Key CONFERENCE

Information Technology Security Policy

Introduction

Preamble

Policy

Introduction

Key Conference Solutions (the company) acknowledges an obligation to ensure appropriate security for all Information Technology data, equipment, and processes in its domain of ownership and control. Every employee of the company shares this obligation, to varying degrees.

The Preamble section of this document sets the context for IT security within the company by:

- listing the elements that constitute IT security;
- explaining the need for IT security;
- specifying the various categories of IT data, equipment, and processes covered by this policy; and
- indicating, in broad terms, the IT security responsibilities of the various roles in which each employee of the company may function.

The Policy section provides a high level statement of measures and controls to protect corporate information. It is a statement of principles. Detailed standards and procedures derived from this Policy will be contained in associated documents.

Preamble

1. Scope of IT security

Security can be defined as 'the state of being free from unacceptable risk'. The risk concerns the following categories of losses:

- confidentiality of information
- integrity of data
- assets
- efficient and appropriate use
- system availability.

Confidentiality refers to the privacy of personal or corporate information.

Integrity refers to the accuracy and completeness of data. Protection is required against deliberate or accidental corruption of data.

Efficient and appropriate use ensures that company IT resources are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others.

Availability is concerned with the full functioning of a system and its components.

The potential causes of these losses are termed 'threats'. These threats may be human or non-human, natural, accidental, or deliberate.

The IT Security Policy will deal with the following domains of security:

- **Computer system security** Processor, peripherals, operating systems and applications. This includes information security.
- **Physical security** Premises occupied by IT personnel and equipment or used for data storage.
- **Operational security** Environment control, power equipment, and operational activities.
- **Procedural security** By IT staff, vendor staff, management personnel, as well as company employee users.
- **Communications security** Communications equipment, personnel, transmission paths, and physical infrastructure.

2. Policy objectives

Confidentiality of information is imposed by common law, formal statute, explicit agreement, convention and for the maintenance of good will. Different classes of information warrant different degrees of confidentiality.

The use of company IT assets in other than a manner and for the purpose for which they were intended represents a misallocation of valuable resources, and possibly a threat to the company’s reputation or a violation of the law.

Additionally, proper functioning of IT systems is required for efficient operation of the company. A number of corporate systems, such as the Personnel/Payroll, Finance, Research systems are of paramount importance to the mission of the company.

The IT Security Policy is developed to support these principles.

The objectives of the IT Security Policy are:

- to secure the company’s assets against theft, fraud, malicious or accidental damage, breach of privacy or confidence
- to protect the company from damage or liability arising from the use of its IT facilities for purposes contrary to the law or the company’s Standard Operating Procedures

This Policy operates in conjunction with all statutory and common laws, and company policies and procedures.

3. Roles and responsibilities

3.1 Policy Management

Approval of the IT Security Policy is vested with the company Directors.

Formulation and maintenance of the policy is the responsibility of the Information Technology Manager.

3.2 Policy implementation

Each employee of the company will be responsible for meeting published IT policies and standards.

The implementation will be guided by various policy documents appended to this policy.

3.3 Custodians

The 'custodian' is the person or employee responsible and accountable for a particular system.

The various company custodianship responsibilities are as follows:

- the Information Technology Manager will be the custodian of the infrastructure for all corporate systems
- the Information Technology Manager will be custodian of all global web servers
- Individuals employed by the company will be custodians of desktop systems (personal computers, associated storage media and telephone handsets) allocated for their exclusive use.

IT security for each system will be the responsibility of its custodian under the direction and guidance of the Information Technology Manager, who will be responsible for developing and/or implementing the system's security plan.

It is the duty of each custodian to take appropriate action to ensure compliance and prevent breaches of the Policy. Where such action is outside the authority of the custodian, the custodian will notify the Information Technology Manager.

3.4 Individuals

All users of company IT resources:

- will operate under the provisions of the IT Security Policy and appended policy documents.

- are responsible for the proper care and use of IT resources and information under their direct control.

3.5 Standards and procedures

Standards and procedures will be published by the Information Technology Manager to assist users and system custodians to meet their IT security responsibilities. These standards, though presented separately, are an integral part of the company's IT Security Policy and therefore define it in detail.

3.6 Training

The level of security that can be implemented within the company depends to a large extent on the understanding and cooperation of all employees. Effective security is dependent on employees awareness and training.

4. Policy documentation

4.1 Documents

The company's IT security standards and guidelines are defined by various documents, including:

- IT Security Policy
- IT Security Policy - Backup
- IT Security Policy - Incident Response
- IT Security Policy - Passwords

Additional documentation relating to the IT security standards will be published by the Information Technology Manager from time to time. The above list is not exclusive.

There are a number of related company policies and State / Commonwealth statutes that should be read in conjunction with these documents. These include but are not limited to Passwords Security, Intellectual Property, Copyright, Information Privacy, Privacy of Client Records, Privacy Act and Electronic Mail policies.

Policy

5. Measures and controls

5.1 Access to systems

All individuals who require access to system and information resources shall be properly identified, by means of a unique personal identifier.

Appropriate access control shall be introduced into every IT system, with two objectives in mind:

- preventing intruders from entering and misusing the system; and
- constraining the authorised users to their legitimate purposes.

Formal procedures shall be established to define how additions, deletions, and other modifications to user access and privileges are to be performed.

Authorised users of IT systems must:

- be aware of their responsibilities and what they are authorised to do;
- have an expectation of detection if they abuse their privilege; and
- have their access privilege(s) removed as soon as it is no longer needed.

5.2 Authentication policy

All users shall have their identity verified by an authentication mechanism, which may be by their unique personal identifier and a password, or other means that provide equal or greater security, prior to being permitted to use IT resources.

5.3 Inactivity period

If there has been a period of inactivity on a desktop computer or terminal, the system must automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided the proper authentication. When sensitive systems are resident on desktop computers, authentication shall also be required when the computer is powered on or restarted. All corporate applications will incorporate automatic time-out of logins after an appropriate period of inactivity.

5.4 Protection against malicious software

The Information Technology Manager is responsible for procuring and facilitating the distribution of anti-virus software throughout the company.

Users are responsible for ensuring that virus checking and eradication takes place on systems for which they are the custodian.

To decrease the risk of the action of malicious software and to limit its spread:

- all software, data and attachments must be checked where practicable for viruses before installation;
- the provided software tools must be used to detect and remove viruses; and
- systems that are shown to be infected shall be isolated as quickly as practicable and until removal of the malicious software takes place.
- Report any incident of infection or suspicious activity to the Information Technology Manager immediately.

5.5 Software licences

The company and all employees are responsible for complying with the Commonwealth Copyright Act and with the terms and conditions of the particular contracts or software licences relating to purchased, leased or acquired hardware and software. In particular, copying software without authorisation from the copyright holder is a breach of the Act.

5.6 Acceptable use

The company Rules of Usage contained in the IT Security Plan document define the appropriate use of IT resources. Users are required to read and agree to abide by these Rules.

If, as an agent/representative of the company, the user has been granted access to external systems, the user agrees to abide by the rules of the remote site.

5.7 Backup

All sensitive, valuable, or critical information resident on company IT systems shall be periodically backed-up.

An appropriate regular back-up schedule shall be implemented to protect all data and software. A sufficient number of backups of all data and software shall be stored off-site to protect against major damage occurring at the primary location.

(*Refer to Backup section in IT Procedure Manual*)

5.8 Disaster recovery and business continuity planning

Adequate measures shall be in place to prepare for and cope with disaster and to facilitate the resumption of business services in the event of a disruption and to minimise threats to the company’s information assets.

The custodian is responsible for ensuring a Business Continuity Plan (BCP) is implemented for each system taking into account the risk assessment, the company's needs and vulnerabilities. The BCP shall be documented and tested periodically.

5.9 Change management

Change control procedures shall provide a formal approach to the management of change enabling individual changes to be applied in a controlled and consistent manner.

A change control process must be used to ensure that all software, hardware, communications links and procedures move into production only after receiving proper authorisation from the system custodian and systems manager.

5.10 Authority for monitoring activity

Users have a legitimate expectation to privacy in the carrying out of approved activity. However, the company also has a right to inspect any data on a computer system connected to the company resources (regardless of data or system custodianship), to prevent, detect or minimise unacceptable behaviour on that computer system, and to provide to any authorised employee of the company, or law enforcement bodies, any information it possesses regarding the use of the company's resources. Where such action is taken, users who have data inspected, and are found to be conforming to this policy, have a legitimate expectation that confidentiality will be preserved.

As part of the security procedures, access to systems must be monitored on a continuing basis and audit trails or access logs maintained of this access.

The Information Technology Manager will authorise specified staff whose duties include monitoring the use of IT facilities to investigate the suspected security breaches or unauthorised access.

5.11 Physical security

Physical security of IT facilities is necessary to prevent their unauthorised use and to ensure that systems are adequately protected against natural hazards, theft and damage.

Access to every office, computer room, and work area containing sensitive information, or the means to access such information, shall be physically restricted.

Rooms and facilities which house non-public IT resources shall be protected with physical security measures that prevent unauthorised persons from gaining access.

5.12 Risk Management

- A thorough analysis of all company information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats – internal or external, natural or manmade, electronic and non-electronic-- that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities within each entity which potentially expose the information resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection. From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined. The frequency of the risk analysis will be determined by the Information Technology Manager.
- Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

5.12 Training

To assist staff to gain an understanding of how system security can be maintained and enhanced it is necessary to:

- define security policies and procedures for personnel;
- provide education and appropriate supervision; and
- ensure an understanding of confidentiality requirements.

All aspects of IT security shall be incorporated into formal staff induction procedures for all new staff and be conveyed to existing staff on a regular basis.

5.13 Periodic management review

Regular auditing procedures shall be carried out on all computer systems to check for conformance to policy, and to satisfy the requirements of the company’s internal and external auditors. The depth and regularity of each level of audit should be outlined in the system procedures manual.

The Information Technology Manager shall periodically review the adequacy of information system controls as well as compliance with such controls.

The Information Technology Manager is responsible for the maintenance of the security measures documented in each system's security plan, and shall conduct regular checks to ensure that the measures are being followed.

5.14 Availability

The IT Security Policy will be publicly accessible both in hardcopy form and via the company website. The version on the website is deemed to be the current revision of the Policy. There is a requirement that all users of company IT resources be familiar with this policy.

5.15 Amendments to policy

The IT Security Policy is an evolving document that will be amended as required to deal with changes in technology, applications, procedures, legal and social imperatives and perceived risks. All amendments or changes will be approved by the Information Technology Manager.

Additional, related and supporting documents as defined in section 4.1 are also evolving documents. Their content is more specific and technical and potentially more dynamic, and changes will be approved by the Information Technology Manager.

6. Policy violation

Incident response procedures shall be developed for each system to cover breaches of security and their consequent impacts.

Action to correct and recover from security breaches shall be defined so that:

- only authorised staff are allowed access to systems and data;
- all emergency actions taken are documented in detail;
- emergency action is reported to management; and
- the integrity of business systems and security controls is confirmed with minimal delay.

All users shall be made aware of the procedures for reporting an incident and be required to report any observed or suspected incidents as quickly as possible to the correct authority. A formal reporting procedure shall be established together with an incident response procedure.

The company shall refer any incident involving a possible breach of State, Federal or International law to the appropriate authority for investigation. The company will give that authority all reasonable assistance.

If a security breach involves facilities strictly internal to the company, the appropriate disciplinary procedures shall be followed. In the case of serious breaches of this policy by staff, disciplinary procedures for 'misconduct' or 'serious misconduct' may lead to sanctions being imposed, including termination of employment.

If a security breach occurs in which a person or organisation external to the company is involved as a potential victim of the breach, the company shall refer to the external party the details specific to that party.

Procedures shall be established, documented and maintained for establishing the cause of any security breach, whether accidental or deliberate, the corrective action to be taken, and any recommendations on preventing a recurrence. Controls will monitor the implementation and effectiveness of any corrective action, including any required changes to existing procedures.

7. Review of Policy

This policy shall be reviewed by the Information Technology Manager, annually or when required in light of changing circumstances to ensure that the Policy is appropriate for the protection of the company and client interests.