**Data Privacy & Cybersecurity Management Template**

**Baseline Practice**: S0.1 & 2 – Data Privacy & Cybersecurity Management

**Applicable Asset Classes**: Office, ESC, OAR, Light Industrial, Healthcare, Universal, and MURB

|  |
| --- |
| ***Instructions:****All grey italic text with borders are instructions to help you prepare the required Baseline Practice for your building Data Privacy Template.* 1. *Replace all* [blue text in brackets] *in the document with building Data Privacy information*
2. *Where required, complete the necessary tasks, or engage a third-party consultant to complete the tasks so that you are able to fill the relevant sections of the template.*
3. *Delete all grey italic text when you have filled all relevant sections with building specific information.*
 |

***Note!***

***Developing a comprehensive cybersecurity policy is essential for IT organizations in Canada to protect your information assets and comply with national laws and regulations. Below is a structured guide to create such a policy.***

**Data Privacy Policy**

[Insert Building Name and Address]

[Insert Name of Organization]

[Insert Contact Information]

# Data Privacy Policy Purpose

[Insert Data Privacy Policy Purpose]

The purpose of this Cybersecurity Policy is to establish a comprehensive framework that safeguards [Organization Name]'s information assets against cyber threats, ensuring the confidentiality, integrity, and availability of data. This policy aims to:

* **Protect Information Assets:** Implement measures to defend against unauthorized access, disclosure, alteration, and destruction of organizational data.
* **Ensure Regulatory Compliance:** Adhere to applicable AHJ (Authority Having Jurisdiction) laws and regulations, including the Personal Information Protection and Electronic Documents to maintain legal and ethical standards.
* **Define Security Responsibilities:** Clearly delineate roles and responsibilities related to cybersecurity across all levels of the organization to foster accountability and proactive risk management.
* **Promote Security Awareness:** Cultivate a culture of security awareness through regular training and education, empowering employees to recognize and respond to potential cyber threats effectively.
* **Facilitate Incident Response:** Establish protocols for timely detection, reporting, and response to cybersecurity incidents to minimize impact and support swift recovery.

By achieving these objectives, [Organization Name] aims to protect its digital infrastructure, support business continuity, and uphold the trust of clients, partners, and stakeholders.

***This section should define the policy's applicability, specifying the information systems, data, employees, contractors, and third parties subject to the policy.***

# Data Privacy Policy Scope

[Insert Data Privacy Policy Scope]

The Scope of this Cybersecurity Policy encompasses all individuals and systems interacting with [Organization Name]'s information assets. Specifically, it applies to:

* Personnel: All employees, contractors, consultants, temporary staff, volunteers, and any other individuals granted access to [Organization Name]'s information systems and data.
* Information Assets: All data, whether electronic or physical, that is owned, managed, or processed by [Organization Name], including confidential, sensitive, and personal information.
* Information Systems: All hardware, software, networks, applications, and devices (both organization-owned and personal) that access or handle [Organization Name]'s data.

This policy is applicable across all operational environments, including on-site locations, remote work settings, and any other scenarios where [Organization Name]'s information assets are accessed or utilized. Adherence to this policy is mandatory for all aforementioned parties to ensure the security and integrity of [Organization Name]'s information resources.

***This section should outline the objectives of the cybersecurity policy, including the protection of information assets, compliance with legal requirements, and the establishment of security responsibilities within the organization.***

# Definitions

[Insert Definitions]

In the context of [Organization Name]'s Cybersecurity Policy, the following definitions clarify key terms:

* Access Control: Mechanisms that restrict access to information systems and data to authorized users, processes, or devices, ensuring that only permitted activities are executed.
* Confidential Information: Data that is restricted to authorized individuals due to its sensitive nature, including personal data, proprietary business information, and any other information classified as confidential by [Organization Name].
* Cybersecurity Incident: An event that compromises the confidentiality, integrity, or availability of information systems or data, such as unauthorized access, data breaches, or malware attacks.
* Data Encryption: The process of converting data into a coded format to prevent unauthorized access during transmission or storage.
* Information Assets: All data, hardware, software, and other components that [Organization Name] utilizes to conduct its operations.
* Personal Data: Information about an identifiable individual, including but not limited to contact details, identification numbers, and any data that can uniquely identify a person.
* Risk Assessment: The systematic process of identifying, evaluating, and prioritizing risks to organizational operations and assets.
* Security Controls: Safeguards or countermeasures employed to protect information systems and data from security threats.
* Third Parties: External entities, including vendors, partners, and service providers, that interact with [Organization Name]'s information systems or data.

These definitions are intended to provide clarity within this policy. For a comprehensive glossary of cybersecurity terms, refer to AHJ (Authority Having Jurisdiction) glossary.

***This section should define clear definitions for key terms used in the policy, such as "cybersecurity incident," "confidential information," and "personal data.".***

# Legal and Regulatory Compliance

[Insert Regulatory Compliance]

Ensuring compliance with AHJ (Authority Having Jurisdiction) legal and regulatory frameworks is a cornerstone of [Organization Name]'s Cybersecurity Policy. This commitment encompasses adherence to the following key AHJ.:

1. Personal Information Protection and Electronic Documents within AHJ.

2. An Act Respecting Cyber Security within AHJ

3. Criminal Code of AHJ

4. AHJ Legislation

***Provide additional details regarding the organization's commitment to complying with relevant AHJ laws and regulations.***

# Roles and Responsibilities

[Insert Roles and Responsibilities]

Establishing clear roles and responsibilities is essential for the effective implementation of [Organization Name]'s Cybersecurity Policy. The following outlines the key stakeholders and their respective duties:

1. Board of Directors
* Governance Oversight: Ensure that cybersecurity strategies align with organizational objectives and regulatory requirements.
* Resource Allocation: Approve necessary resources for the development and maintenance of cybersecurity programs.

2. Chief Executive Officer (CEO)

* Strategic Leadership: Champion cybersecurity initiatives and integrate them into the organization's overall strategy.
* Policy Enforcement: Ensure adherence to cybersecurity policies across all departments.

3. Chief Information Security Officer (CISO)

* Policy Development: Draft, implement, and update cybersecurity policies and procedures.
* Risk Management: Identify, assess, and mitigate cybersecurity risks.
* Incident Response: Lead the response to cybersecurity incidents and coordinate recovery efforts.

4. Information Technology (IT) Department

* Infrastructure Security: Implement and maintain security controls for hardware, software, and networks.
* Monitoring and Maintenance: Regularly monitor systems for vulnerabilities and apply necessary updates.

5. Department Managers

* Policy Implementation: Ensure that their teams comply with cybersecurity policies and procedures.
* Training Facilitation: Coordinate cybersecurity awareness training for team members.

6. Employees and Contractors

* Policy Adherence: Follow established cybersecurity policies and report any suspicious activities.
* Security Practices: Protect organizational data by using strong passwords and safeguarding sensitive information.

7. Third-Party Partners

* Compliance Assurance: Adhere to [Organization Name]'s cybersecurity standards and undergo regular security assessments.
* Incident Reporting: Promptly report any security incidents that could impact [Organization Name].

By clearly defining these roles and responsibilities, [Organization Name] aims to foster a culture of security awareness and ensure the protection of its information assets.

***This section should assign specific cybersecurity responsibilities to various roles within the organization.***

# Risk Management

[Insert Risk Management Stratagy]

Effective risk management is essential for safeguarding [Organization Name]'s information assets and ensuring compliance with Canadian cybersecurity standards. Our approach aligns with the AHJ (Authority Having Jurisdiction) Cyber Security's guidelines, particularly the IT Security Risk Management.

1. Risk Management Framework

We adopt a structured risk management framework that integrates into our organizational processes, encompassing:

* Risk Identification: Systematically identify potential threats and vulnerabilities that could impact information systems.
* Risk Assessment: Evaluate identified risks to determine their potential impact and likelihood.
* Risk Mitigation: Implement appropriate controls to reduce risks to acceptable levels.
* Risk Monitoring: Continuously monitor the risk environment and the effectiveness of controls.

2. Roles and Responsibilities

* Senior Management: Provide oversight and ensure resources are allocated for risk management activities.
* Risk Management Team: Conduct risk assessments, develop mitigation strategies, and monitor risk levels.
* All Employees: Adhere to security policies and report any observed risks or incidents.

3. Risk Assessment Process

Our risk assessment process includes:

* Asset Identification: Catalog information assets and their importance to organizational operations.
* Threat Analysis: Identify potential threats, including cyber-attacks, natural disasters, and human errors.
* Vulnerability Assessment: Determine weaknesses that could be exploited by threats.
* Impact Analysis: Assess the potential consequences of risk events on operations and assets.
* Risk Evaluation: Prioritize risks based on their assessed impact and likelihood.

4. Risk Mitigation Strategies

To address identified risks, we implement:

* Preventive Controls: Measures such as firewalls, access controls, and encryption to prevent incidents.
* Detective Controls: Systems like intrusion detection to identify and alert on incidents.
* Corrective Controls: Procedures to restore systems and data after an incident.

5. Continuous Monitoring and Review

Recognizing the dynamic nature of cyber threats, we:

* Regularly Update Risk Assessments: Reflect changes in the threat landscape and organizational operations.
* Audit Controls: Ensure implemented controls are effective and compliant with policies.

By adhering to this risk management approach, [Organization Name] commits to protecting its information assets and maintaining resilience against evolving cyber threats.

***This section should describe the process for identifying, assessing, and mitigating cybersecurity risks, including regular risk assessments and the implementation of appropriate controls.***

# Security Controls

[Insert Security Control Measures]

To safeguard [Organization Name]'s information assets, we implement the following administrative measures:

1. Policy Development and Enforcement

* Information Security Policies: Establish comprehensive policies outlining security expectations and protocols for all personnel.
* Acceptable Use Policy: Define appropriate use of organizational resources, including internet, email, and devices.
* Data Classification Policy: Categorize data based on sensitivity to determine requisite protection levels.

2. Access Management

* Access Control Procedures: Implement processes to grant, modify, and revoke access rights, ensuring only authorized individuals access specific information.
* Least Privilege Principle: Restrict user access to the minimum necessary for job functions.
* Regular Access Reviews: Conduct periodic audits to verify appropriate access levels.

3. Personnel Security

Background Checks: Perform screenings for employees and contractors handling sensitive information.

* Security Awareness Training: Provide ongoing education on security policies, threat recognition, and best practices.
* Confidentiality Agreements: Require personnel to sign agreements to protect organizational information.

4. Incident Response Planning

* -Incident Response Plan: Develop and maintain procedures for identifying, reporting, and addressing security incidents.
* Incident Response Team: Designate a team responsible for managing and mitigating incidents.
* Post-Incident Analysis: Conduct reviews to identify lessons learned and improve future responses.

5. Risk Management

* Risk Assessments: Regularly evaluate potential threats and vulnerabilities to information assets.
* Risk Mitigation Strategies: Implement controls to reduce identified risks to acceptable levels.
* Continuous Monitoring: Track risk environment changes and control effectiveness.

6. Compliance and Audit

* Regulatory Compliance: Ensure adherence to applicable laws and standards..
* Regular Audits: Perform internal and external audits to assess policy compliance and control efficacy.
* Documentation: Maintain records of compliance efforts and audit results.

7. Third-Party Management

* Vendor Security Assessments: Evaluate third-party partners' security practices before engagement.
* Service Level Agreements (SLAs): Include security requirements in contracts with third parties.
* Ongoing Monitoring: Regularly review third-party compliance with security standards. By adhering to this risk management approach, [Organization Name] commits to protecting its information assets and maintaining resilience against evolving cyber threats.

By implementing these administrative measures, [Organization Name] aims to establish a robust security posture, ensuring the protection of information assets and compliance with relevant regulations.

***In this section outline the technical and administrative measures in place to protect information assets.***

# Policy Review and Approval

This Data Privacy & Cybersecurity Policy shall be reviewed on an annual basis to ensure it remains current, effective, and aligned with evolving cybersecurity threats, legal requirements, and best practices. Any necessary updates shall be documented and communicated to all relevant personnel.

**Review Schedule**

• Next Review Date: [Insert Date]

• Review Conducted By: [Insert Name/Title]

**Sign-Off Acknowledgment**

By signing below, the undersigned confirm that they have reviewed and approved this Data Privacy & Cybersecurity Policy and acknowledge their responsibility to ensure compliance with its provisions.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Title | Signature | Date |
| [Insert Name] | [Insert Title] | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | [Insert Date] |
| [Insert Name] | [Insert Title] | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | [Insert Date] |
| [Insert Name] | [Insert Title] | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | [Insert Date] |