Frank Cowan Company

Security Policy

Instructions

This template is a starting point to enable you to create a Security Policy tailored to meet the needs of your organization.

Perform a full document replacement of **<Organization>** with the proper name of your organization.

When you have customized the policy to your satisfaction, you can simply delete these instructions and paste the remaining text into your own policy document format. Alternatively, you may modify the footer in this document to suit your organization.

Policy Change Log

Date	Change	Edited by:	Approved by:
	Policy creation		

Table of Content

Purpose

This Information Security Policy (“Policy”) expresses <Organization>’s commitment to managing information security risks effectively and efficiently, coordinated globally and in compliance with applicable regulations wherever it conducts business.

This Policy is the foundation for all information security activities. It focuses not only on the technology for the storage, processing, and transmission of information, but also on administrative and operational practices for the protection of all information, data, files, and processing resources owned by <Organization>.

It is the intent of this Policy to facilitate the exchange of information and computing resources while balancing the need for protecting information with the cost of implementation.

This Policy is the property of <Organization>. It is intended for distribution to all employees and users of information systems at <Organization> locations.

Scope

This Policy applies to all employees, vendors, contractors, and consultants, who create, distribute, access, or manage information by means of <Organization>’s information technology systems including personal or corporate computers, networks, and communication services by which they are connected. It equally applies to individuals and enterprises, who by nature of their relationship to <Organization>, are entrusted with confidential or sensitive information.

This Policy addresses all aspects of information security and continuity from initial design of a system through implementation and operation. It also addresses any device used to store, process, or communicate <Organization> proprietary or other protected information.

Definitions

Information Owner

Information Owners are the managers who bear responsibility for the acquisition, development, and maintenance of applications that process <Organization> information. All application and company information must have a designated Information Owner. For each type of information, Information Owners designate the relevant sensitivity classification, designate the appropriate level of criticality, define which users will be granted access, and approve requests for various ways in which the information will be utilized.

Custodians

Custodians are in physical or logical possession of either <Organization> information or information that has been entrusted to <Organization>. While System Administrators are Custodians, whenever information is maintained only on a personal computer, the User is also a Custodian. Custodians are responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and making backups so that critical information will not be lost. Custodians are also required to implement, operate, and maintain the security measures defined by Information Owners.

Information Users

Information Users (“Users”) include all employees of <Organization> who access or receive information produced, stored, or communicated by <Organization>’s information technology systems. Users also include all individuals, who by nature of their relationship with <Organization> (e.g., contractors, vendors, service providers, consultants, etc.) are entrusted with sensitive or confidential information. Users are responsible for compliance with the Information Security Policy and individual Standards and Procedures.

Policy Requirements

Security Management

The security of corporate information, applications, systems, and networks is fundamental to the continued success of <Organization>. Security management seeks to establish controls and measures to minimize the risk of loss of information and system resources, corruption of data, disruption of access to the data, and unauthorized disclosure of information. Security management is achieved through effective policies, standards, and procedures that will ensure the confidentiality, integrity, and availability of <Organization> information, applications, systems, and networks for authorized Users.

Confidentiality

Confidentiality relates to the protection of information from unauthorized access regardless of where it resides or how it is stored. Information that is sensitive or proprietary needs to be protected to a higher level than other information. Policies are in place to identify what information is confidential and the period of time it should remain confidential. The

Information Classification and Handling Policy provides a framework for classifying the confidentiality of data according to its characteristics and indicates associated security requirements for each confidentiality ranking.

Integrity

Integrity is the protection of information, applications, systems, and networks from intentional, unauthorized, or accidental changes. It is also important to protect the processes or programs used to manipulate data. Information should be presented to Information Owners and Users in an accurate, complete, and timely manner. The key to achieving integrity is identification and authentication of all Users accessing information, applications, systems, and networks through the use of manual and automated checks. Employees must not take any action that could compromise the integrity of the information, application, system, or network.

Availability

Availability is the assurance that <Organization> information and resources are accessible by authorized Users as needed. There are two issues relative to availability: denial of services caused by a lack of security controls (e.g., destruction of data or equipment, computer virus), and loss of services from information resources due to natural disasters (e.g., storms, floods, fires). Loss of services is addressed as part of the Business Continuation Planning process. The Business Continuity Plan provides a framework for classifying the availability of data according to its characteristics and indicates associated security requirements for each availability ranking.

Authentication

Authentication requires that the origin of a message be correctly identified with assurance that it is not a false or forged identity. Passwords are used to authenticate a User based upon the fact that only the User should know the password. Strong passwords will be used and must contain a number of rules such as combinations of letters and numbers with combinations of upper and lower cases. One-time passwords will also be implemented for high-risk applications as well as encryption to provide the authentication security service to identify the origin of messages.

Information Assets

All information, data, applications, networks, and equipment are the property of <Organization> and are provided to its employees so that they can conduct their job responsibilities effectively. These assets should be treated with privacy and confidentiality when conducting business and should not be made available or accessible to anyone outside the enterprise without specific written permission of the Chief Information Officer.

<Organization> information and information processing infrastructure are vital assets requiring protection commensurate with their value. Organizational information, applications, systems, and networks must be actively managed to ensure security, confidentiality, integrity, and availability.

Accountability

<Organization> administrative and computing environments will maintain consistent standards for establishing the accountability and authenticity of system Users, which will be compatible with internal accounting control standards prescribed by <Organization>.

These environments will develop unique standards for protecting information, applications, systems, and network resources contained within these environments that will be commensurate with fulfilling the mission of <Organization> and maintaining the integrity of those critical resources.

To maintain accountability for system access, <Organization> will implement the following:

- All individuals with access to the systems will use a User ID that has been authorized by company management and specifically assigned to that individual. Sharing of User IDs is prohibited except in specific, approved situations.
- All individuals with network, system, and application User IDs will retain a confidential password that will be used to authenticate the identity of the individual. Intentional disclosure or sharing of passwords is prohibited.

Information Access

All access to information is to be authorized by responsible management, with access granted or revoked based on business requirements only. Access to administrative data will be granted to <Organization> employees only. Individuals outside of <Organization> can be authorized access to <Organization> data only if that authorization is granted by the Information Owner.

Access and update capabilities/restrictions will apply to all <Organization> data, stored company computing facilities. Security measures apply to all systems developed and/or maintained by <Organization> organizations, affiliates, outside vendors, or contractors.

The appropriate Head of Business Unit and the System Administrator are responsible for authorizing access to systems and information, verifying information integrity, and controlling extracted information. Management is responsible for developing secure processing systems and operating these systems in a controlled environment. Employees are required to comply with management's direction for the use and protection of information technology processing systems and information. Employees must be kept aware of the importance of information security. All managers and employees are required to act with urgency and diligence to fulfill these requirements.

Risks must be evaluated to determine the optimum level of control required for each type of information technology system. Adequate controls are to be included to ensure that information security, confidentiality, integrity, and availability are achieved.

Policy Responsibilities

Security Officer

The Security Officer of <Organization> has overall responsibility for information security matters. These responsibilities are to:

- Ensure appropriate User access and authentication controls are in place.
- Ensure that the documented security policies, standards, and procedures are reviewed, updated, and maintained periodically by appropriate individuals.
- Evaluate security exposures, misuse, or non-compliance situations and ensure implementation of security controls to address those incidences.
- Ensure that employees execute their security responsibilities in accordance with related policies, standards, and procedures.
- Develop and implement the Security Awareness Program

Information Resources

Information resources including computer software and support systems should be protected appropriately to maintain the sensitivity and critical nature of information that is processed, stored, or communicated. Information systems should be protected in such a manner to ensure that unauthorized persons are not able to directly access the device and either cause physical damage or modify internal components that could affect the results of computing or other processes. Environmental and security controls should be appropriate for the level of risk. An assessment that balances risk with the cost of implementing the control should be completed when determining what security and environmental controls are appropriate.

Users are responsible for adhering to copyright, patent laws, and license agreements for intellectual property.

Communication facilities and equipment should be protected from unauthorized modification and tampering to ensure that messages in transit are not modified or received by unintended parties or that communication services are not interrupted. Communication facilities can include all equipment rooms and wiring closets and may include facilities and resources provided by third-party service providers.

Questions concerning the appropriateness of physical and environmental controls should be addressed to the Security Officer.

System and Information Ownership

<Organization> is the owner of all information, applications, systems, and software that are developed, used, or distributed to employees or designated representatives of entities operating as business partners. Although <Organization> maintains the ultimate ownership responsibility, certain managers are responsible for executing this responsibility.

Systems and information owners are responsible for identifying and managing risks relating to the security, integrity, and continuity of information, and for the business processes and system functions that create, modify, delete, or use this information. They are responsible for assessing the level of risk to <Organization> for providing access to information, as well as for determining the impact to the organization if information, business processes, or system functions were not available or if they are misused.

The level of security, integrity, and continuity risk needs to be communicated by the owner to individuals or groups responsible for implementing <Organization> security and business continuity controls.

Periodically, the Information Owner and the Security Officer will review the current set of accesses and update capabilities granted to each individual on the system in order to ensure that the appropriate level of access has been granted and that no changes are necessary.

Access to Systems and Information

All access to systems and information is provided based on business need. Information owners, as part of their management responsibility, are required to authorize requests for access to information or systems, and to verify that such access meets a legitimate business need, prior to access being implemented.

An Access Request Form will be completed and will indicate the system or information access that the User should be permitted. This form will be authorized by a Head of Business Unit or the Information Owner as required.

Access to sensitive information needs to be restricted. Owners may also designate a retention period during which the information or access may be authorized and after which all access is to be revoked.

When approval for outside access to <Organization> information is granted, instructions must be provided to the recipient notifying them of any security requirements, including the need to maintain the confidentiality of the information, requirements for distribution of the information within their organization, and procedures for destruction or return of the information following the period of access. All non-employees will sign a Non-disclosure Agreement.

All employee, contractor, vendor, and consultant User IDs must be disabled without delay upon their leaving the company.

When a Head of Business Unit is notified of an employee termination/resignation, they should review the disposition of the User's data and files with the User prior to separation from <Organization>.

Security Monitoring and Enforcement

It is the responsibility of the Security Officer to implement appropriate measures to detect attempts to compromise the security or integrity of information or information technology systems. When implementing monitoring capabilities, consideration should be given as to what situations are to be monitored based on the extent of risk, the most effective means for monitoring security activities, the resources available for monitoring, and system constraints that limit the ability to monitor security events. If appropriate measures are not available within a system environment to effectively monitor security events, additional controls to mitigate security risks should be implemented.

When activity occurs that is in conflict with security policies and standards, Head of Business Units should take the appropriate steps to enforce desired security practices. The steps involved range from training of the Users, revoking access, altering security parameters and possibly disciplinary actions.

Due to the likelihood of damage and destruction of information resulting from malicious code, including viruses, detection capabilities must include malware detection software within the local area network environment, as well as on systems that are at high risk for infection.

The facts surrounding an intrusion, infection, or system compromise must be documented, reported to the Security Officer, and include the circumstances that led to the discovery of the incident, actions which were immediately taken, the names of persons involved in investigating the incident, and detailed observations about what transpired, what damage was caused, and what systems or files were compromised.

Security Awareness Program

It is the responsibility of management to ensure that all Users of information understand how to protect company assets, including information and information resources and comply with security policies, standards, and procedures. Supervisors and managers must ensure that persons working within their department understand general information security requirements and they are sufficiently knowledgeable about the information technology security policies, standards, and procedures to recognize the need for protecting information and the requirements for which they are specifically responsible.

The Security Officer is responsible for developing and implementing an Information Security Awareness Program that supports employee awareness. Managers need to be aware of User performance in this area, encourage good security practices, and address inappropriate behavior.

Computer Security Incident Response

<Organization> shall develop effective plans and procedures for responding to suspected information security incidents that affect the confidentiality, integrity, or availability of data processed or owned by <Organization> or for which <Organization> serves as a custodian.

These plans and procedures shall address the following stages of incident response:

a. Preparation
b. Detection and Reporting
c. Analysis
d. Containment
e. Recovery
f. Post-Incident Activities

Disaster Recovery/Business Continuity Planning

It is the responsibility of management to ensure that planning and preparation is performed to minimize loss, reduce impact, and ensure continuity of the organization's functions and revenue stream. A Business Continuity Plan (BCP) will be developed and tested for effectiveness. The BCP will address pre-planning risk control, crisis management, and business recovery.

Compliance

<Organization> complies with all applicable federal, state, provincial, local, industry and contractual regulations.

Non-compliance or violation of this policy should be brought to the immediate attention of the Security Officer. The Security Officer will work with company management and System Administrators to ensure that the problem is resolved and to address necessary steps to eliminate future violations. An escalation process will define the course of action for all violations consistent with the severity of the violation.

<Organization> reserves the right to discipline, terminate, suspend, or prosecute, at its discretion, individuals who violate the information Security Policy.

Service Delivery

<Organization> promotes secure practices in delivery of its products and services through awareness, training and generally accepted security practices.

Physical and Environmental Security

<Organization> maintains controls to limit access to physical assets and mitigates risks associated with environmental issues (fires, floods, power loss) to help ensure data protection and system availability.

Delivery Partner Management

<Organization> ensures processes exist to evaluate the service capability of potential business partners through:

- Non-disclosure agreements
- Due diligence, including references, accreditations, etc.

<Organization> monitors partners and suppliers to ensure defined service objectives are met.

<Organization> ensures processes exist for vendor termination that provide minimal disruptions and maintain data confidentiality.

Additional Policies

[Instructions] You can attach additional issue-specific policies to this Security Policy and list them below. A list of possible issue-specific policies is shown.

The following policies pertain to specific topics or issues and are attached. These issue-specific policies shall be considered part of this Security Policy and are subject to the same provisions:

a. Acceptable (Computer) Use Policy
b. Desktop Configuration Policy
c. Remote Access Policy
d. Information Lifecycle and Disposal Policy
e. Laptop and Mobile Device Policy
f. Backup and Disaster Recovery Policy
g. Business Continuity Policy
h. Physical Security Policy
i. Wireless Network Security Policy
j. Password Policy
k. Personnel Security policy
l. Update / patching policy
m. Web application policy
n. Incident Response Policy
o. Privacy Policy

Policy Review

This policy and supporting Information Security policies will be reviewed annually and updated as required.