Cybersecurity Plan
Policy Mappings

Cybersecurity frameworks provide systematic approaches for assessing and documenting an organization's risk. They are generally very comprehensive and can require extensive resources to be fully compliant. Our Template Cybersecurity Policy is specifically targeted towards small businesses and is thus smaller in scope than most frameworks and requires fewer resources to complete. We highly recommend the Policy be used in conjunction with an existing framework so organizations can tailor the Policy to their needs using the framework's existing tools and guidance or so they can pursue future certification without restarting their program. To aid our users, we have provided a mapping of the template to 3 of the most common frameworks.

1. NIST Cybersecurity Framework
    a. The CSF is an internationally recognized standard that "enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience."
    b. The CSF categorizes activities into 5 Core Functions and then into a series of categories and subcategories. All 3 areas are mapped either explicitly or in the format XX.YY-ZZ, where XX is the Core Function, YY is the category, and ZZ is the subcategory.

2. Center for Internet Security's (CIS) Controls
    a. "The CIS Controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks."

b. The current version of the CIS Controls, v7.1, contains 20 main controls, each with sub-controls. They are mapped in a number format of XX.YY, where XX is the main control and YY is the sub-control.

3. ISO/IEC 27001 Information Security Management System (ISMS)
   a. The 27001-series is an international standard that defines a management system and process for information security that systematically examines risks and requires the implementation of a suite of associated controls.
   b. 27001 contains 14 clauses with 114 total controls. They are mapped in the format A.XX.YY.ZZ, where A is the Annex number and is always present, XX is the clause categorization, and YY.ZZ is the specific control number.
   c. These mappings were provided as part of the NIST CSF documentation.

Identify

1. Roles and Responsibilities
    a. NIST CSF: ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
    b. CIS: 17.3: Implement a Security Awareness Program; 19.2: Assign Job Titles and Duties for Incident Response
    c. ISO 27001 (per CSF mapping): A.6.1.1

2. Legal and regulatory requirements
    a. NIST CSF: ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
    b. CIS: N/A
    c. ISO 27001 (per CSF mapping): A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5

Protect

1. Account Management
    a. Use administrator accounts according to the principles of least privilege and separation of duties
        i. NIST CSF: PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
        ii. CIS: 4 (especially 4.3)
        iii. ISO 27001 (per CSF mapping): A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5
    b. Promptly revoke credentials upon separation
        i. NIST CSF: PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
        ii. CIS: 16 (especially 16.7, 16.8, 16.9, 16.10, and 16.12)
        iii. ISO 27001 (per CSF mapping): A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4,A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3

2. Authentication and Password Management
    a. Enable multi-factor authentication (MFA) where possible
    b. Consider using a password manager
        i. NIST CSF: PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
        ii. CIS: 4.2, 4.4, 4.5, 16.3
        iii. ISO 27001 (per CSF mapping): A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4

3. User Training
    a. NIST CSF: PR.AT-1: All users are informed and trained
    b. CIS: 17 (most, especially 17.3)
    c. ISO 27001 (per CSF mapping): A.7.2.2, A.12.2.1

4. Data Backups and Disposal
    a. Backups
        i. NIST CSF: PR.IP-4: Backups of information are conducted, maintained, and tested
        ii. CIS: 10 (especially 10.1, 10.4, 10.5)
        iii. ISO 27001 (per CSF mapping): A.12.3.1,A.17.1.2, A.17.1.3, A.18.1.3
    b. Disposal
        i. NIST CSF: PR.IP-6: Data is destroyed according to policy
        ii. ISO 27001 (per CSF mapping): A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7

5. Incident Response Plan
    a. Shall include notification to the City of incidents affecting City data
        i. NIST CSF: PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
        ii. CIS: 19 (especially 19.1)
        iii. ISO 27001 (per CSF mapping): A.16.1.1,A.17.1.1, A.17.1.2, A.17.1.3

6. Incident Recovery Plan
        i. NIST CSF: PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
        ii. CIS: 19 (especially 19.1)
        iii. ISO 27001 (per CSF mapping): A.16.1.1,A.17.1.1, A.17.1.2, A.17.1.3

7. Vulnerability Management Plan. Specifically, vendors shall:
    a. Enable automatic software updates where possible
    b. Perform antivirus and antimalware scanning
    c. Establish a vulnerability disclosure program (VDP)
        i. NIST CSF: PR.IP-12: A vulnerability management plan is developed and implemented
        ii. CIS: 3 (3.1, 3.2, 3.4); 8 (8.1, 8.2)
        iii. ISO 27001 (per CSF mapping): A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3

Detect

1. Execution of the Vulnerability Management Plan
    a. NIST CSF: DE.CM-4: Malicious code is detected
    b. NIST CSF: DE.CM-8: Vulnerability scans are performed

Respond

1. Execution of the Incident Response Plan
    a. NIST CSF: RS.RP-1: Response plan is executed during or after an incident

Recover

1. Execution of the Incident Recovery Plan
    a. NIST CSF: RC.RP-1: Recovery plan is executed during or after a cyber-security incident