REFERENCE SHEET

INFORMATION SECURITY POLICY

Purpose of the document

An information security policy helps demonstrate management's commitment to ensuring information security. The policy must be disclosed to all users and made available, accessible and presented in an appropriate format.

The sections presented in this template should be part of your own security information policy. The content will have to be adapted to the occupational requirements and regulations in effect.

Content of the policy

Title	**Information Security Policy**
Effective date	
Last reviewed	
Review frequency	E.g. Every 3 years
Unit responsible	E.g. Information Security Officer
Approved by	E.g. Board of Directors
Intended for	E.g. All employees

1. GOALS

The Information Security Policy (the "Policy") sets out legal and regulatory requirements as well as practices recognized in the industry.

This Policy establishes the guiding principles intended to mitigate risks while maintaining the operational efficiency of [NAME OF COMPANY].

This Policy supports the implementation and maintenance of information protection measures that reduce to an acceptable level risks that could compromise the availability, integrity and confidentiality of information, cause financial losses. or damage the reputation of [NAME OF COMPANY].

2. GUIDELINES

2.1.1. Considering the potential impact of an information security breach on clients' confidence as well as on the company's reputation and financial situation, information security is everyone's responsibility. It concerns all executives,

employees and consultants, as well as all suppliers and subcontractors who provide services or have access to information.

2.1.2. Information security investments are planned by [NAME OF INDIVIDUALS IN CHARGE] in order to maintain information security risks at an acceptable level for [NAME OF COMPANY].

2.1.3. The information protection measures to put in place are proportional to the security risks identified and determined based on the importance and potential impacts on the assets to protect.

2.1.4. In order to protect the assets of [NAME OF COMPANY] and to detect and thwart the main threats, it is essential to manage information security activities and related processes. Information security incidents are managed to efficiently and effectively deal with emerging threats.

2.1.5. Risks to IT assets and protection measures must be assessed periodically.

2.1.6. Information security is based on employees' integrity, knowledge and vigilance. Human resources management processes, together with an information security awareness and training program, are indispensable for ensuring that the

employees of [NAME OF COMPANY] have an appropriate level of competency and expertise regarding information security.

2.1.7. The agreements and contracts in which [NAME OF COMPANY] is a stakeholder must contain explicit provisions attesting to compliance, by all parties, with information security and protection requirements.

2.1.8. [NAME OF COMPANY] complies with the applicable information security regulations and industry requirements.

3. RESPONSIBILITIES, APPLICATION AND REVISION

3.1. Roles and responsibilities

3.1.1. Executive Committee of [NAME OF COMPANY]

- Appoints the Information Security Officer
- Allocates the financial resources for information security
- Communicates the importance of information security to the executives and employees of [NAME OF COMPANY]
- Ensures that protection measures have been put in place

3.1.2. Information Security Officer

- Assesses the risks and threats that could affect the assets of [NAME OF COMPANY]
- Ensures that protection measures have been put in place
- Fosters awareness and provides training to employees regarding information security

3.1.3. Managers

- Adopt behaviours to ensuring information security and set an example for their employees when it comes to information security
- Protect the IT assets under their responsibility, if applicable
- Perform the responsibilities ascribed to them in the protection measures
- Make sure that all employees under their responsibility:
    - Take and apply the security information awareness and training program
    - Understand and comply with the protection measures
    - Are only granted the accesses they need to perform their functions

3.1.4. Employees

- Take the security information awareness and training program and put it into practice
- Adopt behaviours to ensure information security
- Comply with information protection measures

3.2. Policy review

XX is responsible for reviewing this Policy at least once every XX years.

4. EFFECTIVE DATE

The Policy takes effect immediately upon adoption.