



## Council Policy

# IT System Security and Information Management Policy

© City of Albany, 2007

## Objective

The City of Albany's Information Technology system provides the organisation with a framework in which to transmit, store and retrieve data in a digital format. The accuracy, efficiency and reliability of these systems is vital to the City from both an operational and legislative perspective.

Under the State Records Act 2000, the City is required to develop a Record Keeping Plan. At its meeting on 18 March 2008, the State Records Commission approved the City's Record Keeping Plan for a 5-year period (expires March 2013).

The Record Keeping Plan outlines a number of principles and standards that the City's record keeping system is required to comply with. Under Principle Two, the City is required to create a Record Keeping Policy.

Given the synergy that exists between what the Record Keeping Plan is trying to achieve and the objectives of the City's Information Technology Team from a system security perspective, this policy has been created to address the City's legislative responsibilities and to ensure that the City's IT systems remain secure and maintain integrity.

## Scope

This policy applies to all staff, elected members and contractors commissioned by the City to perform functions on behalf of the organisation.

## Definitions

<b>Files/Records/Fields</b>	A format in which digitalised data is stored.
<b>Record</b>	Any record of information however recorded and includes: a) E-mails, faxes, letters, file notes, diaries, calendars and memorandums; b) Anything on which there is writing or Braille; b) A map, plan, diagram or graph; c) A drawing, pictorial or graphic work, or photograph; d) Anything on which there are figures, marks, perforations, or symbols, having a meaning for persons qualified to interpret them; e) Anything from which images, sounds or writings can be reproduced with or without the aid of anything else; and f) Anything on which information has been stored or recorded, either mechanically, magnetically, or electronically.

<b>Significant record</b>	Any record that has administrative, fiscal, legal, evidential, historic or legal value and includes records that: a) Approve or authorise actions; b) Constitute formal communications between staff; c) Constitute formal communications between staff and individuals outside the organisation; d) Signify a policy change or development; e) Relate to significant projects or activities being carried out; f) Contain advice or provide guidance; g) Support a project or activity being carried out by the City.
<b>Transient record</b>	Any record of little value that has a routine or instructional nature and includes: a) Duplicates of documents, without additional notions; b) Copies of another organisation's reports, information and files; c) Telephone messages of a routine or trivial nature; d) Desk calendars and office diaries where no entries pertaining to work activities have been recorded; e) Individual Survey responses where a report summarising all the collated responses has been prepared and stored onto the City's Records System.
<b>Relevant Legislation</b>	a) The State Records 2000 b) Freedom of Information Act 1992
<b>IT</b>	Stands for Information Technology

## Policy Statement

### Internet and Electronic Mail Services

Internet and electronic mail services are provided to employees for organisational purposes only. Employees of the City must not utilise these services to access and/or circulate inappropriate, discriminatory, fraudulent or unlawful material.

### Corporate Ownership

All information created as a result of the City's business activities are corporate assets and as such do not belong to individual employees, contractors or Elected Members. The unsolicited reproduction or transmission of this material to external parties is prohibited.

### System Security

Employees of the City are required to ensure that access to the City's electronic systems is secure. This prohibits sharing passwords, accessing material on storage

devices without scanning for viruses, leaving computer terminals unattended for extended periods and not closing down computers at the days end.

### **Software Development**

Employees of the City are not permitted to develop or install any software, applications or databases without the appropriate authorisation from their manager and the Executive Director Corporate and Community Services.

### **Record Creation and Storage**

Officers, elected members and contractors are responsible for the capture and registration of significant records into the City's Corporate Records Management System. Transient records will be captured at their point of creation and saved to the City's computer network or in hard copy working files. Corporate files/data are not to be stored on a PC's hard drive (e.g. C drive).

### **Guidelines**

The IT System and Security Guidelines define the appropriate use of IT resources. Upon commencement of employment, users are required to read and acknowledge these guidelines prior to system access being granted.

### **Inspection of Information**

The organisation reserves the right to inspect without consent any data on a computer system connected to the City's network. Such inspections will occur to prevent, detect and minimise the unacceptable usage of the corporate computer system.

## **Legislative and Strategic Context**

The State Records Act 2000 and Information Technology Strategy provide both the legislative and strategic context under which this document has been created.

## **Review Position and Date**

Manager Customer Services to review on or before 30/6/2010

## **Associated Documents**

- IT System Security Guidelines
- Records Management Team Procedures
- Records Management End User Procedures
- Registering Email Procedure

CEO Authorisation:  \_\_\_\_\_

Date: 21/10/08