion

This cybersecurity plan is designed to protect ABC Telecom's critical infrastructure and ensure the confidentiality, integrity, and availability of its services. By adopting the NIST Cybersecurity Framework (version 2.0), the company commits to a risk-based, resilient approach to cybersecurity that will adapt to an evolving threat landscape.