CYBERSECURITY POLICY TEMPLATE

1. PURPOSE AND SCOPE This policy establishes the framework for protecting [ORGANIZATION]'s information assets and ensuring compliance with applicable regulations.

2. INFORMATION SECURITY OBJECTIVES - Protect confidentiality, integrity, and availability of information - Comply with applicable laws and regulations - Minimize risk of security incidents - Ensure business continuity

3. ROLES AND RESPONSIBILITIES - Chief Information Security Officer (CISO): Overall security strategy - IT Security Team: Implementation and monitoring - All Employees: Compliance with security procedures - Management: Resource allocation and oversight

4. ACCESS CONTROL - Principle of least privilege - Multi-factor authentication for sensitive systems - Regular access reviews and audits - Strong password requirements

5. DATA PROTECTION - Encryption of data at rest and in transit - Regular data backups and testing - Data classification and handling procedures - Secure disposal of sensitive information

6. INCIDENT RESPONSE - 24/7 security monitoring - Incident response team activation - Evidence collection and preservation - Communication and notification procedures

7. VENDOR MANAGEMENT - Security assessments of third-party vendors - Contractual security requirements - Regular vendor security reviews - Incident notification procedures

8. TRAINING AND AWARENESS - Annual security awareness training - Phishing simulation exercises - Regular security updates and communications - Role-specific security training

9. COMPLIANCE AND AUDITING - Regular security assessments - Compliance monitoring and reporting - External security audits - Continuous improvement processes

10. POLICY REVIEW AND UPDATES This policy shall be reviewed annually and updated as necessary to reflect changes in technology, regulations, or business requirements.

APPROVED BY: [NAME] - Chief Information Security Officer [DATE]

REVIEW DATE: [NEXT REVIEW DATE]