SAMPLE POLICY

Information Security

General Guidance Note:

This sample policy is not legal advice or a substitute for consultation with qualified legal counsel. Laws vary from country to country. Policies should have effective dates noted on the face of the policy and the company should retain an archive of earlier versions. This sample policy should not be implemented or executed except on the advice of counsel.

Sample Text:

OVERVIEW

Company has a duty and responsibility to protect the information under its custody and control. Being able to access complete and accurate information is vital to Company's ability to operate efficiently and successfully provide products and services to customers.

Company also collects, stores, uses and discloses confidential and personal information on private individuals, employees, partners and suppliers and its own operations. Company has a duty to safeguard such information when processing it.

This Information Security Policy (this "Policy") generally aligns with the information security management systems standards published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (EC) as more specifically set forth in ISO 27001 and 27002. Implementing this Policy will therefore help Company comply with various aspects of such international data security standards.

PURPOSE

The purpose of this Policy is to:

- Protect Company's information against loss or theft, unauthorized access, disclosure, copying, use, modification or destruction (each an "Information Security Incident")
- Describe and clarify roles and responsibilities in respect of the creation, collection, use, storage, disclosure and destruction of information
- Strengthen Company's business continuity in the event that information is compromised or lost
- Enhance Company's compliance with applicable laws, regulations and contractual obligations
- Ensure that Company's procedures and processes prioritize the protection of the following aspects of information:
    - Confidentiality, so that information is accessible only to authorized individuals
    - Integrity, so that the accuracy and completeness of information are not compromised
    - Availability, so that authorized users have access to all relevant information when required.

SCOPE

This Policy establishes the framework for the management of information security within Company.

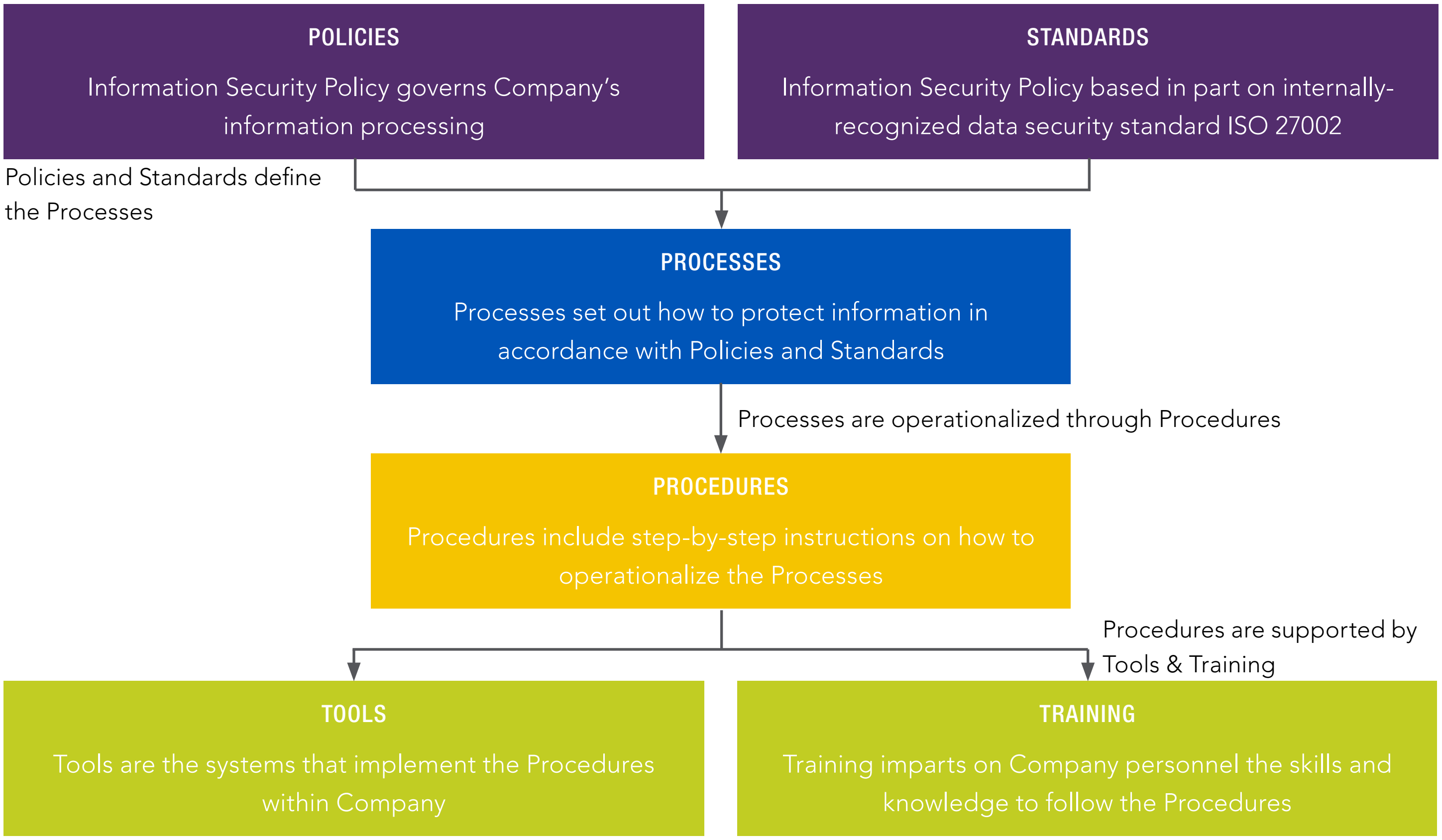
This Policy and the procedures, processes and other measures connected to it apply to all directors, officers and employees of Company, as well as third-party contractors and agents of Company that have access to Company's information or information systems (collectively, "Individual Users").

This Policy applies to all forms of information created, communicated, collected, used, stored and disclosed in connection with Company's operations, including:

- Oral communications
- Documents, records and other information in hard-copy or electronic form
- Documents, records and other information transmitted by post, courier, fax, electronic mail, text messages and other means
- Information stored in Company servers, computers, laptops, mobile phones and other information systems
- Information stored on any type of removable media, including memory sticks, digital cameras, discs and other means.

STRUCTURE

This Policy is based on ISO 27002 and structured around the 11 main security category areas set forth therein. This Policy is supported and implemented by various controls intended to protect Company information, including those set forth in standards, processes, procedures and other measures (see below)



POLICIES

Information Security Policy governs Company's information processing

STANDARDS

Information Security Policy based in part on internally-recognized data security standard ISO 27002

Policies and Standards define the Processes

PROCESSES

Processes set out how to protect information in accordance with Policies and Standards

Processes are operationalized through Procedures

PROCEDURES

Procedures include step-by-step instructions on how to operationalize the Processes

Procedures are supported by Tools & Training

TOOLS

Tools are the systems that implement the Procedures within Company

TRAINING

Training imparts on Company personnel the skills and knowledge to follow the Procedures

RISKS

A failure to adhere to this Policy and the procedures and processes implemented thereunder may put information at risk of an Information Security Incident.

Information Security Incidents can result in a broad range of negative consequences, including embarrassment, financial loss, non-compliance with standards and legislation and liability to third parties. An Information Security Incident could occur at any point of the life cycle of the affected information (i.e., at its creation, collection, use, processing, storage, disclosure, deletion or destruction).

Company will therefore regularly undertake risk assessments to identify, quantify, and prioritize risks associated with its information, and subsequently develop controls to mitigate such risks. Company will undertake risk assessments using a consistent and systematic approach.

SECURITY POLICY

This Policy sets out Company's approach to managing information security. This Policy is approved by management and is communicated to all staff and employees of Company, contractual third parties and agents of Company.

The security requirements for Company will be reviewed at least annually by the head of the IT Security Department and any changes to the Policy shall first be approved by the Board of Directors.

Organization of Information Security

The Head of the IT Security Department will review and make recommendations on the security policy, policy standards, directives, procedures, Incident management and security awareness education.

Company shall incorporate all applicable statutory, regulatory and contractual requirements in this Policy and its information security processes and procedures. Company will also work to adhere to the ISO 27000 standards (the International Standards for Information Security), including by:

- Issuing guidance on what constitutes an Information Security Incident
- Implementing processes and procedures that require all known or reasonably suspected Information Security Incidents and vulnerabilities to Company's information security systems to be reported to the IT Security Department and subsequently investigated
- Producing, maintaining and testing business continuity plans
- Preparing and administering information security education and training to all Individual Users as appropriate
- Ensuring that Individual Users only have access to and use Company information as required for legitimate business purposes
- Obtaining specialist external advice where necessary to maintain this Policy and any processes and procedures hereunder to address new and emerging threats and standards.

The requirements of this Policy shall be reflected in Company's processes, procedures and contractual arrangements.

INFORMATION SECURITY RESPONSIBILITIES

The Head of the IT Security Department is the designated owner of this Policy and is responsible for the maintenance and administration of this Policy and the processes and procedures thereunder.

Heads of Company Departments are responsible for ensuring that Individual Users are made aware of and comply with this Policy and the processes and procedures thereunder.

Company's auditors shall review the adequacy of the controls that put in place to protect Company's information and recommend improvements where deficiencies are identified.

All Individual Users are required to adhere to this Policy and the processes and procedures thereunder. Failure to comply may result in disciplinary action up to and including termination from employment for cause, termination of contract, and civil penalties and/or criminal sanctions, depending on the circumstances.

ASSET MANAGEMENT

All Company assets (data, information, software, computer and communications equipment, service utilities and people) shall be accounted for and have an owner response for their maintenance and protection.

HUMAN RESOURCES SECURITY

Company's information and other security policies will be communicated to all directors, officers, employees contractors and other third parties to ensure that they understand their responsibilities.

Company's job descriptions and terms and conditions of employment shall include the relevant Individual User's security responsibilities.

Background checks shall be carried out on new Individual Users to determine whether any particular Information Security Incident risks may be identified.

PHYSICAL AND ENVIRONMENTAL SECURITY

Company shall store Company information using reasonable physical and environmental safeguards appropriate to their sensitivity.

In particular, areas in which Company stores Company information will be secured by defined security perimeters with appropriate security barriers and entry controls.

Furthermore, critical and sensitive information will be physically protected from unauthorized access, damage and interference.

COMMUNICATIONS AND OPERATIONS MANAGEMENT

Company will define responsibilities and implement processes and procedures regarding the management, operation and ongoing security and availability of all data and information processing facilities.

Wherever appropriate, Company shall segregate duties and build additional checks into operational processes and procedures to reduce the risk of negligent or deliberate Information Security Incidents.

ACCESS CONTROL

Company will control Individual Users' access to Company information.

In particular, an Individual User's access to information and information systems will be set in accordance with Company's business requirements. Access will be granted to employees, third parties and other individuals according to their business role and only to the extent necessary to permit them to carry out their duties. A procedure will be implemented to document and update individuals' access privileges to Company information.

INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, MAINTENANCE

Company shall identify relevant information security requirements and undertake information risk assessments prior to or during the development, implementation or modification of Company information systems so that information security risks are accounted for as early as possible. Company shall implement reasonable and appropriate controls to mitigate any risks that are identified.

INFORMATION SECURITY INCEDENT MANAGEMENT

Everyone subject to this Policy shall report any known or reasonably suspected Information Security Incident or vulnerability to Company's information systems to the IT Security Department as soon as practicable. Company shall ensure that all directors, officers, employees, contractors and other third parties are made aware of the procedures for reporting the different types of Information Security Incidents or vulnerabilities that may affect Company's information systems.

Company shall take all required and appropriate corrective actions in response to an Information Security Incident, including providing any notifications to privacy and data protection regulators and affected individuals where required by applicable law.

BUSINESS COMMUNITY MANAGEMENT

Company will identify its critical business processes and implement measures to protect such processes from the effects of Information Security Incidents, natural disasters and other major failures of information systems ("Major Disruptions").

In particular, Company will implement an enterprise-wide business continuity management process to minimize the impact on Company of any Major Disruption, recover information assets from loss wherever possible, and ensure that critical business processes resume as quickly as possible.

Where a Major Disruption occurs, Company shall undertake a business impact analysis to assess the consequences of such event.

COMPLIANCE

Company shall comply with all statutory, regulatory and contractual obligations that affect the design, operation, use and management of its information systems.

RESPONSIBILITY FOR THIS POLICY

The [[BOARD OF DIRECTORS] OR [COMMITTEE] OR [POSITION]] has overall responsibility for the effective operation of this policy but has delegated day-to-day responsibility for overseeing its implementation to [POSITION]. All managers have a specific responsibility to operate within the boundaries of this policy, take effective steps so that all employees understand the standards of behavior expected of them, and to take action when behavior falls below its requirements. Managers will be given training in order that they may do so. Effective Date: [insert]

ABOUT BAKER & MCKENZIE

Founded in 1949, Baker & McKenzie advises many of the world's most dynamic and successful business organizations through our 12,000 staff in 77 offices in 47 countries. The Firm is known for its global perspective, deep understanding of the local language and culture of business, uncompromising commitment to excellence, and world-class fluency in its client service. For more information, visit www.bakermckenzie.com.