

UMJINDI LOCAL MUNICIPALITY

INFORMATION SECURITY POLICY

Core Business Area	Financial Services Directorate
Operational Area	IT Section

Version:	Review.01
Date:	01 JULY 2008
File Name:	Information Security Policy Document
Business Owner:	S Godfrey

Owner: IT Section
Client: Umjindi Local Municipality

Document Classification:
Confidential
© Umjindi Local Municipality 2008

<i>REVISION HISTORY</i>			
Date	Version	Description	Author/s
01-07-2008	0.01	Draft	S Godfrey

<i>DOCUMENT APPROVAL</i>			
Position	Name	Signature	Approval Date
Mayor	R V Lukhele		
Municipal Manager	S F Mnisi		
Chief Financial Officer	M S Tlali		
Business Owner	S Godfrey		

EFFECTIVE DATE: 1st JULY 2008

TABLE OF CONTENTS

1. Introduction	4
2. Aim	5
3. Scope	5
4. Abbreviations	6
5. Terms and Definitions	6
6. Organizational Security	9
6.1 Information Security Infrastructure	9
6.1.1 Electronic Information Resource Security Policies Officer	9
6.1.2 Chief Information Resource and Communications Manager	10
6.1.3 Electronic Information Resource Manager	10
6.1.4 Electronic Information Resource Custodian	10
6.1.5 Electronic Information Resource User	11
6.2 Outsourcing	11
7. Asset Control	11
7.1 Information Classification	11
8. Personnel Security	12
8.1 Security in job definition and resourcing	12
9. Physical and Environmental Security	13
9.1 Secure Areas	13
9.1.1 Disaster Controls	13
9.1.2 Physical Access Controls	13
9.1.3 Procedural Controls	13
10. Operations Management	14
10.1 Operational Procedures and Responsibilities	14
10.2 Protection against malicious software and cyber crime	14
10.3 Backups	15
10.4 Media handling and security	15
10.5 Incident Response	15
11. Communications Management	16
11.1 Communications Security	16
11.1.1 Firewall and External Connectivity	16
11.1.2 Intrusion Detection System	16
11.1.3 Encryption	16
12. Access Control	17
12.1 Access Controls	17
12.1.1 Electronic Information Resource Sensitivity	17
12.1.2 Electronic Information Resource Criticality	17
12.2 Monitoring system access and use	18
12.3 System Administration Access Controls	19
13. Systems Development and Maintenance	20
14. Business Continuity Management	21
14.1 Disaster Recovery	21
15. Compliance	22

15.1 Compliance with legal requirements	22
15.2 Intellectual Property Rights (IPR)	22
15.3 Data protection and privacy of personal information	22
15.4 Reviews of security policy and technical compliance	22
15.4.1 Compliance with the Information Security Policy	22
15.4.2 Technical Compliance Checking	23



1. INTRODUCTION .

Security is generally defined as the freedom from danger or as the condition of safety. Computer security, specifically, is the protection of data in a system against unauthorized disclosure, modification, or destruction and protection of the computer system itself against unauthorized use, modification, or denial of service.

Mostly when the term “information security” is heard, people usually focus on single events like website hacking, procuring credit card details, email viruses or the like. The fact is that these are only the tips of the information security iceberg. To fully appreciate the importance and scope of information security we need to widen our view considerably. Information security is more than just IT security. The focus of information security is not on the security of an organization’s IT operations per se, but on the organization’s “Information Assets”. Information security covers the whole of organizations information such as business cards, client and contact databases, personnel information, financial records and transactions, information databases etcetera.

There are three letters to remember when thinking of information security; they are CIA. CIA stands for Confidentiality, Integrity and Availability, the three main checklist items when considering information security.

▣ Confidentiality

Confidentiality is the protection of information in the system so that unauthorized persons cannot access it. The confidentiality of information must be maintained during its collection, storage, processing, and dissemination even if the information is co-mingled with other information or is processed in a manner where the original information is reproducible.

▣ Integrity

Integrity is the protection of system data from intentional or accidental unauthorized changes. As with the confidentiality policy, identification and authentication of users are key elements of the information integrity policy. Integrity depends on access controls; therefore, it is necessary to positively and uniquely identify all persons who attempt access.

▣ Availability

Availability, the condition that electronically stored information is where it needs to be, when it needs to be there, and in the form necessary, is closely related to the availability of the information processing technology. Whether because the process is unavailable, or the information itself is somehow unavailable, makes no difference to the organization dependent on the information to conduct its business or mission. The value of the information’s availability is reflected in the costs incurred over time by the organization, because the information was not available, regardless of cause.

The CIA principles should guide your thinking about information security. A security breach need not be a malicious act; it could be as innocent and simple as a power outage or a failure to set network access privileges correctly, or it could be the total loss of all your facilities through a disastrous event, natural or unnatural.

Umjindi Municipality's information resources, including data, applications, systems, hardware, networks, and software, are valuable assets. These assets are at risk from potential threats such as employee error or other accidents, long-term system failures, natural disasters, and criminal or malicious action. Such events could result in damage to or loss of information resources, loss of data accuracy/integrity or interruption of normal data processing.

The Municipality's goals for risk reduction are based, therefore, on the principle that the level and type of security should reflect an assessment of the criticality of an Electronic Information Resource to the operation of the Municipality, the sensitivity of the data residing in or accessible through the Electronic Information Resource, the cost of preventive measures and controls designed to detect errors or irregularities and the amount of risk that management at the Municipality is willing to absorb.

2. AIM

The first step towards improved security is to identify what it is that has to be protected and from there on build a security framework based on policy. Information Security Risk Analysis shows you how to use cost-effective risk analysis techniques to identify and quantify the threats - both accidental and purposeful - that the organization faces. It is crucial to prioritize the risk and the impact it would have on the organization. This will help management to determine critical assets and where to implement which protection measures.

Security Risk Analysis is a basic requirement of ISO17799 and is referenced throughout the standard. The relationship between risk analysis and compliance with ISO17799 is extremely close. It is therefore important to ensure that the methodology adopted is fully consistent with the demands of the standard.

The aim with the policy is to ensure that the ISO17799 standard, recognised as an international standard, will be used. This standard is very clear with respect to security policies and refers to management for acknowledgement to set clear policy direction, commitment and maintenance to information security. It provides recommendations for information security management and those responsible for initiating, implementing or maintaining the policy.

3. SCOPE

The purpose of the standard is to ensure that management set clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization. Information security, including its overall objectives and scope and the importance

thereof are an enabling mechanism for information sharing. Management intent should state that they will support the goals and principles of information security.

A brief explanation of the security policies, principles, standards and compliance requirements are of particular importance to the organization, with regard to:

- ▣ Compliance to legislative and contractual requirements;
- ▣ Security education requirements;
- ▣ Prevention and detection of malicious software and cyber crime;
- ▣ Business continuity management;
- ▣ Consequences of security policy violations

The policy outline will entail the following guidelines:

- ▣ Organizational Security
- ▣ Asset Control
- ▣ Personnel Security
- ▣ Physical & Environmental Security
- ▣ Operations Management
- ▣ Communications Management
- ▣ Access Control
- ▣ Systems Development & Maintenance
- ▣ Business Continuity Management
- ▣ Compliance

4. ABBREVIATIONS

DBA Database Administrator
NA Network Administrator
LAN Local Area Network
SAPS South African Police Service
DRP Disaster Recovery Plan
BCP Business Continuity Plan
IDS Intrusion Detection System

5. TERMS AND DEFINITIONS

Audit

Activities to detect and investigate events that might represent a threat to security/independent review and examination of system records and activities in order to test for effectiveness of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy or procedures.

Authentication

The process of identifying individuals as belonging to a class, which may be a group or an individual.

Authorization

The process by which a determination is made whether or not the identified individual or class is authorized to access an Information Resource, and at what level (read only, create, delete, modify). Authentication is a term that is also used to verify the integrity of network nodes, programs, or messages.

Authorized User

A Municipality employee, student or other individual affiliated with the Municipality who has been granted authorization by the Electronic Information Resource Manager, or his or her designee, to access an Electronic Information Resource and who invokes or accesses an Electronic Information Resource for the purpose of performing his or her job duties or other functions directly related to his or her affiliation with the Municipality. The authorization granted is for a specific level of access to the Electronic Information Resource as designated by the Electronic Information Resource Manager, unless otherwise defined by Municipality policies. An example of an authorized user includes someone who handles business transactions and performs data entry into a business application, or someone who gathers information from an application or data source for the purposes of analysis and management reporting.

Availability

Being accessible and useable upon demand by an authorized entity.

Business Continuity Plan

A plan for the continued operation of critical business administration in the case of a disaster affecting normal functioning. A Business Continuity Plan is more all-inclusive than a Disaster Recovery Plan, which normally relates to information systems only.

Computer Virus

An example of Intrusive Computer Software (see definition below).

Disaster

Any event or occurrence that prevents the normal operation of Electronic Information Resource(s) for a period of time, such that the resulting disruption and/or losses exceed the acceptable limits established consistent with the policy. A disaster may occur as a result of a natural disaster such as a flood, fire or earthquake, employee error or other accidents, long-term system failures, and criminal or malicious action.

Disaster Recovery Plan

A written plan including provisions for implementing and running Essential Electronic Information Resources at an alternate site or provisions for equivalent alternate processing (possibly manual) in the event of a disaster.

Electronic Information Resource

A resource used in support of Municipality business administration that involves the electronic storage, processing or transmitting of data, as well as the data itself. Electronic Information Resources include application systems, operating systems, tools, communications systems, and data – in raw, summary, and interpreted form – and associated computer server, desktop, communications and other hardware used in support of the Municipality business administration.

Identification and authentication

Functions to establish and verify the validity of the claimed identity of a user.

Information Security

The science and study of methods of protecting information in computer and communication systems against unauthorized disclosure, transfer, modification and destruction whether accidental or intentional.

Integrity

The inherent quality of protection that maintains the accuracy of entities of an information system and the information in a system and ensures that the entities and information are not altered or destroyed in an unauthorized manner.

Intrusive Computer Software

Intrusive computer software (such as a computer virus) is an unauthorized program designed to embed copies of itself in other programs, to modify programs or data, or to self-replicate. Intrusive computer software may be spread via removable storage media (e.g. diskettes for personal computers) or via a network. The term "*intrusive computer software*" as it is used in this policy is

intended to encompass the variety of such unauthorized programs, including viruses, worms, Trojan Horses, etc.

Local Area Network (LAN)

A high bandwidth bidirectional communication infrastructure which enables users to share resources and which operates over a limited geographic area.

Logical Access Control

Access control mechanisms that are implemented and enforced by network operating systems, operating systems, application software and communication processes for example authentication, resource access, audit, etc.

Monitoring

Performance measurement to ensure the confidentiality, availability and integrity of operational systems and information.

Password

Confidential authentication information composed of a string of characters.

Physical Access Control

Physical control measures to prevent and/or detect unauthorized access to a security area.

Physical Security

Measures used to provide physical protection of resources against deliberate and/or accidental threats.

Security

Measures taken to reduce the risk of unauthorized access to Electronic Information Resources, via logical, physical or managerial means, and damage to or loss of Electronic Information Resources through any type of disaster, such as employee

error or other accidents, long-term system failures, natural disasters, and criminal or malicious action. Security also encompasses measures taken to reduce the impact of any violation of security or a disaster that occurs despite preventive measures.

Server

A multi-user computer, including mainframes, servers, and personal computers providing services to multiple users. A computer employed, as a single-user workstation is not considered a server.

User

see Authorized User

6. ORGANIZATIONAL SECURITY

6.1 Information Security Infrastructure

The Municipality will establish procedures and practices that implement this policy. The Municipality Mayor and the Senior Councilors will designate an individual or individuals to have overall responsibility for compliance with this policy.

The Municipality implementation must include provision for designation of a single Municipality authority responsible for tracking, taking preventive measures, and reacting to intrusive computer software, such as computer viruses.

A summary of the Municipality responsibilities assigned in this policy is as follows:

6.1.1 Electronic Information Resources Security Policies Officer

The Electronic Information Security Policies Officer is the person who has been designated to have overall coordination responsibility for the Municipality compliance with the policy. Although responsibility for compliance with the policy will most likely rest with a number of individuals, the Municipality's Electronic Information Resource Security Policies Officer must track individuals who are responsible for implementation in every major Municipality functional area, and shall provide education on the contents of the policy.

This person is responsible for review and approval of the means used to provide the requisite security of restricted or essential Electronic Information Resources, or may designate another person as having this responsibility for specified Electronic Information Resources.

The Municipality procedures must ensure that the Municipality's Electronic Information Resource Security Policies Officer is responsible for confirming that the roles of Information Resource

Manager and Information Resource Custodian are assigned for every essential Information Resource.

6.1.2 Chief Information Resources and Communications Manager

The Chief Information Resources and Communications Manager is responsible for development, maintenance and publication of the policy.

6.1.3 Electronic Information Resource Manager

The Electronic Information Resource Manager is the individual designated by the Municipality Mayor, or his or her designee as having the responsibility for determining the purpose and function of the Electronic Information Resource. Such responsibility may include, for example specifying the uses for a departmentally-owned server, establishing the functional requirements during development of a new application or maintenance to an existing application and determining which users may have access to an application or to data accessible via an application. All Electronic

Information Resources are Municipality resources, and Electronic Information Resource Managers are responsible for ensuring that these resources are used in ways consistent with the mission of the Municipality as a whole.

The Manager, subject to appropriate management review, is responsible for determining the level of security required for access controls, based on the sensitivity of the Electronic Information Resource.

The Electronic Information Resource Manager is responsible for determining the level of criticality of an Electronic Information Resource, subject to appropriate management review. For those Electronic Information Resources deemed essential, the manager has the responsibility for determining the appropriate method for providing business continuity such as performing disaster recovery at an alternate site, performing equivalent manual procedures, etc.

For Electronic Information Resources consisting of applications or data, the Manager is also responsible for specifying adequate data retention, in accordance with Municipality policies.

6.1.4 Electronic Information Resource Custodian

The Electronic Information Resource Custodian is responsible for implementing security measures in accordance with the level of access security identified by the Electronic Information Resource Manager.

For Electronic Information Resources consisting of applications or data, the Information Resource Custodian is responsible for ensuring that data retention requirements are met.

For Electronic Information Resources deemed essential, the Custodian is responsible for disaster recovery preparation and general oversight of the performance of disaster recovery in the event of a disaster.

6.1.5 Electronic Information Resource User

Users of Electronic Information Resources are responsible for familiarizing themselves to complying with all Municipality policies, procedures and standards relating to information security. Users are responsible for appropriate handling of Electronic Information Resources, such as data, as established by the Electronic Information Resource Manager and implemented by the Electronic Information Resource Custodian.

6.2 Outsourcing

The requirements for outsourcing the management and control of all or some of its information systems, networks and/or desktop environments should be addressed in a contract agreed between the parties.

7. ASSET CONTROL

7.1 Information Classification

The Municipality must determine which specific Electronic Information Resources warrant preventive measures based on a risk assessment, including an analysis of the financial effect on the Municipality.

When determining the level of security required for an Electronic Information Resource, there are two basic risk characteristics to be assessed:

- The level of sensitivity of the Electronic Information Resource; and
- The level of criticality or overall importance of the Electronic Information Resource to the continuing operation of the Municipality.

Electronic Information Resources are classified into three levels of criticality:

▫ Essential

An Electronic Information Resource should be designated as essential if its failure to function correctly and on schedule could result in a major failure by the Municipality to perform mission-critical business

functions, a significant loss of funds to the Municipality, or a significant liability or other legal exposure to the Municipality.

▫ Required

An Electronic Information Resource should be designated as required if it performs an important function for the Municipality, but the operation of the Municipality could continue for some designated period of time without the function provided by the Information Resource and there is time for recovery should the Information Resource not perform correctly or on schedule.

▫ Deferrable

An Electronic Information Resource should be designated deferrable if the Municipality could continue operation for an extended period of time without the Information Resource performing correctly or on schedule.

8. PERSONNEL SECURITY

The Municipality implementation should include procedures for promptly reporting to the Electronic Information Resource Manager any significant changes in job duties or other status of a user, if these changes are such as to require modification to the user's authorization. These procedures must also provide for removal of authorization for persons who have terminated employment or other association with the Municipality, except where specifically allowed by policy and by the Electronic Information Resource Manager.

8.1 Security in job definition and resourcing

Some of the positions with job responsibilities related directly to Electronic Information Resources may be deemed critical positions in accordance with Municipality personnel policies for staff.

The Municipality should develop policies and procedures to ensure that candidates for open critical positions related to restricted or essential Electronic Information Resources undergo applicable background checks as part of the selection process.

For staff working in critical positions related to restricted or essential Electronic Information Resources, procedures should be established that can be implemented in the event of disciplinary action or termination.

Where there is a concern that access to Electronic Information Resources endangers the integrity of such resources, management should act to restrict, suspend or terminate access.

During an investigatory leave or after termination, revocation of the individual's access privileges to the Municipality, work is normally warranted.

All procedures must be established in accordance with Municipality personnel policies. Background checks are also required for non-Municipality contractors or consultants engaged to work on restricted or essential Electronic Information Resources.

In certain circumstances, authorization should be removed for individuals who have announced their decision to terminate, where continued access might result in an unacceptable level of risk. For example, retired employees may be allowed continued access to certain Municipality resources under defined circumstances.

The principles of separation of duties should be followed when assigning job responsibilities relating to restricted or essential Electronic Information Resources. No individual should have authorization for both implementing programs into production and updating production data for a restricted or essential application.

9. PHYSICAL AND ENVIRONMENTAL SECURITY

9.1 Secure Areas

The Municipality implementation should establish procedures for the physical protection of Electronic Information Resources, including disaster controls, physical access controls, and procedural controls.

At a minimum, the Municipality will develop policies and procedures to protect physical areas containing shared Electronic Information Resources that support restricted or essential Electronic Information Resources.

These policies and procedures should address the following:

9.1.1 Disaster Controls

Appropriate measures for the prevention, detection, early warning of, and recovery from emergency conditions, including earthquake, fire, water leakage or flooding, disruption of power, air conditioning failures, and environmental conditions exceeding equipment limits.

9.1.2 Physical Access Controls

Controls for limiting physical access to facilities housing restricted or essential Electronic Information Resources through the use of combination locks, key locks, badge readers, sign in/out logs for visitors, verification of identification, etc.

9.1.3 Procedural Controls

Controls over check-stock, produced checks, and other financial instruments. In addition, physical inventories of equipment should be completed and maintained. Departments must also consider physical

security for personal computers and other Electronic Information Resources housed within their immediate work area. Protection of physical equipment or of software and data residing on storage media from theft, damage or improper use should be addressed. Particular attention must be paid where access to or functioning of restricted or essential Electronic Information Resources is concerned. Restricted data should not be transferred and stored on separate portable equipment such as laptops.

10. OPERATIONS MANAGEMENT

10.1 Operational Procedures and responsibilities

The Municipality procedures should provide mechanisms for employees to report violations of the policy.

10.2 Protection against malicious software and cyber crime

The Municipality should determine their exposure to adverse intrusive computer software for different Electronic Information Resources, and put in place precautions commensurate with the level of risk.

The Municipality should designate a Municipality authority responsible for the coordination of tracking, taking preventive measures, and reacting to intrusive computer software such as computer viruses. Any suspicion or detection of such intrusive software should be immediately reported to this authority and to the SAPS if appropriate, in accordance with procedures for investigating misuse of Municipality Resources, unless such intrusive software is already known and can be prevented or eliminated with standard commercial software.

While intrusive computer software such as computer viruses, can potentially affect any type of computer or server, the area of greatest risk is personal computers that receive files from external sources, whether over a network or dialup connection, or via shared detachable storage devices. The Municipality should evaluate their exposure regarding adverse intrusive computer software for different Information Resources, and put in place precautions commensurate with the level of risk and the associated cost to the institution for such anticipated loss. They should also implement

processes to notify users and take other appropriate remedial action in the event of propagation of intrusive computer software.

Proper anti-virus software should be installed on all the computers of the Municipality and the definition files must be updated.

10.3 Backups

Backup copies of data and software associated with restricted or essential Electronic Information Resources must be sufficient to satisfy disaster recovery requirements, application or other Electronic Information Resource processing requirements, and any functional requirements of any Electronic Information Resource Manager dependent upon such data.

Backup copies of essential data for disaster recovery purposes must be stored at a secure, commercial site that provides standard protection. These backup requirements extend to essential or restricted software and data stored on personal computers, as well as software and data stored on shared servers.

Backup and other retention services for data must also comply with Municipality policies regarding data retention.

The Municipality implementation procedures should ensure that backup copies of data and software associated with restricted or essential Electronic Information Resources are sufficient to satisfy disaster recovery requirements, application or other Electronic Information Resource processing requirements, and any functional requirements of any Electronic Information Resource Manager dependent upon such data.

10.4 Media Handling and Security

Before any restricted data may be transferred from one server to another or to a workstation, the user affecting the transfer must ensure that access controls on the destination system are commensurate with access controls on the originating server or commensurate with the security requirements established by the Electronic Information Resource Manager.

Those responsible for granting access to restricted data or to any restricted or essential Electronic Information Resource must ensure that authorized users are aware of this constraint when access is originally granted to the user. They may choose to require the user's signature to acknowledge this notification.

10.5 Incident Response

Supervisors and Department Heads are, in turn, responsible for promptly reporting any known or suspected violations to the Electronic Information Resource Manager or Custodian or to the Internal Audit department.

Depending on the nature of the violation and the likelihood of a recurrence, the Electronic Information Resource Manager or Custodian shall take prompt action to protect against future violations to the extent feasible, and/or remove the means by which the violation occurred.

Depending on the nature of the violation, the Electronic Information Resource Manager or Custodian shall consult with other Municipality authorities in accordance with policies governing potential disciplinary action.

In the event that the violation involves possible unlawful action by a user, Internal Audit or the SAPS should immediately be notified.

Procedures for investigating misuse of Municipality resources should be in place. Notification of Internal Audit or the SAPS should take place before any action is taken, unless prompt emergency action is required to prevent bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of Municipality policy, or significant liability to the Municipality or to members of the Municipality community. The Municipality reserves the right to revoke access to any Electronic Information Resource for any user who violates the policy, or for any other business reasons in conformance with other applicable Municipality policies.

11. COMMUNICATIONS MANAGEMENT

The Municipality implementation should encourage the use of encryption to prevent unauthorized access to restricted data during transmission of such data across a communications network. The Municipality implementation must include procedures for testing software used to provide logical access controls and access control points for connectivity such as firewalls.

11.1 Communications Security

11.1.1 Firewalls and External Connectivity

Communications access controls, such as firewalls, must be present to limit unauthorized access to restricted or essential Electronic Information Resource across the Municipality or Municipality communication networks. These firewalls may be limited to protection at the appropriate subnet level.

11.1.2 Intrusion Detection Systems

The Municipality should consider use of IDS to help identify attempted or actual unauthorized intrusions.

11.1.3 Encryption

Where technology is available that readily supports this capability, the use of encryption is encouraged to prevent unauthorized access to restricted data during transmission.

12. ACCESS CONTROL

This section addresses security measures related to controlling access to Electronic Information Resources through logical measures such as software or network controls, controls related to software development and change control, security of data, communications security, and reduction of risk from intrusive computer software.

12.1 Access Controls

The level of access controls required for an Electronic Information Resource depends on the sensitivity of the Electronic Information Resource, as defined below. The requirement to include a particular Electronic Information Resource in DRP's as part of overall business continuity planning depends on the criticality of the application to the Municipality.

12.1.1 Electronic Information Resource Sensitivity

The sensitivity of an Electronic Information Resource, and therefore the level of security required, depends on the sensitivity of the data retained by or accessible through the Electronic Information Resource.

12.1.2 Electronic Information Resource Criticality

Electronic Information Resource criticality is a measure of the importance of an Electronic Information Resource to the continuing operation of the Municipality. The criticality of an Electronic Information Resource determines whether or not it must be included in the Municipality's DRP.

Access to restricted Electronic Information Resources and data retained within or accessible through these Information Resources must be limited to authorized users. The Electronic Information Resource Manager specifies authorized users and their specific level of privilege, unless otherwise defined by Municipal policy. Such access must be controlled with secure means of authentication and authorization.

Procedures for authorizing users to access Electronic Information Resources or data in or accessible through them shall provide for prompt notification of the Electronic Information Resource Manager of any significant changes in job duties or other status of a user, if these changes are such as to require modification to the user's authorization. Such procedures must also provide for prompt removal of authorization for persons who have terminated employment or other association with the Municipality, except where specifically permitted by policy and by the Electronic Information Resource Manager.

A Municipality's Electronic Information Resource Security Officer will be responsible for the coordination of the review and approval of the means used to provide the requisite security of restricted or essential Electronic Information Resources. Procedures for initially providing users with authorization for access to Electronic Information Resources or to data in or accessible through Electronic Information Resources must incorporate review and approval mechanisms to avoid any unauthorized persons being granted access.

It is a violation of this policy and other Municipality policies for users to attempt to gain unauthorized access to any Electronic Information Resources or in any way damage, alter, or disrupt the operations of these Electronic Information Resources.

For users to capture or otherwise obtain or tamper with passwords, encryption keys, or any other access control mechanism that could permit unauthorized access is a violation of the policy, except where it is expressly required in the performance of their duties, such as when systems personnel need to provide access to Electronic Information Resources when passwords or other keys have been lost or misplaced. Among other possible disciplinary actions, Electronic Information Resource Managers may withdraw the privileges of any user who violates the policy if, in their opinion, continuation of such privileges threatens the security, including integrity, confidentiality and availability, of a restricted Electronic Information Resource. Appeals regarding revocation of privileges should follow normal Municipality conflict resolution procedures.

Passwords selected by users or automatically generated to protect access to Information Resources should be hard to guess and, for essential Electronic Information Resources, should be changed frequently. Passwords must not be shared. When there is a need for shared passwords, specific accounts should be set up for that purpose with the necessary controls in place.

The Municipality implementation policies should specify for example, that passwords must be at least eight characters in length, and must contain at least one numeric digit and at least one alphabetic character. Examples of further password protection include requiring passwords to be changed on a regular basis ("password aging") and limiting re-use of passwords.

12.2 Monitoring system access and use

The Municipality implementation of the policy should encourage, where applicable, the use of system logs to assist in monitoring access to Electronic Information Resources and/or access to data retained within or accessible through such resources. Such logs should include sufficient detail, such as records of all login attempts, to ensure that suspicious patterns of activity can be identified. Since such logs may contain personally identifiable information, the Electronic Information Resource Manager should comply with Municipality policy related to privacy. The Municipality should consider using system tools to automatically identify suspicious patterns of activity within the logs. Controls designed to protect Electronic Information Resources from

unauthorized access must not be so restrictive as to prevent authorized access to the Information Resource. An example of such an over-protection is business data stored in protected format, with no provisions in place to ensure availability of the data to authorized users.

The Municipality procedures for initially providing users with authorization for access to Electronic Information Resources, or data accessible through them must incorporate a review and approval mechanism.

The Municipality implementation procedures should ensure that only authorized personnel can implement changes to software for restricted or essential applications and that such Municipality Information Security changes are carried out according to established procedures.

The Municipality will provide means for performing authentication and authorization functions prior to allowing access to restricted or essential Electronic Information Resources.

The Municipality implementation of these policies must include procedures for testing software used to provide logical access controls and access control points for connectivity such as firewalls.

Supervisors or other employees with responsibilities for security should periodically review the system administration work of personnel with access to privileged "super-user" accounts on shared servers. Such review will be intended to provide a periodic audit or review for those system administration functions that are not otherwise audited or reviewed in the course of being completed.

12.3 System Administration Access Controls

System Administrators routinely require access to Electronic Information Resources to perform essential system administration functions critical to the continued operation of the Electronic Information Resource. Such privileged access is often termed "super-user access" and accounts that provide such privileges to System Administrators are termed "super-user accounts." Privileged or super-user accounts enable vital system administration functions to be performed, such as establishing user-id's or accounts, maintaining authorization for these accounts, terminating another user's session, correcting problems, and other broadly-defined system or other Electronic Information Resource privileges.

Such privileged accounts are especially sensitive and the Municipality must establish procedures, commensurate with the level of risk involved, to ensure that abuse will not occur. In particular, the number of privileged accounts must be kept to a minimum, and only provided to those personnel whose job duties require them. Those personnel who do require privileged accounts should also have less powerful accounts to use when not performing system administration tasks and must be instructed not to use super-user accounts for other than authorized purposes. Activities performed using a super-user account should be logged, and an independent and knowledgeable person

should review the logs on a regular basis. These logs should be printed or stored in a non-convertible form. Super-user accounts should be monitored periodically to ensure they are being used for designated purposes.

The Municipality implementation procedures should ensure that the number of system administration user-ids on shared servers is kept to a minimum, and only provided to those personnel requiring system administration capabilities in order to perform their job duties.

13. SYSTEMS DEVELOPMENT AND MAINTENANCE

Development and maintenance of administrative applications performed by Municipality personnel or performed by any vendor engaged by Municipality personnel must conform to the Specifications Systems Development Standards.

Application development and maintenance efforts must also conform to the standards, procedures, guidelines and conventions. In general, the Municipality is encouraged to involve Internal Audit and

the Municipality Controller in the development or implementation of essential applications in order to obtain advice on establishing proper controls. Internal Audit must be notified of all application system development projects early in the development process.

The purpose of change controls is to ensure the accuracy, integrity, authorization, and documentation of all changes. Only authorized personnel will implement changes to software for restricted or essential applications, and must perform such changes according to change management procedures established by the Municipality.

Change procedures should include assignment of responsibilities to ensure adequate separation of duties, and may also include confirmation of testing, authorization for moving the programs to production, user training requirements, and documentation requirements. In some cases the Electronic Information Resource Manager will be required to authorize program modifications before changes can be implemented in production.

Change procedures should include backup of prior versions of application programs, so that a change may be "rolled back" if problems occur.

The Municipality will provide means for performing authentication and authorization functions prior to allowing access to restricted or essential Electronic Information Resources.

Modifications to data residing in essential applications must be performed according to predefined methods that have been developed with provisions for ensuring data integrity, availability, privacy, and compliance with audit requirements, to avoid circumvention of data integrity and auditing controls. For example, updates to payroll records should be performed only through

the production payroll application. Exceptions may be made on a case-by-case basis, but should always be performed in a controlled manner and with the knowledge of the Electronic Information Resource Manager.

14. BUSINESS CONTINUITY MANAGEMENT

Disaster Recovery

The Municipality is responsible for preparing, periodically updating, and regularly testing the Municipality plan for recovering from a disaster that renders certain Electronic Information Resources unavailable for an unacceptable period of time. Such a DRP should establish the frequency of testing disaster recovery procedures. The site should ensure that any local operations procedures are coordinated with the DRP.

Recovery plans to address the failure of essential Electronic Information Resources must be included in the Municipality DRP. The Municipality must decide whether or not to include recovery plans for required or deferrable Electronic Information Resources in the Municipality DRP.

The DRP will include provisions for implementing and running essential applications at an alternate site or provisions for equivalent alternate processing (possibly manual) in the event of a disaster or

other interruption that renders normal processing inoperable for the period of time specified in the designation of the Electronic Information Resources as essential.

The DRP will also specify emergency response procedures, including specifying teams of personnel assigned responsibility for responding in emergency situations, and specifying procedures to enable team members to communicate with each other and with management during an emergency. For these purposes, an emergency is an event that has led or will imminently lead to a situation in which essential Electronic Information Resources cannot be restored to functioning status within the time specified in the designation of the Information Resources as essential. The DRP should include or ensure the availability of any systems documentation required for performing recovery.

Backup copies of data and software that are sufficient for recovery from an emergency situation pertaining to essential Electronic Information Resources must be stored at a secure, commercial site providing standard protection providing equivalent protection against fire, flood, earthquake, theft, decay, and other hazards. Requirements and procedures for such off-site backup shall be included in the DRP, including procedures and authorities for obtaining access to the Municipality in the event of an emergency.

Disaster Recovery requirements should be specified when establishing maintenance agreements with vendors supplying components of essential Electronic Information Resources, such as ensuring that the vendor can provide replacement components within a reasonable period of time.

15. COMPLIANCE

Compliance with legal requirements

All relevant statutory, regulatory and contractual requirements should be explicitly defined and documented for each information system. The specific controls and individual responsibilities to meet these requirements should be similarly defined and documented.

The following is a list of the necessary legislation in South Africa with regard to securing of information:

- ▣ Copyright Act
- ▣ Cyberlaw
- ▣ Data Protections Act
- ▣ e-Commerce Act
- ▣ Electronic Communications and Transactions Act
- ▣ Intellectual Property Law Rationalization Act
- ▣ Interception and Monitoring Act

- ▣ King II Report
- ▣ Piracy Act
- ▣ Promotions of Access to Information Act
- ▣ Protected Disclosures Act
- ▣ Protection of Information Act 1982

Intellectual property rights (IPR)

Appropriate procedures should be implemented to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright. Copyright infringement can lead to legal action which may involve criminal proceedings. Software products are usually supplied under a licensing agreement. This limits the use of the product(s) that may also limit the copying of the software product only for the creation of a backup.

Data protection and privacy of personal information

Compliance with data protection legislation requires appropriate management structure and control. Often this is best achieved by the appointment of a data protection officer who should provide guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed.

Reviews of security policy and technical compliance

15.4.1 Compliance with the Information Security Policy

If an employee, contractor or consultant becomes aware of the occurrence of any violation of the policy, he or she must report the

violation promptly to his/her supervisor, Department Head, the Electronic Information Resource Manager or Custodian, or the Internal Audit department. In the case of contractors or consultants they must report the violation to their client.

15.4.2 Technical Compliance Checking

Information systems should be regularly checked for compliance with security implementation standards. Technical compliance checking involves the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance checking requires specialist technical assistance. It should be performed manually, supported by appropriate software tools if necessary, by an experienced person, or by an automated software package which generates a technical report for subsequent interpretation by a technical specialist.