Information Technology Security Policy – Acceptable Use

To be read in conjunction with IT Security Policy

IT Acceptable Use and Security Policy

Overview
Scope and Application
Policy Principles

1. Acceptable and Unacceptable Use of IT Facilities
2. Access and Accounts
3. Security of IT Facilities
4. User Responsibilities
5. User Responsibilities and Monitoring of IT Facilities
6. Consequences of Non Compliance

Definitions

Overview

Key Conference Solutions seeks to provide its staff, clients, and other authorised users with secure and timely access to IT equipment and the online services and resources necessary for undertaking their work. Consequently the company is highly reliant on information that is gathered, stored, processed and delivered by computers and their associated communications facilities. The purpose of this Policy is to give a clear statement to all users of company IT facilities and services of their responsibilities, including what constitutes acceptable and unacceptable use; to manage the provision and modification of access to online services; and to express the commitment of the company to providing and maintaining a secure, effective and reliable IT infrastructure to support the company's operations.

Scope and Application

This Policy applies to all users of company IT facilities and services, whether the facilities are managed by the company, or by third-party providers under contract to the company.

Policy Principles

1. Acceptable and Unacceptable Use of IT Facilities and Services

a) Company IT facilities and services are provided for use in administrative and commercial activities of the company. Some reasonable non-commercial personal use may be allowed, but as a privilege and not a right, and if that privilege is abused it will be treated as a breach of this Policy. The Information Technology Manager remains the arbiter of ‘reasonable’.
b) Use of company IT facilities and services must not jeopardise the fair, safe and productive IT environment of the company, nor the company's operations, assets and reputation.
c) Company IT facilities and services must not be used unlawfully or for an unlawful purpose.
d) Specific user responsibilities are set out in section 4 of this Policy.

2. Access and Accounts

a) All company staff are entitled to access to the company IT facilities and services, at a level appropriate to their position and role, via a unique password protected account.
b) Select company clients are entitled to access company IT facilities and services, at a level appropriate to their contractual requirements, via a unique password protected account.
c) Some IT facilities provided for the general public do not require a unique account to enable access.
d) The Information Technology Manager may provide access to company IT facilities and services to approved third parties. Access for personnel of an approved third party must be authorised in accordance with procedures agreed between the company and that third party.
e) The company may impose quotas on the use of company IT facilities and services (including print, file storage, email and internet download) and will revise them as necessary. Where quotas exist, authorised users are expected to comply with them. If an account holder exceeds any of their quotas, they may be personally charged for the cost of their use and/or temporarily prevented from using the affected IT facility.

f) When account holders no longer have a relationship with the company or are no longer authorised to have access to company IT facilities and services, their accounts will be disabled for a set period, and then deleted.

g) Account holders may have their IT access suspended immediately where there is a suspected breach of company IT Security Policy.

3. Security of IT Facilities and Services

a) The company will take all reasonable steps to protect its IT facilities and services from unauthorised and unacceptable use.

b) The Information Technology Manager is responsible for the implementation and management of this Policy in relation to IT facilities owned and operated by the company.

c) To preserve the company 's standard operating environment and ensure compliance with licensing obligations, users of company IT facilities and services may only modify the standard configuration of any of the company's IT facilities and services, after first gaining approval from the Information Technology Manager. Users must never install or use unlicensed or malicious software on company IT facilities and must not connect unapproved networking devices to the company IT infrastructure.

d) Users of company IT facilities and services must not circumvent the company 's authorised internet connections or subvert its IT security measures.

e) All company IT hardware, especially portable devices, must be kept secured at all times against damage, misuse, loss or theft. In addition, hardware and software containing sensitive information or data must be protected with appropriate security measures such as passwords and encryption.

f) Company IT hardware that becomes obsolete must be disposed of in a manner that renders any information illegible and irretrievable at the time of disposal.

g) All account holders must;

- not use their access to company IT facilities and services to gain any inappropriate personal, or other advantage,
- not manipulate company data without authorisation, and
- maintain the confidentiality of any personal or confidential information accessed via company IT facilities and services.

4. User Responsibilities

a) It is a condition of use of company IT facilities and services that this Policy, particularly the principles of acceptable and unacceptable use, and its associated Procedures must be complied with.
b) All account holders are responsible for all activity initiated from their account, must only access company IT facilities and services using their own account, and must ensure that their passwords are securely stored.
c) Users of company IT facilities or services provided by a third-party provider on the company's behalf must comply with any terms and conditions issued by that third-party provider.
d) Users of company IT facilities and services must not create, send, store, upload, access, use, solicit, publish or link to;

- Offensive, obscene, profane or indecent images or material (other than for properly authorised, supervised and lawful purposes, in which case an appropriate warning must be given).
- Material likely to cause annoyance, inconvenience or distress to some individuals or cultures.
- Discriminating or sexually harassing material or messages that create an intimidating or hostile work or study environment for others.
- Defamatory material or material that makes misrepresentations or could otherwise be construed as misleading.
- Material that infringes the intellectual property (including copyright) of another person or organisation.
- Malicious software such as viruses, worms or address-harvesting software.

e) Company IT facilities and services must not be used in the conduct of personal business or unauthorised commercial activities.
f) Company IT facilities and services must not be used for any illegal activity such as sending chain letters, sending SPAM, or attacking other computer systems.
g) Employees must include the appropriate sections of the company's official signature and disclaimer on all email messages sent.
h) Electronic materials must never be forwarded without the express or implied permission of the material's creator.
i) Peer-to-peer software must only be used for lawful purposes authorised by the Information Technology Manager.
j) Any observed security weakness in, or threat to, company IT facilities and services and any known or suspected breach of this Policy and its associated Procedures must be reported as soon as practicable to the Information Technology Manager.
k) Where use of company IT facilities and services would ordinarily breach this Policy, but the use forms a legitimate part of the user's employment or research, an

exemption may be granted from compliance with this Policy by the Information Technology Manager.

5. Company Responsibilities and Monitoring of IT Facilities

a) The company will manage account holders' accounts, maintain a secure IT environment and keep users of company IT facilities and services informed of their user responsibilities and expected best practice standards.
b) The company reserves the right to investigate any and all aspects of its electronic information systems if it is suspected that any user of company IT facilities and services is acting unlawfully or violating this Policy or any other company Policy.
c) The company reserves the right to monitor, log, collect and analyse the activities of account holders in their usage of IT facilities and services
d) The Information Technology Manager may take any action considered necessary to remedy immediate threats to the IT infrastructure or security, including suspending authorised accounts and/or disconnecting or disabling relevant IT facilities or other equipment, with or without prior notice.
e) The company reserves the right to carry out security audits on company IT facilities and services.
f) The company reserves the right to block or filter any network traffic that potentially breaches this policy or is potentially illegal.

6. Consequences of non compliance

a) Minor breaches of this Policy will be addressed by sending emails to users requesting that they desist from the breaching behaviour, as specified in the IT Security Policy.
b) Ongoing or serious breaches of this Policy or related IT Policies by employees or other authorised users will be addressed by the relevant disciplinary procedures.
c) If a breach of this Policy appears to constitute an offence under State or Commonwealth law, the company may (and in some cases is obliged to) refer the suspected breach to the appropriate law enforcement agencies.
d) Accounts may be suspended upon approval by the appropriate delegation holder.

end