TEMPLATE

INFORMATION SECURITY POLICY

Objective

An information security policy demonstrates management's commitment to information security. This policy must be communicated to all users in a format that is appropriate, accessible and understandable.

The sections outlined in this template should be found in your information security policy. The content should be tailored to your specific business requirements and all applicable laws and regulations.

Document recipient: company manager or information security manager

Last revision date: 2016-12

Policy content

Title	**Information Security Policy**
Effective date	[Date]
Last revision date	[Date]
Revision frequency	E.g., every 3 years
Document owner	E.g., information security manager
Approved by	E.g., Board of Directors
Intended for	E.g., all employees

1. PURPOSE

The information security policy (hereinafter the "Policy") establishes legal and regulatory requirements and complies with recognized industry practices.

This Policy establishes guiding principles for mitigating risks while maintaining the operational effectiveness of the activities of [COMPANY NAME].

This Policy supports the implementation and maintenance of measures for protecting information that reduce, to an acceptable level, risks that could

negatively affect the availability, integrity or confidentiality of information, cause financial losses or harm the reputation of [COMPANY NAME].

2. GUIDING PRINCIPLES

2.1.1. Considering the potential impact that the exploitation of an information security vulnerability could have on client trust and the reputation and financial situation of the company, information security is everyone's responsibility. It concerns all executives, employees, consultants and any supplier or subcontractor that provides services or has access to the information.

2.1.2. Information security investments are planned by [MANAGERS' NAMES] to keep information security risks at an acceptable level for [COMPANY NAME].

2.1.3. The information protection measures to be put in place will be proportionate to the security risks that are identified and determined according to the potential impact on the assets being protected.

2.1.4. The management of information security operations and related processes is essential for ensuring that the assets of [COMPANY NAME] are protected, as well as for detecting and mitigating key threats. Information security incident management is in place to quickly and efficiently handle threats that have arisen.

2.1.5. Risks to and measures for protecting IT assets will be periodically evaluated.

2.1.6. Information security hinges on employee integrity, knowledge and vigilance. Human resource management and the information security awareness and training program are essential for ensuring an appropriate level of information security skill and expertise on the part of the staff of [COMPANY NAME].

2.1.7. Agreements and contracts that [COMPANY NAME] enters into must contain written provisions that guarantee that all parties comply with information protection and security requirements.

2.1.8. [COMPANY NAME] will comply with the applicable regulations and industry requirements concerning information security.

3. RESPONSIBILITIES, APPLICATION AND REVISION

3.1. Roles and responsibilities

3.1.1 The Board of Directors of [COMPANY NAME]:

- Appoints the information security manager
- Allocates financial resources associated with information security
- Conveys the importance of information security to the executives and employees of [COMPANY NAME]
- Supports the implementation of protective measures

3.1.2. The information security manager:

- Evaluates the risks and threats that may affect the assets of [COMPANY NAME]
- Ensures that protective measures are put in place
- Increases awareness of and trains employees on information security

3.1.3. Managers:

- Adopt behaviours aimed at keeping information secure and serve as models for information security to their employees
- Protect the IT assets under their responsibility, as applicable
- Take on the responsibilities assigned to them by the protective measures
- Make sure that the employees for which they are responsible:
    - Participate in the information security awareness and training program and apply what they have learned
    - Understand and follow the protective measures
    - Only have the access permissions necessary to perform their duties

3.1.4. Employees:

- Participate in the information security awareness and training program and apply what they have learned
- Adopt behaviours that keep information secure
- Follow the measures for protecting information

3.2. Policy revision

XX is responsible for revising the Policy at least every XX years.

4. EFFECTIVE DATE

The Policy will be effective from the date it is adopted.