



**CITY OF RICHMOND**

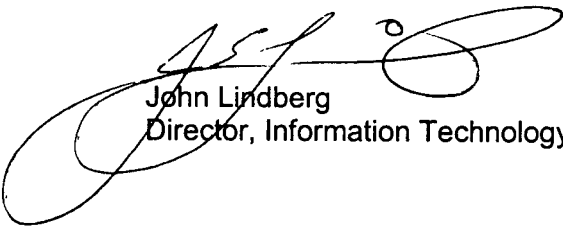
**REPORT TO COMMITTEE**

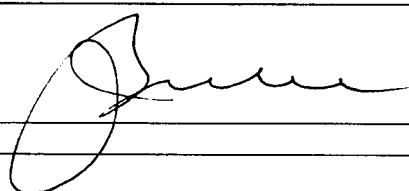
**TO:** General Purposes Committee  
**FROM:** John Lindberg  
Director, Information Technology  
**RE:** Policy and Procedures on the use of Information Technology resources.

*To General Purposes - July 3, 2001*  
**DATE:** June 11<sup>th</sup>, 2001  
**FILE:** - 1300-00

**STAFF RECOMMENDATION**

That Council approve the Policy on the use of Information Technology Resources.

  
John Lindberg  
Director, Information Technology

<b>FOR ORIGINATING DIVISION USE ONLY</b>	
<b>CONCURRENCE OF GENERAL MANAGER</b>	

STAFF REPORT

Not applicable.

ORIGIN

To provide policy and procedures for the proper use of the City's Information Technology Resources as suggested by the KPMG management letter. To also provide the foundation for the employer orientation information package on proper use of the City's Information Technology Resources.

ANALYSIS

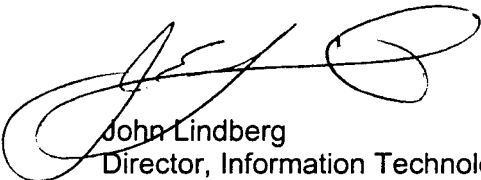
With the continually increasing requirement for city staff to use the city computer resources to fulfill their job functions, guidelines on the proper use of these resources need to be in place. With the city relying in an ever-increasing manner on electronic data and information, security of this information and data must be formalized. It has therefore been determined by the auditors that the authority, responsibility and accountability around the whole Information Technology Resources issues requires to be approved in policy by council and conveyed to all staff to ensure proper security and understanding of the use of the city's resources are in place.

FINANCIAL IMPACT

None.

CONCLUSION

To institute a formal policy approved by council on the proper control and use of the City's Information Technology Resources.



John Lindberg  
Director, Information Technology



## **POLICY**

### **It is Council policy that:**

#### **1. IT Resources:**

- Information Technology Resources includes, but is not limited to computer hardware, software, and services; network systems and services (including Internet connections); printers, modems and other peripheral equipment.
- The Information Technology Resources of the City are to be used solely for the purpose of aiding City staff in fulfilling the responsibilities of their positions as determined by the IT Department in consultation with the operating department.

#### **2. IT Security:**

- All security related to Information Technology Resources is the responsibility of the Information Technology Department. The Information Technology Department shall administer all security and endeavour to provide the highest level of protection for the City's information technology and data assets without creating unreasonable hardships on the legitimate users of those assets.

#### **3. Hardware and Software:**

- All hardware/software and consulting services involving information technology shall first be approved by the Information Technology Department.
- No software or hardware will be purchased for, or installed on the City's information technology resources without prior approval from the Information Technology Department.
- No design or development is to take place on the City's Information Technology Resources, without prior approval from the Information Technology Department

#### **4. Systems Technology:**

- The Information Technology Department will determine the information systems and technology to be supported by the City.



ADMINISTRATIVE PROCEDURE  
TABLE OF CONTENTS

	Page
<b>1. Appropriate Use of IT Resources .....</b>	<b>2</b>
I. Prohibited Activities.....	2
II. E-mail to Send Personal Messages .....	2
III. E-mail Traffic.....	2
IV. Internet Use .....	2
<b>2. IT Security .....</b>	<b>2</b>
I. Classifying Data .....	2
II. Protecting Data .....	2
III. Application Security .....	2
IV. Secured Data from Destruction .....	2
V. Portable IT Assets.....	2
VI. Connectivity to devices .....	2
<b>3. Hardware and Software.....</b>	<b>3</b>
I. Unlicensed Software .....	3
II. Software downloaded from Internet, or by E-mail.....	3
III. Hardware Peripherals .....	3
IV. Test of new Hardware and Software .....	3
V. Level of Support for Software.....	3
<b>4. Systems Technology.....</b>	<b>3</b>
I. Accordance with Resources.....	3
II. Architecture Document .....	4
<b>5. Disaster Recovery .....</b>	<b>4</b>
I. Review of Disaster Recovery Plan .....	4
II. Operational Aspects.....	4
III. Recovery List.....	4
IV. Procedures to recover.....	4
<b>6. Project Management .....</b>	<b>4</b>
I. Project over \$50,000 dollars .....	4
II. Project Owner .....	4
III. Project Manager .....	4
IV. Project Charter.....	4
<b>7. Appendixes .....</b>	<b>5</b>
I. Data Classification .....	5
II. Hardware and Software Classification.....	6



- 1. The purpose of this administrative procedure is to confirm to all City staff what is acceptable and what is unacceptable in using Information Technology Resources owned by the City.**
  - i. The use of Information Technology Resources for purposes other than stated in the policy is prohibited at all times. Prohibited activities include, but are not limited to private business activities; gambling; viewing of pornography, racist, hate, or otherwise offensive materials; and entertainment-oriented multimedia.
  - ii. The City reserves the right to monitor and inspect any activities taking place on City resources, including E-mail traffic, in order to ensure compliance with this policy.
  - iii. The city also reserved the right to monitor E-mail for size and content to ensure system integrity, and to maintain the systems effectiveness.
  - iv. All Internet uses are subject to the same specific prohibitions listed in paragraphs above.
  - v. Non compliance with this policy could result in discipline, up to and including dismissal.
  
- 2. IT Security - To provide a framework for Information Technology security procedures:**
  - i. The Information Technology Department shall devise, and periodically review, a system to classify data depending on need-to-know, and sensitivity.
  - ii. The Information Technology Department will insure all security of records are established and governed in accordance with the freedom of Information and Protection of Privacy Act.
  - iii. The Information Technology Department shall endeavour to protect all classes of data from unauthorised or accidental alteration, deletion, or additions, and virus infection.
  - iv. The Information Technology Department shall endeavour to protect all secured data from unauthorised viewing and control all application security.
  - v. Requests for access or increase access to applications is to be initiated by the user's supervisor to ensure that the access request is based on the user's role and responsibility and to ensure appropriate segregation of duties. User access privileges are reviewed by IT periodically.
  - vi. Final approval of request(s) for access must be given by the manager of the department that owns the data or application.
  - vii. The Information Technology Department shall ensure that all classes of data are secured from destruction as proscribed in the Disaster Policy.
  - viii. Portable IT assets (including laptop computers, personal digital assistants, and computer screen projectors) shall be assigned to a designated custodian, who is responsible for the physical security of that asset.
  - ix. City staff shall not connect, or cause to be connected, any device which provides access to the City's computer network without consent of the Information Technology Department. This includes but is not limited to modems and wireless data transceivers.
  - x. The Information Technology Department will receive all change of status of employment notifications from Human Resources Department to allow proper security access measures



to be taken. (e.g., extended leaves, retirements, termination and resignation of employment).

**Termination of staff's access to IT resources will be as follows:**

**1. For first 6 months**

- NT account will be disabled (in case of rehire)

**2. After 6 months**

- delete home directory
- disable REDMS account
- Delete NT account
- delete mailbox
- remove kixtart entry

Note: This policy restricts login to the system immediately but leaves all information for 6 months on the system. After 6 months, E-mail and home directory material are deleted.

- xi. The Information Technology Department will insure that all archive data and records will be maintained in a manner that insures access will be achievable.

**3. Hardware and Software**

The purpose of this procedure is to provide a framework for IT service levels, establish authority for hardware and software purchases, and set the expectations for all City staff as to the type of support they can receive.

- i. No computer software will be purchased for the City without prior approval from the Information Technology Department.
- ii. No unlicensed software will be installed on the City's Information Technology resources by any person.
- iii. No software downloaded from the Internet or received by E-mail will be installed on the City's Information Technology resources by any person other than members of the Information Technology Department, except when:  
The software contains emergency fixes for software already legally licensed, and said software is authorized by the Information Technology Department.
- iv. No computer hardware (including peripherals) will be purchased for the City without approval from the Information Technology Department.
- v. No hardware will be connected to the City's Information Technology resources without approval from the Information Technology Department.
- vi. The Information Technology Department shall test all new hardware and software for compatibility before approval.



- vii. The Information Technology Department shall not approve hardware or software purchases when existing and available resources with equivalent functionality have already been approved.
- viii. The Information Technology Department shall devise, and periodically review, a system to classify software depending on: breadth-of-use; purpose, type, complexity and revision level of software; prohibited software.
- ix. The Information Technology Department shall post or publish the level of support for each class of software.

#### **4. Systems Technology**

The purpose of this procedure is to provide a framework for describing the technology standards supported by the City's Information Technology infrastructure. While the actual technologies employed and described will change over time, standards provide a basis for the City to evaluate proposed new systems and applications, maintain compatibility with the existing Information Technology infrastructure, minimise support costs, reduce training requirements, and enable the Information Technology Department to commit to service levels.

- i. The Information Technology Department shall devise, post or publish, and periodically review, a Technology Architecture Document, which describes the information technologies that the City supports and uses, or plans to use in accordance with the resources available to the Information Technology Department.
- ii. The Technology Architecture Document shall include, but not be limited to, descriptions of desktop, server, network, database, data exchange, and applications (including, but not limited to, word processing, spreadsheet, presentation, scheduling and E-mail)

#### **5. Disaster Recovery**

The purpose of this procedure is to provide a framework for IT disaster recovery plans and procedures. This would provide guidance for administrative procedures covering storage of user data, backup, off-site storage, critical server redundancy, network redundancy, and contingency plans for business continuity at an alternate location.

- i. The Information Technology Department shall devise, post or publish, and periodically review, a Disaster Recovery Plan.
- ii. Operational aspects of the Disaster Recovery Plan will be tested at least once annually, as resources permit.
- iii. The Disaster Recovery Plan shall list all of the Information Technology resources critical to the continuation of service to the people of Richmond, by: Hardware, Applications, Data, and Network.
- iv. The Disaster Recovery Plan shall describe the City's vulnerabilities for each of these resources.
- v. The Disaster Recovery Plan shall describe the procedures to recover from a failure, loss, or destruction of each of those resources.



- vi. The Information Technology Department shall maintain a secure copy of the City's data in a location other than City Hall, and such secured data shall never be more than eight days old.

## 6. Project Management

The purpose of this procedure is to set minimum standards for formal project management. This will help ensure accountability, and ensure that proper reporting systems are in place for all valuable Information Technology projects.

- i. This policy applies to any Information Technology project with a combined value greater than fifty thousand dollars (\$50,000) in hardware, software, or services.
- ii. Every such project shall have designated a project owner, who bears overall responsibility for the project.
- iii. Every such project shall have designated a project manager, who manages the project and delivers status reports to the project owner on a weekly basis.
- iv. The project owner shall document a project charter, including, but not limited to, the following descriptions:
  - *Project purpose*
  - *Project owner, manager, and other key staff*
  - *Resources, including capital and maintenance budget information*
  - *How success will be measured*
  - *Completion date*
  - *Formal signoff by stakeholders.*

## 7. Appendixes

The appendixes contain suggested classifications to the above policies. They may be adopted or changed by the Information Technology Department.

- i. **IT Security Policy – Data Classification, two major categories, secured and unsecured:**

Unsecured Data Classification:

Public – May be viewed by anyone (including City staff and the general public).

Secured Data Classification:

- Corporate – May be viewed by City staff only.
- Sensitive – May be viewed by City managers and designated staff only.
- Confidential – May be viewed by City senior management team only.
- Personal – May be viewed by the subject and Human Resources only.
- Private – May be viewed by the owner only.

- ii. **Hardware and Software**

*Software will be classified into the following categories:*





- 1) Infrastructure Software. This includes but not limited to the standard "bundle" of software delivered with each desktop system, and used by all staff. This includes the current versions of Operating System, Electronic Mail & Scheduling, Word Processing, Spreadsheets, Document Management, Internet Browser, Anti-Virus.
- 2) Enterprise Applications. This includes the standard applications that are widely used by the City, but not by all staff. This includes the current versions of PeopleSoft, Hansen, Amanda, PowerPoint, WinFax, and MS Project.
- 3) Departmental Applications. This includes the specialized applications that are used primarily within departments, and have been tested by IT for compatibility and suitability. Examples include ParkSmart, Quick Law, and OpenTax.
- 4) Development Applications. This includes applications that are used as tools to create complex documents or completely new applications. Examples include MS Access, ESRI GIS, FrontPage, Visio, and AutoCAD.
- 5) Unsupported Applications. This includes software that is installed, but not supported by IT. Software that is used by only one person in the City usually falls into this category.
- 6) Unauthorised Applications. This includes the following situations: software (including device drivers) not installed by IT, games, software downloaded from the Internet, unlicensed software, custom screen savers, cartoon figures.

**iii. Disaster Recovery**

*Disasters will be classified into the following categories:*

- 1) System Fault. The complete failure of a single application system, due to a user, hardware or software failure, not resulting in any destruction of data.
- 2) System Failure. The complete failure of a single application system, due to a user, hardware or software failure, resulting in destruction of data.
- 3) General Failure. The complete failure of multiple application systems, due to a user hardware, software, or environmental failure, resulting in destruction of multiple sets of data.
- 4) General Disaster. The physical destruction of multiple application systems, due to an environmental or social incident, resulting in destruction of processing systems as well as multiple sets of data.