Elements of Privacy Program

An effective privacy program combines an understanding of the applicable privacy and data protection principles, frameworks, and laws, with reasonable policies and procedures that are implemented through program activities.

1. **Privacy Principles and Frameworks**
    a. NIST Privacy Framework
    b. AICPA Privacy Management Framework
    c. FIPPs Fair Information Practice Principles
    d. OECD Privacy Principles
    e. Legal/regulation driven principles, such as EU GDPR or CCPA/CPRA
    f. Sample Organizational Privacy Principles
        i. Management
        ii. Agreement, Notice, and Communication
        iii. Collection and Creation
        iv. Use, Retention, and Disposal
        v. Access
        vi. Disclosure to Third Parties
        vii. Security for Privacy
        viii. Data Integrity and Quality
        ix. Monitoring and Enforcement

2. **Applicable Laws and Regulations**
    a. U.S. Federal Privacy Laws
        i. Unfair and deceptive trade practices (FTC Section 5)
        ii. Sectoral laws (FERPA, HIPAA, FCRA, GLBA, etc.)
        iii. Marketing laws (TCPA, CAN-SPAM)
    b. State privacy laws
        i. State data breach notification laws
        ii. State comprehensive/consumer privacy laws
        iii. Topic specific laws – data security, artificial intelligence, biometrics, health, employment, etc.
        iv. State mini-FTC laws relating to unfair and deceptive trade practices
    c. Global Privacy Laws
        i. EU General Data Protection Regulation, and UK GDPR
        ii. Canada Personal Information Protection and Electronic Documents Act
        iii. China Personal Information Protection Act
        iv. Brazil General Data Protection Law (LGPD)
        v. Data Protection Laws of the World

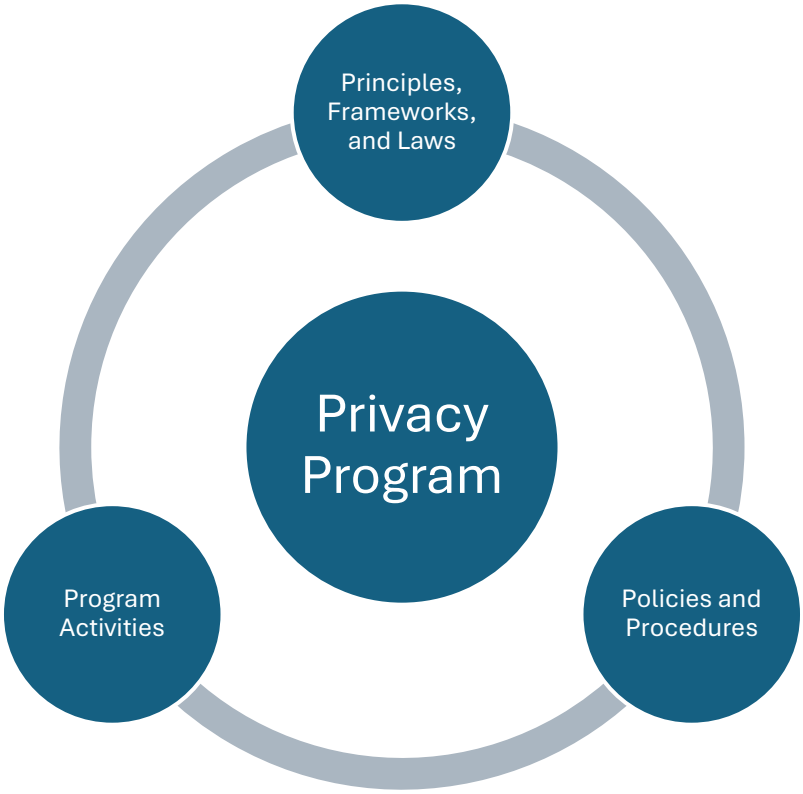
3. **Policies, Standards, and Procedures**
    a. Privacy Notice
        i. Publicly facing statement of organization's privacy practices

ii. Covers topics required by applicable law, such as what personal information is collected and for what purpose, if and how personal information is disclosed to third parties, and who to contact with privacy-related questions or complaints

b. Internal Privacy Policy
    i. Defines personal information and sensitive personal information
    ii. Establishes minimum standards for handling personal information
    iii. Informs personnel how to report a data incident
    iv. Assigns accountability for protection of personal information at organization
        1. Establishing policies and monitoring for compliance
        2. Determining applicable laws and monitoring for changes
        3. Maintaining a comprehensive information security program that protects personal information
        4. Establishing appropriate oversight at Board or Board committee level
        5. Managing third party vendors
        6. Reviewing allocation of personnel, budgets, and other resources
    v. Includes standards and procedures as needed, such as classifying personal information, data minimization, data incident response, data subject requests, and data inventory

4. Program Activities

a. Data Inventory and Mapping
b. Responding to Data Subject Requests
c. Data Protection Impact Assessments
d. Data Retention and Minimization
e. Vendor Management and Data Processing Agreements
f. Privacy and Data Protection by Design
g. Data Security
h. Training and Awareness
i. Monitoring and Evaluation
j. Coordinate with Related Functions and their Policies and Practices
    i. Information Security
    ii. Data Governance
    iii. Records Management
    iv. Ethical Research


Principles, Frameworks, and Laws
Privacy Program
Program Activities
Policies and Procedures