Information Technology Security Policy – EMAIL

To be read in conjunction with IT Security Policy (as amended)

Email Management requirements for KCS Management, Staff and Authorised System Contractors

Introduction

An electronic mail message or email is probably the most frequently used form of communication by KCS owing to the ease and speed of sending and receiving information electronically. The growth of this form of communication underlines the fact that electronic mail messages, like all forms of records, must be managed in accordance with the business needs of a professional business organisation. Records provide information about and evidence of company and client activities, decision-making and accountability. It is crucial that all KCS staff and contractors adhere to good information/records management practices and be familiar with the applicable legislative and policy requirements for the management of such records.

Purpose

The purpose of this document is to provide guidance to KCS Staff and Contractors (including Managers), on the management of email as records of the company.

Scope

This document applies to all KCS Staff and Contractors.

Definitions

- Electronic mail (email) messages are communications, sent or received internally or externally on an electronic mail system, and include any attachments transmitted with the message as well as the associated transmission and receipt data.
- Record includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine readable record, and any other documentary material, and any copy thereof.
- Spam mail is unsolicited commercial email (UCE) which is also known as bulk email, or commonly - junk mail.
- Transitory Records are those records that are required only for a limited time to ensure the completion of a routine action or the preparation of a subsequent record.

Guidelines

1. Most email messages are records

Email messages, including any electronic attachments, created, collected, received or transmitted in the normal course of company business which reflect the functions, business activities, and decisions of KCS are *records*.

A record is under the control of the company when the company is authorised to grant or deny access to the record, to govern its use and, subject to the approval of the Directors, to dispose of it. Regarding the question of physical possession, a record held by KCS, irrespective of the location at which that record is held, is presumed to be under its control unless there is evidence to the contrary. A record held elsewhere on behalf of KCS is also under its control, for example at an employee's or contractors home.

Since most email messages are records, they must be managed in accordance with all applicable legislation and federal government policies such as the relevant *Privacy Acts*, and any other legislation either state of federal.

2. Email records relating to the business of an institution must be kept

- Email messages created, collected, received or transmitted during the normal course of business are *records of the company*. Such messages and their attachments reflect the functions, business activities, and decisions of the company. They must be kept to ensure the integrity of the corporate memory of the company.
- Email messages of a transitory nature are permitted to be deleted and should be deleted once they have served their purpose. Transitory email is defined as

forwarded email; spam mail (junk mail); information in the form of casual communication; process versions of electronic information that were not communicated outside of the creating office; electronic versions of documents used for information, reference or convenience only or draft versions of documents where annotations and additional records are incorporated into subsequent versions. Electronic documents used to produce a hard copy version maintained in hard copy files should also be considered to be transitory however e-records are the preferred record.

- Email messages whose content is of a personal nature are not records of the company and therefore are not covered by this Procedure Policy. Examples include email messages regarding arrangements for lunch, an employee's personal information such as email relating to hobbies, extracurricular activities, announcements, unsolicited advertising, etc. Such messages should be deleted once their usefulness is completed. However, a user must not delete records where the institution has received a formal request, under any State or Federal legal requirement, formal request, or demand by way of court order, relating to these records.

3. Email messages must remain intact

Where electronic messages and their attachments pertain to the business of KCS, they must remain intact in terms of their structure (layout or format and links to attachments and related documents), content (the information contained in the message) and context (information pertaining to the sender and recipients as well as any header information and transmittal data such as time and date). This is to ensure they retain their value as evidence of company business. Additionally, these messages must be protected against unauthorised access, use, manipulation, destruction or loss.

4. Email messages should be captured into a recognisable records system

Electronic messages relating to the business of the company should be filed pursuant to the records management practices of the company. The IT Manager (as nominated by the Directors) is responsible for records systems and advising all users how to file their electronic messages, attachments and other corporate documents.

If a corporate electronic records system exists within the company, email messages created/received in the course of company business should be filed electronically to the corporate system. If no electronic records system exists the email messages should be forwarded either electronically or as a printed hard copy, depending on advice from the company IT Manager for inclusion in the existing corporate records management system. If a user has a large quantity of email messages not yet in the company's record keeping system, they should contact the IT Manager to discuss approaches to managing the situation.

5. Email messages must be managed efficiently and effectively

Electronic messages must be managed in accordance with good information/records management practices in order to preserve the integrity of the record, meet the business needs of the company, and comply with accountability requirements.

Good information/records management practices for the life cycle of the record will ensure that electronic messages remain accessible, i.e. retrievable and readable, over time. Email messages must also be protected to safeguard unauthorised disclosure of sensitive or personal information. It is also important to note that records, **including email**, cannot be destroyed by individuals or institutions within SEVEN YEARS of its creation date.

6. Privacy and Security measures must be applied

Users of electronic mail systems should not assume or have an expectation of privacy or security of their email.

Commercially sensitive information must be protected, and access to it controlled. Where company email systems do not have enabled security features, classified or protected email should not be sent. When in doubt, the IT Manager should be consulted.

7. Roles and Responsibilities of:

Individual Users

- All users including staff and contractors are responsible for distinguishing between electronic messages relating to the official business of the company and those relating to activities of a personal nature. The latter should be deleted once their usefulness has passed.
- Any person acting on behalf of the company will employ means and processes provided by the company exclusively. The use of personal email accounts is prohibited unless a written direction approving such use is provided by the IT Manager.
- Staff are responsible for forwarding email relating to the business of the company into the corporate records system as required and defined by the IT Manager.
- If users have any doubts about the value of an email message as an official record, they should contact the IT Manager for advice. It is better to retain such a message than delete it and lose potentially valuable information, and/or face sanctions for the unauthorised destruction of a record.

The application of effective information management policies will enable the company to meet legislative as well as business and accountability requirements. All staff and authorised users of IT facilities provided by KCS should be familiar with the requirements of this Policy.

8. Breech of Policy

Any breech or event that could reasonably be interpreted as a breech, of the standards, rules, regulations, procedures and requirements as defined by this Policy, or as could reasonably be expected to be interpreted from the intention of this Policy will be referred to the IT Manager immediately. The IT Manager will determine if a breech has occurred and what action will be taken in response to that breech.