Fetakgomo Local Municipality

Council Resolution No. C79/2016

INFORMATION COMMUNICATION TECHNOLOGY POLICY

Table of Contents

1. OVERVIEW OF THE INFORMATION COMMUNICATION TECHNOLOGY POLICY

1.1 INTRODUCTION

Information Communication Technology is one of the pivotal strategic tools for the municipality to fast track service delivery and conducive working environment. Information communication technology (ICT) - the people, processes, infrastructure and information - is embedded across the

Municipality creating an enterprise wide community of owners and stakeholders. As a major investment the ICT is expected to deliver value and has been found to deliver greater 'value' for the Municipality when used as a strategic enabler rather than being influenced by a stream of diverse tactical initiatives. This policy document is made out of sub-policies which are not covered in other existing information technology policies and procedures of the municipality.

1.2 PURPOSE

All the employees' share the information communication technology facilities at Fetakgomo Local Municipality (FTM). These facilities are provided to employees for the purpose of conducting municipality business.FTM does permit a limited amount of personal use of these facilities, including but not limited to computers, printers, e-mail and internet access. However, these facilities must be used responsibly by everyone, since misuse by even a few individuals has the potential to negatively impact productivity, disrupt municipal business and interfere with the work or rights of others. Therefore, all employees are expected to exercise responsible and ethical behavior when using FTM's Information Communication Technology facilities. Any action that may expose potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.

The Fetakgomo Local Municipality ICT Policy (ICTP) document sets out the principles and standards which determine acceptable use of the Information Communication Technology of the Municipality. The primary aim of this ICTP document is to balance protection of the systems, services and information that makes up those resources.

1. 3 INFORMATION COMMUNICATION TECHNOLOGY POLICY INCORPORATED IN THE ICTP DOCUMENT.

1.3.1 The ICT policy document consists of the following sub-policies:

1) Software Licensing Policy
2) Policy on the Use of Computer Equipment
3) IT Server Documentation Policy
4) Information Protection Policy
5) VPN Virtual Private Network Policy
6) Systems Development and Maintenance
7) Website Use Policy
8) IT Procurement Policy and Procedure
9) Incident Handling Policy and Procedure
10) Insurance Policy and Procedure
11) Systems Development and Maintenance
12) Communications and Operational Management

2. SOFTWARE LICENSING POLICY

2.1 INTRODUCTION

End-User license agreements used by software and other information communication technology companies to protect their valuable intellectual information technology assets and to advise technology users of their rights and responsibilities under intellectual property and other applicable laws.

Fetakgomo Local Municipality software Licensing policy applies to all individuals or employees that use any municipality information resources.

2.2 SOFTWARE LICENSING POLICY OBJECTIVES

2.2.1 There are two main objectives that will be achieved by having an underpinning Software licensing policy in place:

a) Ensure licensing compliance.
b) Prevent piracy practices.

2.3 POLICY STATEMENTS

2.3.1 The software licensing policy will take effect under different circumstances, namely:

a. Approval of new software purchases
b. Management of software installations
c. Monitoring of software licensing
d. Physically secure disks/licenses

2.3.1.1 New software

a) The divisions or units purchasing software must consult with the information technology office and verify that the product is compatible and appropriate before the purchases.
b) New software must be approved by the relevant supervisor with the recommendation from the Information Technology Manager. This approval must be verifiable via a filed purchase order signed by all parties. The new software is to be shipped to Fetakgomo Local Municipality when possible.
c) Fetakgomo Local Municipality will retain all setup mediums, licenses and manuals, excluding end user manuals. Any setup disks and or licenses not currently stored in the municipality must be relinquished to Fetakgomo Local Municipality upon approval of this policy.

2.3.1.2 Software Installations

a) All software installations will be performed by Fetakgomo Local Municipality Information technology personnel or approved service provider, with Fetakgomo Local Municipality approval via instructions or automatically active directory. Software will not be installed without a proper licenses and approval of information technology manager.

2.3.1.3 License control

a. All software licenses must be stored centrally within Fetakgomo Local Municipality. Information technology office will maintain a license inventory of all restricted licenses. This includes all software purchases, granted, "free" for educational use, shareware or any other restricted license.

2.3.1.4 Setup Medium Control

1) All mobile setup mediums (disks, CDs, Flash drive, tapes, etc.) must be stored centrally within Fetakgomo Local Municipality.

2.4 GENERAL

2.4.1 Fetakgomo Local Municipality provides a sufficient number of licensed copies of software such that workers/employees can get their work done in an expedient and effective manner. Management must make appropriate arrangements with the involve vendor(s) for additional licensed copies if and when additional copies are needed for business activities.

2.4.2 Third party copyrighted information or software, that Fetakgomo Local Municipality does not have specific approval to store and/or use, must not be stored on Fetakgomo Local Municipality systems or networks. Systems administrators will remove such information and software unless the involved users can provide proof of authorisation from the rightful owner(s).

2.4.3 Third party software in the possession of Fetakgomo Local Municipality must not be copies unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes.

2.4.4 All personnel are responsible for managing their use of information technology and Are accountable for their actions relating to information technology security. Municipality employees are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.

2.4.5 All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected at all times.

2.4.6 On termination of employment or contract of employment with Fetakgomo Local Municipality, users must surrender all computer related equipment to IT office. All security policies and procedures for information technology apply to and Remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.

2.4.7 All commercial software used on computer systems must be supported by a Software license agreement that specifically describes the usage rights and Restrictions of the product. All employees must be abide by all license agreements and must not illegally copy licensed software. The Information Technology Manager or personnel reserves the right to remove any unlicensed software from any computer system of the municipality.

2.5 DISCIPLINARY ACTIONS

a) Any violation of this policy may result action which may lead to disciplinary hearing, a termination of employment relation in the case of contractors or consultants, dismissal for interns and volunteers or a suspension. Additionally,

individuals are subject to loss of Fetakgomo Local Municipality information Resource access privileges, civil, and criminal prosecution

3. POLICY ON THE USE OF COMPUTER EQUIPMENT

3.1 PURPOSE

The purpose of this policy is to regulate use of computer equipment so that the Municipality:

a) Control costs with a standardized set of software and hardware that can be well supported in terms of maintenance and user training.
b) Uses municipal assets efficiently.
c) minimizes loss of, or damage to, equipment, software and data;
d) Is protected from legal difficulties
e) Is productive, by limiting personal use to reasonable levels.

3.2 SCOPE

This policy is applicable to everyone who works at the Fetakgomo Local Municipality. This means all permanent, contract or temporary personnel including anyone supplied by a labour broker or service-provider to the Municipality, Referred to as "personnel" or "users" in this document.

This policy must be made an enforceable part of any contract with a labour broker or service provider whose personnel use the Municipality's computers.

3.3 POLICY STATEMENT

3.3.1 PERSONNEL MAY BE ISSUED WITH A COMPUTER

At the request of your manager you may be issued with computer equipment/ Laptop and access to computer-based services. These are provided to help you do your job. Qualifying criteria are set by management.

Qualifying personnel will normally get a standard-issue computer from IT Unit, along with standard-issue software. New equipment will be bought only if necessary. Printers are allocated in the same way, but you may be expected to share a printer with other personnel.

Some personnel may need non-standard equipment or software to do their job effectively. To get this, your manager must make a recommendation in the form of a submission to management. The submission must include the details and cost of the software or equipment you need.

3.3.2 THE COMPUTER SYSTEMS BELONG TO THE MUNICIPALITY

The computers, the printers, software licenses, network and data that you use at the Municipality remain the property of the Municipality.

3.3.3 MANAGEMENT WILL SPECIFY THE STANDARD ISSUE PERSONAL COMPUTER

To make for cost-effective use of equipment and software, the Municipality will standardize on a core set of software and hardware products. The specifications will be set, and revised from time to time, by management and the ICT Steering committee. The Committee may set different standards for different parts of the organization. The standards will cover the following:

a) Hardware specifications for standard issue desktop computers, notebook computers and printers. Users will be issued with a computer that meets this standard. When the standard is raised, computers below the standard will be upgraded or replaced (budget allowing), without the need for a motivation from the user.
b) Specifications for new desktop computer, notebook computer or printer hardware. When the Municipality buys a new computer or printer, its specification will conform to this standard.
c) Additional software set. A list of software that may be installed if needed to do the job. To control maintenance cost, no other software may be used without the written approval of both the user's Director and the ICT Manager.
d) Disallowed software and hardware. A list of software, hardware or categories of software or hardware that is not allowed. In setting the standard, the ICT Committee will consider the following issues as a minimum: security, licensing, support and risk of harassment (through offensive material)

3.3.4 USE OF PERSONAL COMPUTERS IS ENCOURAGED FOR OFFICIAL PURPOSES

The use of your personal computer is encouraged for Fetakgomo Local Municipality business or activities sponsored or authorized by the Municipality. An Employee may use his/her computer only under the following circumstances:

a) Computer equipment on **repairs**.
b) Instructed by his/her Director and **approved** by Municipal Manager.
c) Waiting for **new** Computer equipment to be delivered.

3.3.5 YOU HAVE A DUTY TO USE MUNICIPAL RESOURCES RESPONSIBLY

2.3.5.1 Take care to use your computer responsibly, ethically and lawfully. Do not waste computer resources or unfairly monopolize resources to the exclusion of others.

3.3.5.2 Any file copied from an external source must be scanned for computer viruses. This includes files from a CD, USB drive, e-mail or Internet.

1. You may **not** use the Municipality's computer facilities to:

(a) Play games or run other entertainment software.
(b) Save files containing images, music, sound or video onto Municipal servers, unless they are for official purposes.
(c) Make or store illegal copies of material protected by copyright. This includes software programs, music, and publications, in whole or in part.
(d) Back up your entire local hard drive onto Municipal servers.
(e) Print large documents if there is a viable on-screen alternative

3.3.6 YOU MAY HAVE TO PAY FOR LOST, DAMAGED OR STOLEN EQUIPMENT

2.3.6.1 If an item is lost, damaged or stolen while it was under your control or responsibility, the Municipality will not normally ask you to pay for it, **but** you may lose Municipal cover if you fail to follow treasury regulations or standing instructions. The main elements are summarized here. But, this summary does not replace the original prescripts, which will be used to deal with any loss. It is **not allowed** to install Municipal software on personal computer equipment

1. You may lose your Municipal cover against loss if you:

a) Were not on official business when the loss occurred;
b) Did not obtain permission from the Director/Manager and approval of Municipal Manager;
c) Were under the influence of alcohol or drugs when the loss occurred;
d) Had not been issued with a permit to take the item off Municipal premises;
e) Did not obtain a receipt for equipment you voluntarily surrendered;
f) Acted recklessly or negligently;
g) Intentionally caused the damage; or ignored any standing instructions (including Municipal Circulars);
h) Water Damage of computer equipment;
i) Vandalized;

3.3.7 MANAGERS ARE ACCOUNTABLE FOR COMPUTER USE BY THEIR STAFF

Managers should ensure that all their computer-using staff, whether temporary, permanent or contract is made aware of the contents of this policy. You are required to apply the policy to all those who report to you. You are accountable for the use your staff makes of personal computer equipment, software and services.

3.4 LEGAL SUPPORT FOR THIS POLICY

(a) Code of Conduct for the Public Service, which is part of the Public Service Regulations 1999 and issued in terms of the Public Service Act, 1994.
(b) National Treasury Regulations - Chapter 12: Management of Losses and Claims.
(c) Disciplinary Code and Procedures (Public Service Coordinating Bargaining Council Resolution No: 2 of 1999).
(d) Copyright Amendment Act 125 of 1992
(e) Copyright Act 98 of 1978
(f) Occupational Health and Safety Act, 1993

4. IT SERVER DOCUMENTATION POLICY

4.1 PURPOSE

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Fetakgomo Local Municipality. Effective implementation of this policy will minimize unauthorized access to Fetakgomo Local Municipality proprietary information and technology.

4.2 SCOPE

This policy applies to server equipment owned and/or operated by Fetakgomo Local Municipality, and to servers registered under any Fetakgomo Local Municipality-owned internal network domain.

This policy is specifically for equipment on the internal Fetakgomo Local Municipality network. For secure configuration of equipment external to Fetakgomo Local Municipality on the DMZ, refer to the *Internet DMZ Equipment Policy*.

4.3 POLICY

4.3.1 OWNERSHIP AND RESPONSIBILITIES

All internal servers deployed at Fetakgomo Local Municipality must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by InfoSec. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec.

1) Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    a) Server contact(s) and location, and a backup contact
    b) Hardware and Operating System/Version
    c) Main functions and applications, if applicable
2) Information in the corporate enterprise management system must be kept up-to-date.
3) Configuration changes for production servers must follow the appropriate change management procedures.

4.4 GENERAL CONFIGURATION GUIDELENES

a. Operating System configuration should be in accordance with approved InfoSec guidelines.
b. Services and applications that will not be used must be disabled where practical.
c. Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
d. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
e. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
f. Always use standard security principles of least required access to perform a function.
g. Do not uses root when a non-privileged account will do.
h. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

i. Servers should be physically located in an access-controlled environment.

j. Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.5 MONITORING

i. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

(a) All security related logs will be kept online for a minimum of 1 week.

(b) Daily backups will be retained for at least 1 month.

(c) Weekly full tape backups of logs will be retained for at least 1 month.

(d) Monthly full backups will be retained for a minimum of 2 years.

ii. Security-related events will be reported to InfoSec, who will review logs and report incidents to Information Technology management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

(a) Port-scan attacks

(b) Evidence of unauthorized access to privileged accounts

(c) Anomalous occurrences that are not related to specific applications on the host.

4.6 COMPLIANCE

4.6.1 AUDITS WILL BE PERFORMED ON A REGULAR BASIS BY AUTHORIZED ORGANIZATIONS WITHIN FETAKGOMO LOCAL MUNICIPALITY

i. Audits will be managed by the internal audit group or InfoSec, in accordance with the *Audit Policy*. InfoSec will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remedial action or justification.

ii. Every effort will be made to prevent audits from causing operational failures or disruptions.

4.7 ENFORCEMENT

3.7.1 Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.8 DEFINITION

Term	Definition
DMZ:	De-militarised Zone: A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as an internal Fetakgomo local Municipality Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

5. INFORMATION PROTECTION POLICY

5.1 INTRODUCTION

The Fetakgomo Local Municipality has a large variety of assets, including valuable proprietary and confidential information. Protecting information is critical. Fetakgomo Local Municipality information is an asset of the municipality and needs to be protected wherever it exists. This section identifies basic controls that must be controls that must be active on all types of computer workstations and media to protect the municipality's information. The next section discusses the additional requirement that exist when dealing with the Fetakgomo Local Municipality's confidential data. Note that several different controls are specified. They address different threats, and all the controls that are available on a workstation must be implemented.

The primary requirement for protecting the Fetakgomo Local Municipality's information is that it must be protected from all access or viewing except by people who have a business need to know the information.

5.2 POLICY STATEMENTS

5.2.1 All data created, stored or archived on any computer equipment housed within Fetakgomo Local Municipality premises or owned by the municipality and used by the Fetakgomo Local Municipality employees and any other authorized user, is the regarded as Fetakgomo Local Municipality's property. The Municipality's Information Technology personnel reserves the right to request and inspect this data at any time without a notice.

5.2.2 The unauthorized possession and /or usage of any computer equipment or software that Could potentially be used to overwrite or alter any of the municipality's data, no matter Where or how stored, will result in appropriate disciplinary action being taken.

5.2.3 A person who intentionally and without authority to do so interferes with data in a way which Causes such data to be modified, loosed, destroyed or otherwise rendered ineffective is guilty of An offence in terms of Section86 (2) of the Electronic Communication Transaction (ECT) act 25 of 2002 and may be liable of disciplinary Action and /or criminal prosecution.

5.2.4 The following security controls must be activated on all the computer workstation connected to The municipality's network:

(a) Set a power-on password
(b) Set a password protected keyboard/screen lock that is automatically activated by a period of inactivity-the inactivity time interval should be no more than ten minutes.

5.2.5 Computer workstations available for shared use in any Fetakgomo Local Municipality location Are not required to have power-on and keyboard/screen lock passwords applied. However Municipality employees must not place Fetakgomo Local Municipality confidential Information, file sharing software, user-ID files, mail files or databases on workstation.

5.2.6 When user store Fetakgomo Local Municipality confidential information on computer system (e.g. Group web sites, access database or other shared data repositories), you must use software controls to manage and limit access to the information.

5.2.7 Security controls must never be set to allow unrestricted access (e.g. World-readable, "public") To Fetakgomo local Municipality confidential information, including calendars. To understand How to correctly set or use the security controls, advice or assistance will be provided by the Information Technology office.

5.2.8 When Fetakgomo Local Municipality confidential information is stored on removable computer Media, such as diskettes, memory keys, compact disks (CDs), etc. the information must be Protected against theft and unauthorized access. Label the media confidential and keep Them in a locked area or storage device when they are not in use. Never leave them expose in Unattended areas.

5.2.9 When printing municipality confidential information the information must be protected against Theft and unauthorized viewing –the term "printer" includes printers, plotters and any other Device used to create hard copy output.

5.2.10 Fetakgomo Local Municipality confidential information may only be printed:

a. In a controlled access area, with access based on "need to know"
b. In an attended Fetakgomo Local Municipality printer facility, where the output is given only to its owner.
c. On a printer with capture/release facility that user controls.
d. On a printer that a user is personally attending.
e. If none of these options are available at a user's location, user may use a printer located within an open area internal office space, but you must pick up your Printout material within fifteen (15) minutes.

5.2.11 When participating in Fetakgomo Local Municipality confidential teleconference, confirm that All participants are authorized to participate.

5.2.12 Do not store confidential municipality information on either internet or intranet servers.

5.2.13 All Fetakgomo employees shall not forward information appearing on the intranet or internal Work related e-mail communique to the third parties without going through the appropriate Internal channels (such as Fetakgomo Local Municipality Manager or Communication division or IT Manager).

5.2.14 All Fetakgomo Local Municipality employees are responsible for ensuring that they are Utilizing the most up-to date anti-virus software in their computer's workstation. The Employees must apply updates sent via email as soon as they are received. The IT office Should be contacted if any update message is unclear or if you are unsure as to how to apply The updates.

6. VPN VIRTUAL PRIVATE NETWORK (POLICY)

6.1 PURPOSE

The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the Fetakgomo Local Municipality corporate network.

6.2 SCOPE

This policy applies to all Fetakgomo local Municipality employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Fetakgomo Local Municipality network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

6.3 POLICY

Approved Fetakgomo Local Municipality employees and authorized third parties (approved consultants.) may utilize the benefits of VPNs, which are a supplied by the Information Technology Unit as a service. This means that the Information Technology Department through the prescribed Procurement policies is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the ***Remote Access Policy***.

Additionally,

1) It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Fetakgomo Local Municipality internal networks.
2) VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3) When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4) Dual (split) tunnelling is NOT permitted; only one network connection is allowed.
5) VPN gateways will be set up and managed by Fetakgomo Municipality network operational groups.
6) All computers connected to Fetakgomo Municipality internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
7) VPN users will be automatically disconnected from Fetakgomo Municipality's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8) The VPN concentrator is limited to an absolute connection time of 24 hours.
9) Users of computers that are not Fetakgomo Municipality-owned equipment must configure the equipment to comply with Fetakgomo Municipality's VPN and Network policies.
10) Only InfoSec-approved VPN clients may be used.
11) By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Fetakgomo Municipality's network, and as such are subject to the same rules and regulations that apply to Fetakgomo Municipality-owned equipment, i.e., their machines must be configured to comply with InfoSec's Security Policies.

7. SYSTEMS DEVELOPMENT AND MAINTENANCE

7.1 Security requirements of systems

Objective: *To ensure that security is built into information systems.*

This will include infrastructure, software packages and user-developed applications. The design and implementation Of the business process supporting the application or service can be crucial for security. Security requirements should be identified and agreed prior to the development of information systems.

All security requirements, including the need for fallback arrangements, should be identified at the requirements phase of a project and justified, agree and documented as part of the overall business case.

7.2 Security requirements analysis and specification

Statements of business requirements for new systems, or enhancements to existing systems should specify the requirements for controls. Such specifications should consider the automated controls to be incorporated in the system, software packages and the need for supporting manual controls. Similar conditions should be applied when evaluating software packages for business applications.

Security requirements and controls should reflect the business value of the information assets involved, and the potential for business damage, which might result from a failure or absence of security. The framework for analysing security requirements and identifying controls to fulfill them is risk assessment and risk management.

Controls introduced at the design stage are significantly cheaper to implement and maintain than those included during or after implementation.

7.3 Security in application systems

Objective: *To prevent loss, modification or misuse of user data in application systems.*

Appropriate controls and audit trails or activity logs should be designed into application systems, including user written applications. These should include the validation of input data, internal processing and output data.

7.3.1 Input data validation

Data input to application systems should be validated to ensure that it is correct and appropriate. Checks should be applied to the input of business transactions, standing data (names and addresses, customer reference numbers) and parameter tables (rates, grades). The following controls should be considered and implemented as appropriate:

(a) dual input or other checks to detect the following errors:

  (i) out-of-range values;

  (ii) invalid characters in data fields;

  (iii) missing or incomplete data;

  (iv) exceeding upper and lower data volume limits; *and*

  (v) unauthorized or inconsistent control data.

(b) periodic review of the content of key fields or data fields to confirm their validity and integrity;

(c) inspecting hard-copy input documents for any unauthorized changes to input data (all changes to input documents should be authorized);

(d) procedures for responding to validation errors;

(e) procedures for testing the plausibility of the input data; *and*

(f) defining the responsibilities of all personnel involved in the data input process.

7.3.2 Control of internal processing

(a) Areas of risk

Data that has been correctly entered can be corrupted by processing errors or through deliberate acts. Validation checks should be incorporated into systems to detect such corruption. The design of applications should ensure that restrictions are implemented to minimize the risk of processing failures leading to a loss of integrity. Specific areas to consider include:

(i) the use and location in programs of add and delete functions to implement changes to data;

(ii) the procedures to prevent programs running in the wrong order or running after failure of prior processing; *and*

(iii) the use of "correction" programs to recover from failures to ensure the correct processing of data.

(b) Checks and controls

The controls required will depend on the nature of the application and the business impact of any corruption of data. Examples of checks that can be incorporated include:

(i) session or batch controls, to reconcile data file balances after transaction updates;

(ii) balancing controls, to check opening balances against previous closing balances, namely:

a. run-to-run controls;

b. file update totals; *and*

c. Program-to-program controls.

(iii) validation of system-generated data;

(iv) checks on the integrity of data or software downloaded, or uploaded, between central and remote computers;

(v) hash totals of records and files;

(vi) checks to ensure that application programs are run at the correct time;

(vii) checks to ensure that programs are run in the correct order; *and*

(viii) checks to ensure that programs terminate in case of a failure and that further processing is halted until the problem is resolved.

7.4 Message authentication

Message authentication is a technique used to detect unauthorized changes to, or corruption of, the contents of a transmitted electronic message. Message authentication must be considered for applications where there is a security requirement to protect the integrity of the message content, *e.g.* electronic funds transfer (EFT), or similar electronic data exchanges. An assessment of security risks should be conducted to determine if message authentication is required and to identify the most appropriate method of implementation.

7.5 Output data validation

Data output from an application system must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. Typically, systems are constructed on the premise that having undertaken appropriate validation, verification and testing the output will always be correct. This is not always the case. Output validation may include:

(a) plausibility checks to test whether the output data is reasonable;

(b) reconciliation control counts to ensure processing of all data;

(c) providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision and classification of the information;

(d) procedures for responding to output validation tests; *and*

(e) defining the responsibilities of all personnel involved in the data output process.

7.6 Cryptographic controls

Objective: *To protect the confidentiality, authenticity and integrity of information, cryptographic systems and techniques should be used for the protection of information that is considered to be at risk and for which other controls do not provide adequate protection.*

7.6.1 Policy on use of cryptographic controls

The use of cryptographic controls is determined by the security needs of the municipality, which in turn need to be determined by a risk analysis. At the present time, and in the absence of such a risk analysis, it is considered that there is no need to resort to cryptographic controls in the short to medium term but this standpoint needs to be reviewed annually.

The balance of the Cryptographic Controls section therefore covers the use thereof in general terms, rather than being specific to the municipality.

When developing a cryptographic controls policy, the following should be considered:

(a) the management approach towards the use of cryptographic controls across the organisation, including the general principles under which business information should be protected;

(b) the approach to (cryptographic) key management, including methods to deal with the recovery of encrypted information in the case of lost, compromised or damaged keys; *and*

(c) roles and responsibilities, *i.e.* who is responsible for:

  (i) the implementation of the policy;

  (ii) the key management;

  (iii) how the appropriate level of cryptographic protection is to be determined; *and*

  (iv) the standards to be adopted for the effective implementation throughout the organisation.

7.6.2 Encryption

Encryption is a technique that can be used to protect the confidentiality of information. It should be considered for the protection of sensitive or critical information.

Based on a risk assessment, the required level of protection should be identified taking into account the type and quality of the encryption algorithm used and the length of the cryptographic keys to be used.

7.6.3 Digital signatures

Digital signatures provide a means of protecting the authenticity and integrity of electronic documents, for example to verify who signed a document and to check whether the contents of the document have been altered.

Digital signatures can be applied to most forms of documents being processed electronically and can be implemented using a cryptographic techniques based on a uniquely related pair of keys where one is used to create a signature (the private key) and the other to check the signature (the public key).

Self-evidently, great care must be taken to protect the confidentiality of the private key, since anyone having access to this key can sign documents, thereby in effect forging the signature of the owner of that key. In addition, protecting the integrity of the public key is important. This protection is provided by the use of a public key certificate (see below).

7.6.4 Non-repudiation services

Non-repudiation services should be used where it might be necessary to resolve disputes about occurrence or non-occurrence of an event or action, *e.g.* a dispute involving the use of a digital signature on a document. They can help to establish evidence to substantiate whether a particular event or action has taken place, *e.g.* denial of sending a digitally signed instruction using electronic mail.

7.6.5 Key management

(a) Protection of cryptographic keys

The management of cryptographic keys is essential to the effective use of cryptographic techniques. Any compromise or loss of cryptographic keys may lead to a compromise of the confidentiality, authenticity and/or integrity of information. A management system should be in place to support the organisation's use of the two types of cryptographic techniques, which are:

(i) secret key techniques, where two or more parties share the same key and this key is used to encrypt and decrypt information. This key has to be kept secret since anyone having access to it is able to decrypt all information encrypted with this key, or to introduce unauthorized information; *and*

(ii) public key techniques, where each user has a key pair, a public key (which can be revealed to anyone) and a private key (which has to be kept secret). Public key techniques can be used for encryption and to produce digital signatures.

(b) Standards, procedures and methods

A key management system should be based on an agreed set of standards, procedures and secure methods for:

(i) generating keys for different cryptographic systems and different applications;

(ii) generating and obtaining public key certificates;

(iii) distributing keys to intended users, including how keys should be activated when received;

(iv) storing keys, including how authorized users obtain access to keys;

(v) changing or updating of keys, including rules on when keys should be changed and how this will be done;

(vi) dealing with compromised keys;

(vii) revoking keys, including how keys should be withdrawn or deactivated, *e.g.* when keys have been compromised or when a user leaves the organisation (in which case keys should also be archived);

(viii) archiving keys, *e.g.* for information archived or backed up;

(ix) destroying keys; *and*

(x) logging and auditing of key management related activities.

In order to reduce the likelihood of compromise, keys should have defined activation and deactivation dates so they can only be used for a limited period of time. This period of time should be dependent on the circumstances under which the cryptographic control is being used and the perceived risk.

Procedures may need to be considered for handling legal requests for access to cryptographic keys, *e.g.* encrypted information may need to be made available in an unencrypted form as evidence in a court case.

In addition to the issue of securely managed secret and private keys, the protection of public keys should be considered. There is a threat of someone forging a digital signature by replacing a user's public key with their own. This problem is addressed by the use of a public key certificate. These certificates should be produced in a way that uniquely binds information related to the owner of the public/private key pair to the public key. It is therefore important that the management process that generates these certificates can be trusted. This process is

normally carried out by a certification authority which should be a recognized organisation with suitable controls and procedures in place to provide the required degree of trust.

The content of Service Level Agreements or contracts with external suppliers of cryptographic services, *e.g.* with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services.

7.7 Security of system files

***Objective**: To ensure that IT projects and support activities are conducted in a secure manner, access to system files must be controlled.*

Maintaining system integrity should be the responsibility of the user function or development group to whom the application system or software belongs.

7.7.1 Control of operational software

Control must be exercised over the implementation or deployment of software on operational systems. To minimise the risk of corruption of operational systems, the following controls must be implemented:

(a) the updating of the operational program libraries shall only be performed by the nominated librarian upon appropriate authorization;

(b) operational system libraries shall contain only executable code;

(c) executable code shall not be deployed to operational systems until evidence of successful testing and user acceptance is obtained, and the corresponding program source libraries have been updated;

(d) automatic program version incrementing must be provided for in the development environment and version checking must be incorporated into the executable;

(e) an audit log should be maintained of all updates to operational program libraries; *and*

(f) previous versions of software must be retained as a contingency measure.

Vendor supplied software used in operational systems must be maintained at a level supported by the vendor. Any decision to upgrade to a new release should take into account the security of the release, *i.e.* the introduction of new security functionality or the number and severity of security problems affecting this version. Software patches should be applied when they can help to remove or reduce security weaknesses.

Physical or logical access should only be given to suppliers for support purposes when necessary, and with management approval. The supplier's activities must be monitored.

7.7.2 Protection of system test data

Test data should be protected and controlled. System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data. The use of operational data bases containing personal information must be avoided. If such information is used, it should be depersonalized before use. The following controls should be applied to protect operational data, when used for testing purposes:

(a) the access control procedures, which apply to operational systems, should also apply to test application systems;

(b) there should be separate authorizations each time operational information is copied to a test application system;

(c) operational information should be erased from a test application system immediately after the testing is completed; *and*

(d) the copying and use of operational information should be logged to provide an audit trail.

7.7.3 Access control to program source library

In order to reduce the potential for corruption of computer programs, strict control must be maintained over access to program source code libraries, as per the following:

(a) program source libraries must not be held on operational systems;

(b) access to program source libraries must be restricted to development staff only;

(c) programs under development or maintenance must not be held on operational systems;

(d) updating of program source libraries and the issuing of program sources to developers must preferably be completely automated;

(e) program listings should only be printed when absolutely necessary and disposed of securely when no longer required;

(f) audit logs must be maintained automatically of all accesses to program source libraries;

(g) old versions of programs must be automatically archived by the development environment as part of the process of source library updating; *and*

(h) maintenance and copying of program source libraries must be subject to strict change control procedures.

7.8 Security in development support processes

Objective: *To maintain the security of application system software and information.*

Project and support environments must be strictly controlled. Managers responsible for application systems must also be responsible for the security of the project or support environment and formal change control procedures must be followed.

7.8.1 Change control procedures

In order to minimize the risk of corruption of information systems, strict controls must be maintained over the implementation of changes. Developers must only be given access to those parts of the system necessary for their work, and that work must be subject to formal change control procedures.

Changing application software can impact the operational environment. Wherever possible, application and operational change control procedures should be integrated. This process should include:

(a) maintaining a record of agreed authorization levels;

(b) ensuring changes are submitted by authorized users;

(c) reviewing controls and integrity procedures to ensure they will not be compromised by the changes;

(d) identifying all computer software, information, data base entities and hardware that require amendment;

(e) obtaining formal approval for detailed proposals before work commences;

(f) ensuring that the authorized user accepts changes prior to any implementation;

(g) ensuring that implementation is carried out so as to minimize business disruption;

(h) ensuring that the system documentation set is updated on the completion of each change and that the old documentation is disposed of or archived;

(i) maintaining version control for all software updates;

(j) maintaining a record of all change requests;

(k) ensuring that operating documentation and user procedures are changed as necessary to be appropriate; *and*

(l) ensuring that the implementation of changes takes place at the right time and is not disturbing the business process involved.

7.8.2 Technical review of operating system changes

Periodically, it is necessary to change/upgrade operating systems, *e.g.* when new software releases or patches are available. When changes occur, application systems should be reviewed carefully to ensure that there is no adverse impact on operation or security. This process should cover:

(a) review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes;

(b) ensuring that the annual support plan and budget will cover reviews and system testing resulting from operating system changes;

(c) ensuring that appropriate fallback plans are in place should the upgrade fail for whatever reason and reversion to the current release be necessary;

(d) ensuring that notification of operating system changes is provided in time to allow appropriate reviews to take place before implementation; *and*

(e) ensuring that appropriate changes are made to business continuity plans.

7.8.3 Restriction on changes to software packages

Modifications to software packages should be discouraged and allowed only in exceptional circumstances. Where there is a valid business justification for modifying a software package, the following points must be considered:

(a) the risk of built-in controls and integrity processes being compromised;

(b) the ability of the vendor to support such modifications in the future, *i.e.* to support multiple versions of the package;

(c) the cost of having the vendor modify the package;

(d) the degree of dependence on the vendor for future maintenance and support on the modified package, and the cost thereof;

(e) the time involved in the vendor making the changes, and the time to respond to future support requirements;

(f) the possibility of having the vendor incorporate the modifications as standard features of the software; *and*

(g) the impact on the municipality if it becomes dependent on the modified software and the vendor either reneges on support agreements, goes out of business or demands exorbitant support fees.

If package modification is deemed essential, arrangements should be made to kept a copy of the current source code in escrow.

7.8.4 Cover channels and Trojan code

A covert channel can expose information by some indirect and obscure means. It may be activated by changing a parameter accessible by both secure and insecure elements of a computing system, or by embedding information into a data stream. Trojan code is designed to affect a system in a way that is not authorized and not readily noticed and not required by the recipient or user of a program. Covert channels and Trojan code rarely occur by accident. Where covert channels or Trojan code are a concern, the following should be considered:

(a) buying programs only from reputable sources;

(b) where possible, buying the source code so that the code may be verified;

(c) using only thoroughly evaluated products;

(d) where possible, inspecting all source code before operational use;

(e) controlling access to, and modification of, source code once installed; *and*

(f) using staff of proven trustworthiness to work on key systems.

7.8.5 Outsourced software development

Where software development is outsourced, the following points must be considered:

(a) licensing arrangements, code ownership and intellectual property rights;

(b) certification of the quality and accuracy of the work carried out;

(c) escrow arrangements in the event of failure of the third party;

(d) rights of access for audit of the quality and accuracy of the work done;

(e) contractual requirements for the quality of code; *and*

(f) testing before installation to detect Trojan code.

7.9 BUSINESS CONTINUITY MANAGEMENT

7.9.1 Aspects of business continuity management

Objective: *To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.*

A business continuity management process must be implemented to reduce the potential for disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery controls.

The consequences of disasters, security failures and loss of service should be analysed. Contingency plans must be developed and implemented to ensure that essential business processes can be restored within the required timescales. Such plans must be maintained and practiced to become an integral part of all other management processes.

Business continuity management must include controls to identify and reduce risks, limit the consequences of damaging accidents, and ensure the timely resumption of essential operations.

7.9.2 Business continuity management process

A managed process for developing and maintaining business continuity throughout the municipality needs to be in place. It should bring together the following key elements of business continuity management:

(a) understanding the risks the municipality is facing in terms of their likelihood and their impact, including an identification and prioritization of critical business processes;

(b) understanding the impact which interruptions are likely to have on the municipality's business – both smaller incidents and more serious incidents that could threaten the viability of the municipality – and establishing the business objectives of information processing facilities;

(c) considering the purchase of suitable insurance which may form part of the business continuity process;

(d) formulating and documenting a business continuity strategy consistent with the agreed business objectives and priorities;

(e) formulating and documenting business continuity plans in line with the agreed strategy;

(f) regular testing and updating of the plans and processes put in place; *and*

(g) ensuring that the management of business continuity is incorporated in the municipality's processes and structure.

8. WEB SITE USE POLICY

8.1 INTRODUCTION

The Fetakgomo Local Municipality Web Site is one of the most important means of internal communication and accordingly specific policies and procedures apply regarding what can be published to the site and how this content is managed and maintained.

8.2 SUBMISSION OF CONTENT AND USE OF THE SITE

1) The Site is to be used for lawful purposes only. However, should the user choose to use this Site from locations other than the Republic of South Africa, they do so at their own initiative and you are responsible for compliance with applicable local laws.

2) Users are prohibited from posting or transmitting , by means of reviews, comments, suggestions, ideas, questions or other information through the site, any content which is, unlawful, harmful, threatening, abusive, harassing, defamatory, vulgar, obscene, sexually explicit, profane, hateful, racially, ethnically or otherwise objectionable content of any kind, including but not limited to:

   (a) Any content that encourages conduct that would constitute a criminal offence or give rise to civil liability, or otherwise violate any applicable local, provincial, national, or international law: or
   (b) Any content that constitutes an invasion of privacy right; or
   (c) Any content that contains software viruses; or
   (d) Any content that constitutes a political statement, commercial solicitation, or Spam-

3) Although Fetakgomo local municipality does not purport to review (nor is it under any obligation to do so) any submitted content, it reserves the right to remove any content from the site that deems, in its sole discretion, to be an infringement of the above or harmful in anyway whatsoever. Should this policy be breached then Fetakgomo local municipality may

immediately terminate and/or suspend the user's access to all or parts of the site, without any further notice.

Each user must warrant that:

a) They own or otherwise control all rights to the content that they may submit to the site;
b) That any use of such content will not cause injury or harm to any person or entity; and
c) They will indemnity Fetakgomo local municipality or its affiliates, directors, officers and employees, for all claims resulting from the submitted content.

4) By submitting reviews, comments and/or any other content (other than personal details) to Fetakgomo local municipality for posting on the site, the user automatically grants Fetakgomo local municipality and its affiliates a non-exclusive, royalty – free, perpetual, irrevocable right and license to use, reproduce, publish, translate, sublicense, copy and distribute such content in whole or in part worldwide, and to incorporate it in other works in any form, media, or technology now known or hereinafter developed for the full term of any copyright that may exist in such content. Subject to this license being granted, the user retains any and all rights that may exist in such content.

5) The following activity on or through the site is expressly prohibited:
   (a) Any non-personal or commercial use of any robot, spider, other automatic device or technology, or manual process to monitor or copy portions of the site, or the content contained therein, without the prior written authority of Fetakgomo local municipality; and
   (b) The collection or use of any listings, descriptions, or price list from the site, for the benefit of a competing merchant that supplies products comparable to those offered on the site; and
   (c) Any use or action that imposes an unreasonable or disproportionately large load of traffic on the site, or otherwise interferes with its proper and timely functioning.

6) The user is responsible for maintaining the confidentiality and security of their User Name and Password for access to the site, and accepts full liability for all activities that occur under their User Name.

7) Any person that delivers or attempts to deliver any damaging code to this web site or attempts to gain unauthorized access to any page on this web site shall be prosecuted and civil damages shall be claimed in the event that Fetakgomo local municipality suffers any damage or loss.

8.3 THE USE OF THIRD PARTY CONTENT

a) Fetakgomo local municipality host information, pricing, opinions and other content supplied by third parties ("Third Party Content") on the site. Fetakgomo local municipality has no editorial over such content. Fetakgomo local municipality will, therefore, not be responsible for any incorrect pricing due to typographical errors or errors in pricing.

b) Opinions, statements, offers or any other information that may constitute Third Party Content, is that of the respective user and not of Fetakgomo local municipality, its affiliates or any of their directors, officers, employees or agents. Fetakgomo local municipality, its affiliates, or any directors, officers, employees, agents, do not guarantee the accuracy, completeness, and/or usefulness of any Third Party Content. All Third Party Contentment is provided as is.

c) It is the users' responsibility to evaluate Third Party Content available on and through the Site. Fetakgomo local municipality and its affiliates, and their directors, officers and employees are not liable for any loss, damage or harm caused by any User reliance on Third Party Content obtained on or through the site. Before making any decision or placing reliance on Third Party Content provided on or through the site, users should take all further reasonable steps to ensure and verify the accuracy of such content. This notice must be displayed in its entirety should one wish to publish any Third Party Content obtained from the site.

d) Fetakgomo local municipality does not review (nor is it under any obligation to do so) or control any third-party web sites that link to or from the site. Fetakgomo local municipality is not responsible for the content of any Third Party site linked to or from the site.

8.4 SERVICES ADVERTISED BY MEANS OF THE SITE

The price and potential availability for each listing on the site is listed on that particular item's page. Fetakgomo local municipality cannot guarantee the availability of every or any listing on the site.

8.5 INTELLECTUAL PROPERTY RIGHTS

a) All content included on this web site, such as text, graphics, logos, buttons, icons, images, photographs, audio clips, databases and software("the content"), is the property of Fetakgomo local municipality or its content supplier and protected by South Africa and international copyright laws. Furthermore, the compilation (meaning the collection, arrangement, and assembly) of all content on this web site is the exclusive property of Fetakgomo local municipality and is protected by South Africa and international copyright laws.

b) Except as stated herein, none of the material may be copied, reproduced, distributed, republished, downloaded, displayed, posted or transmitted in any form or by any means, including, but not limited to, electronic, mechanical, photocopying, recording, or otherwise, except as permitted by the fair use privilege under the South Africa copyright laws or without the prior written permission of Fetakgomo local municipality or the copyright owner.

c) Users are expressly prohibited to "minor" any content, contained on the site, on any other server unless with the prior written permission of Fetakgomo local municipality.

d) Users are granted a limited, revocable, and non-exclusive right to create a hyperlink to the home page of the site so long as the link does not portray Fetakgomo local municipality, its affiliates, or their products or services in a false, misleading, derogatory, or otherwise offensive matter. Users may not use any Fetakgomo local municipality logo or other proprietary graphic or trademark as part of the link without the express permission of Fetakgomo local municipality, its affiliates or content supplier.

e) All trademarks are the exclusive property of Fetakgomo local municipality or the trademark holder.

f) The unauthorized submission, removal, modification or distribution of copyrighted or other proprietary content is illegal and the user could be subject to criminal prosecution as well as personal liability for damages.

8.6 LIMITTED LIABILITY

The information, content, services, products and materials published on the site, including without limitation, text, graphics and links are provided on an "as is" basis. Fetakgomo local municipality makes no representations or warranties of any kind, express or implied, as to the operation of the site or the accuracy, correctness or completeness of the information, content, materials, or products included on the site. Without limiting the generality of the foregoing:

a) Fetakgomo local municipality does not warrant that the site, will be error free, or will meet any particular criteria of accuracy, completeness or reliability of information, performance or quality; and

b) Whilst Fetakgomo local municipality has taken reasonable measures to ensure the integrity of the site and its contents, no warranty, whether express or implied, is given that any files, downloads or applications available via the site are free of viruses, Trojans, bombs, time-locks or any other date or code which has the ability to corrupt or affect the operation of your system.

c) To the full extent permissible by applicable law, Fetakgomo local municipality disclaims all warranties, express or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose. Fetakgomo local municipality will not be liable for any damages of any kind arising from the use of the Fetakgomo local municipality site, including, but not limited to direct, incidental, punitive, and consequential damages.

8.7 PRIVACY

8.7.1 Fetakgomo local municipality respects the privacy of its users. Without limiting the a foregoing:

a) Fetakgomo local municipality is dedicated to maintain the privacy of its online visitors and users. On this site, Fetakgomo local municipality does not collect personally identifiable information from individuals unless they provide it to us voluntarily and knowingly.

b) Any information collected is used solely by Fetakgomo local municipality and its business partners who are involved in the operation of this site for internal purposes. Fetakgomo local

municipality's client lists are never sold to third parties unless the person who has submitted the information has authorized Fetakgomo local municipality to do so, or if Fetakgomo local municipality is required to by law.

8.8 GOVERNING LAW

This site hosted, controlled and operated from the Republic of South Africa and therefore governed by South African law.

8.9 HYPERLINKS

No person, business or web site may link to any page on this site without the prior written permission of Fetakgomo local municipality. Such permission could be obtained from the Municipal Manager. This clause does not apply to parties that have entered into e-trader agreements with Fetakgomo local municipality.

Hyperlinks provided on this site to non- Fetakgomo local municipality sites are provided as is and Fetakgomo local municipality does not necessarily agree with, edit or sponsor the content on such pages.

8.10 FRAMING

No person, business or web site may frame this site or any of the pages on this site in any way whatsoever.

8.11 SPIDERS AND CRAWLERS

No person, business or web site may use any technology to search and gain any information from this site without the prior written permission of Fetakgomo local municipality.

9. IT PROCUREMENT POLICY AND PROCEDURE

9.1 INTRODUCTION

'Procurement' is the term we use to cover the entire process of buying goods and services from our suppliers.

a) Fetakgomo local municipality aims to provide its supplier, both current and prospective, with up to date information on our requirements and procurement policies and procedures under which we seek to meet those needs. We also aim to develop a strong, mutually beneficial relationship with our suppliers based on openness, fairness and transparency in the conduct of our procurement process.

b) We believe our supplier are an essential partner in making Fetakgomo local municipality and intend this information as an aid in contributing to enhance the capabilities of our suppliers in supplying our business requirements.

c) This policy guide is also intended to help Fetakgomo local municipality support the Government's procurement policy, as municipal managers are responsible and strictly accountable for the efficient and effective operation of their authorities, and have substantial managerial discretion in operational matters such as procurement. Accordingly, this guide generally does not set down prescriptive purchasing rules or procedures, except as set out in the supply chain policy. The only exceptions are certain mandatory information and notification requirements which cabinet has decided should apply to local government departments.

d) The procurement policy has general application to acquisition by purchase, hire, lease, rental, exchange and competitive tendering and contracting (outsourcing) arrangements. In this policy the focus is on purchasing by Fetakgomo local municipality of goods and services either directly or through a third party, and the terms "procurement" and "purchasing" used interchangeably.

e) This policy has also endorsed certain principles namely: transparency, value for money, open and effective competition, fair dealing, accountability and due process, and non-discrimination.

f) The procurement policy approach supports Fetakgomo local municipality sustainable industry and regional development objectives, through enhanced identification of competitive opportunities for local enterprises and their capabilities to exploit those opportunities.

9.2 OBJECTIVES OF FETAKGOMO LOCAL MUNICIPALITY'S PURCHASING POLICIES AND PROCEDURES

Our policies and procedures have been developed to ensure that all our purchasing activities achieve the following goals:

(a) Procuring goods and services, which best contributed to Fetakgomo local municipality's performance.

(b) To procure as efficiently as possible and to obtain best value for money, over whole of life, without compromising appropriate quality/standards.

(c) To eliminate waste.

(d) To encourage open and effective competition.

(e) To provide for full and fair opportunity for domestic supplier based within Fetakgomo.

(f) To improve business capabilities, including e-commerce capability.

(g) To ensure good financial and budgetary control.

(h) To ensure that BEE companies are given ample opportunity to tender for business with Fetakgomo local municipality.

(i) To ensure compliance with State and Municipal Directives (MMFA).

(j) To maintain ethical business standard and full legal compliance.

Fetakgomo local municipality should also note that environmental issues are an increasingly important element in procurement policy, and they should ensure that their procurement is consistent with the environmental policies and procedures of the government.

9.3 PURCHASE POLICY STATEMENTS

We at Fetakgomo Local Municipality believe in:

a) Fair Trade
b) Mutual Prosperity
c) Obeying Laws
d) Keeping Trust/ Confidentiality
e) Expanding business opportunities within Fetakgomo

1) We promise potential supplier an open and impartial opportunity to supply, based on economic factors such as quality, price, and delivery time, continuity/stability of supply as

well as continuity of management and technological compatibility and development capability.

2) We wish to establish good business relationships based on mutual trust and we aim to negotiate for mutually acceptable and beneficial condition of business.

3) We look for supplier who can best co-operate with us on mutual trust and help us to achieve our organizational goals and objectives.

4) In our purchasing activities as in all our areas of business, we make it a firm rule to obey the laws and respect their spirit. We also respect the confidentiality relating to products and technologies which we obtain and will not disclose such confidential information to third parties without prior agreement of the supplier concerned bearing in mind that we are subject to the Access to Information Act.

10. INCIDENT HANDLING POLICY AND PROCEDURE

10.1 INTRODUCTION

The aim of this policy is to:

a) Allow Fetakgomo local municipality to keep a record of all faults/problems and systems changes to document such changes.
b) Allow the IT Manager to monitor all computer faults within the departments so that any matter arising can be monitored.
c) Allow the IT office to monitor all requests vendors.
d) Monitor cost to establish if it is still economically viable to repair certain equipment, or to allow management to make decisions to replace equipment that is no longer economically viable to be repaired or outdated and obsolete.

10.2 POLICY STATEMENTS

10.2.1 The following statements describe the incident handing policy:

a) The occurrence of all incidents and change and service requests must be logged with the IT Office on 015 622 8045 or 8094. This policy covers a new service being required, a problem being experienced or further information being requested.
b) No action will be taken or assistance and support provided unless it is logged.

10.2.2 Depending on the nature of the problem or request, there are different procedures to follow when requesting a change, service or information or reporting a fault or a problem. However the policy is that:

a) The staff member must report the problem/ fault to IT Office and the user will be requested to fill in the IT log book. This can be done verbally, in writing, via e-mail or telephonically.
b) The IT office will then attend to the problem.

In addition, no staff member may request any work directly from any ICT vendor without first following the above policy.

10.2.3 The vendors have been instructed that any requests attended to without the proper policy and procedure having been followed will not be for the account of Fetakgomo local municipality. In cases where a staff member does not follow this procedure, any charge levied by the vendor, will be for the account of the relevant staff member.

10.3 GENERAL GUIDELINES

During an emergency situation the following guidelines and principles are advised:

a) Remain calm – A compromised system is a call to action but not a cause for panic.
b) Take good notes – Take detailed, organized and complete notes while handling any computer security incident preferably in an automated manner following a template so that no critical details is missed especially if it may be required as evidence in the future. The documentation should be time stamped and auditable.
c) Notify the right people and get help – Inform those who 'need to know' about the incident. Again this should be an automated process.
d) Enforce a 'need to know' policy – This is one of the hardest things about handling an incident as they can be misdiagnosed early on. It is better therefore to inform those who need to be appraised of the situation so as to manage consistent communication.

e) Use out-of-band communication – whenever possible, use telephones and faxes during a computer security incident. If the attackers have full access to the Help Desk's computer and they can read the mail. If the Help Desk's computers are used' this allows the intruder to know when the incident is reported and what response is received.

f) Contain the problem – The first time that the compromised computer is touched, it should be to disconnect it from the network, even if is a core infrastructure resource. In order to contain the problem and regain control, all communication between the compromised host and other hosts on the network must be stopped.

g) Make backups – Make backups of the system information as well as file-system information. Process tables, network connections, the/tmp directory and other volatile data sources should be dumped to files and then backed up with the rest file-system. Make multiple full backups using at least two different methods. Ensure file-system integrity with the first method and analytical portability with the second method. Any executable employed in the incident handling process should be trusted software. Once the file-system is backed up in a variety of manners, the computer can be halted.

h) Get rid of the problem – The problem must be completely eradicated. Determine the cause of the incident, then reload a clean operating system and improve the system's defences by installing the appropriate software. Only then can the system be reconnected to the network.

i) Get back in business – The goal is to make the recovered system resistant enough so that Fetakgomo local municipality has a fair chance of determining that it is under attack before it falls.

10.4 INCIDENT HANDLING PROCEDURE

10.4.1 The following phases are the constituents of Fetakgomo local municipality's incident handling
Procedure:

10.4.1.1 Phase 1 Identification

a) Assign a person to be responsible for the incident matching the person's skill set with the incident.

b) Determine the extent of the incident utilizing diagnostic tool kits.

c) Be careful to maintain a provable chain of custody particularly when it relates to a security incident as the evidence may be required in a court of law. Examples of this could be:

d) Identify every piece of evidence with a witness.

e) Sign, seal and date a copy of everything.

f) Place everything in a tamper-proof locked place that only a very limited number of people have access to (and be able to prove only a limited number of people have access).

g) Coordinate with the people who provide your network services as they can proactively block incoming and outgoing traffic and can help trace security violators.

10.4.1.2 Phase 2 Containment

a. Deploy the On-Site Fetakgomo local municipality team to survey the situation avoiding disruption of normal routines. Task somebody to be the 'recording secretary' so that nothing is left to memory possibly using an incident Containment Form template and Incident Survey Form that was filled in by the incident handler.

b. Keep a low profile so as to contain the problem and not raise tension at Fetakgomo local municipality unnecessarily.

c. Avoid potentially compromised code so as not to risk 'spreading' the incident's impact.

d. Back up the system.

e. Determine the risk of continuing the operation of the system. The On-Site Fetakgomo local municipality team only provides a recommendation and presents the data to justify the recommendation and the Fetakgomo local municipality IT executive must make the actual decision itself.

f. Continue to consult with the System Owners so that they are informed and will not disrupt the team that is handling the incident.

10.4.1.3 Phase 3 Eradication

a. Determine the cause and symptoms of the incident.

b. Improve defenses.

c. Perform vulnerability analysis.

d. Remove the cause of the incident.

e. Locate the most recent clean backup.

10.4.1.5 Phase 4 Recovery

a) Restore the system.
b) Validate the system.
c) Decide when to restore operations when it would have least business impact.
d) Monitor the systems.

10.4.1.5 Phase 5 Follow-up

a) Develop a follow-up report.

11. INSURANCE POLICY AND PROCEDURE

11.1 INTRODUCTION

Fetakgomo Local municipality employees are responsible for the safekeeping and correct usage of the Fetakgomo local municipality's information technology assets. Should an asset be damaged or lost, the procedures below must be followed, whether or not an insurance claim is to be made, and irrespective as to the reasons why the assets was lost or damaged.

11.2 RISKS

11.2.1 The risks of not following these policies and procedures are:

b) An employee may find themselves personally liable for costs associated with the loss.
c) The Fetakgomo local municipality's insurance company may repudiate valid insurance claims.
d) Unnecessary delays in the replacement/repair of the asset may take place.
e) Fraud and theft may go undetected.

11.3 POLICY STATEMENTS

a. The employee must immediately inform their manager, Fetakgomo security, and asset register in supply chain the moment the loss or damage is apparent.
b. In the event of loss or suspected deliberate damage, the employee must inform the SA police, within 24 hours, and a case number must be obtained.
c. The employee must submit the written report together with the affidavit from the SA police detailing the incident happened to IT office.
d. IT office will investigate, quote on missing items and remove all in-operable salvageable equipment to storage (prevent further theft).

11.4 RISKS

Should the procedure and checklist below not be followed, Fetakgomo local municipality is exposed to the following major risks:

a) Fraud – through the unauthorized usage of Fetakgomo local municipality systems and assets
b) Financial Loss – through the utilization of assets and facilities that are no longer applicable.
c) Information loss – through the unauthorized dissemination of confidential Fetakgomo local municipality information.

11.5 POLICY AND PROCEDURE STATEMENTS

a. Manager contact HR to initiate the normal Fetakgomo local municipality separation process.
b. HR to complete Part 'A" of ICT checklist.
c. HR forward to IT Office, via E-mail.
d. IT office initiates actions and completes part B
e. IT office returns form to initiating HR party
f. Fetakgomo local municipality HR signs and attaches completed form to normal exit/contract termination documentation.
g. Fetakgomo local municipality files documentation according to normal Fetakgomo local municipality HR procedures.

11.6 Fetakgomo Local Municipality Separation Form – IT Procedures

Fetakgomo Local Municipality Employee Separation Form – IT Procedures			
Part A – to be completed by HR Department			
Employee Name			
Employee Number			
Exit Date			
Phone			
Cell Number			
Manager			
Department			
Office Location			
Part B – to be completed by IT Office			
IT Assets			
Equipment Type	Asset Number	Serial Number	Date Returned
Desktop			
Laptop			
Printer			
PDA			
Other - specify			
Software			
Access to	User ID	Date Cancelled	Comments
E-mail			
Internet			
Financial System			
HR System			
Network (AD)			
Sign Off			
IT Manager			
Depart Manager			
HR Manager			
Internal Audit			
Notes			
Location of Equipment:			
Equipment to be transferred to:			

12. SYSTEMS DEVELOPMENT AND MAINTENANCE

12.1 Security requirements of systems

Objective: To ensure that security is built into information systems.

a) This will include infrastructure, software packages and user-developed applications. The design and implementation Of the business process supporting the application or service can be crucial for security. Security requirements should be identified and agreed prior to the development of information systems.

b) All security requirements, including the need for fallback arrangements, should be identified at the requirements phase of a project and justified, agree and documented as part of the overall business case.

12.2 Security requirements analysis and specification

a) Statements of business requirements for new systems, or enhancements to existing systems should specify the requirements for controls. Such specifications should consider the automated controls to be incorporated in the system, software packages and the need for supporting manual controls. Similar conditions should be applied when evaluating software packages for business applications.

b) Security requirements and controls should reflect the business value of the information assets involved, and the potential for business damage, which might result from a failure or absence of security. The framework for analysing security requirements and identifying controls to fulfil them is risk assessment and risk management.

c) Controls introduced at the design stage are significantly cheaper to implement and maintain than those included during or after implementation.

12.3 Security in application systems

1) Objective: To prevent loss, modification or misuse of user data in application systems.

Appropriate controls and audit trails or activity logs should be designed into application systems, including user written applications. These should include the validation of input data, internal processing and output data.

12.4 Input data validation

1) Data input to application systems should be validated to ensure that it is correct and appropriate. Checks should be applied to the input of business transactions, standing data

(names and addresses, customer reference numbers) and parameter tables (rates, grades).

a) The following controls should be considered and implemented as appropriate:

dual input or other checks to detect the following errors:

out-of-range values;

invalid characters in data fields;

missing or incomplete data;

2) Exceeding upper and lower data volume limits; and unauthorized or inconsistent control data.

a) periodic review of the content of key fields or data fields to confirm their validity and integrity;

inspecting hard-copy input documents for any unauthorized changes to input data (all changes to input documents should be authorized);

procedures for responding to validation errors;

procedures for testing the plausibility of the input data; and

defining the responsibilities of all personnel involved in the data input process.

Control of internal processing

12.5 Areas of risk

1) Data that has been correctly entered can be corrupted by processing errors or through deliberate acts. Validation checks should be incorporated into systems to detect such corruption. The design of applications should ensure that restrictions are implemented to minimize the risk of processing failures leading to a loss of integrity. Specific areas to consider include:

the use and location in programs of add and delete functions to implement changes to data;

the procedures to prevent programs running in the wrong order or running after failure of prior processing; and

the use of "correction" programs to recover from failures to ensure the correct processing of data.

2) Checks and controls

The controls required will depend on the nature of the application and the business impact of any corruption of data. Examples of checks that can be incorporated include:

session or batch controls, to reconcile data file balances after transaction updates;

balancing controls, to check opening balances against previous closing balances, namely:

run-to-run controls;

file update totals; and

program-to-program controls.

validation of system-generated data;

3) checks on the integrity of data or software downloaded, or uploaded, between central and remote computers;

hash totals of records and files;

checks to ensure that application programs are run at the correct time;

checks to ensure that programs are run in the correct order; and

checks to ensure that programs terminate in case of a failure and that further processing is halted until the problem is resolved.

4) Message authentication

Message authentication is a technique used to detect unauthorized changes to, or corruption of, the contents of a transmitted electronic message. Message authentication must be considered

for applications where there is a security requirement to protect the integrity of the message content, e.g. electronic funds transfer (EFT), or similar electronic data exchanges. An assessment of security risks should be conducted to determine if message authentication is required and to identify the most appropriate method of implementation.

12.6 Output data validation

Data output from an application system must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. Typically, systems are constructed on the premise that having undertaken appropriate validation, verification and testing the output will always be correct. This is not always the case. Output validation may include:

plausibility checks to test whether the output data is reasonable;

reconciliation control counts to ensure processing of all data;

providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision and classification of the information;

procedures for responding to output validation tests; and

defining the responsibilities of all personnel involved in the data output process.

12.7 Cryptographic controls

Objective: To protect the confidentiality, authenticity and integrity of information, cryptographic systems and techniques should be used for the protection of information that is considered to be at risk and for which other controls do not provide adequate protection.

Policy on use of cryptographic controls

The use of cryptographic controls is determined by the security needs of the municipality, which in turn need to be determined by a risk analysis. At the present time, and in the absence of such a risk analysis, it is considered that there is no need to resort to cryptographic controls in the short to medium term but this standpoint needs to be reviewed annually.

The balance of the Cryptographic Controls section therefore covers the use thereof in general terms, rather than being specific to the municipality.

When developing a cryptographic controls policy, the following should be considered:

the management approach towards the use of cryptographic controls across the organisation, including the general principles under which business information should be protected;

the approach to (cryptographic) key management, including methods to deal with the recovery of encrypted information in the case of lost, compromised or damaged keys; and

roles and responsibilities, i.e. who is responsible for:

the implementation of the policy;

the key management;

how the appropriate level of cryptographic protection is to be determined; and

the standards to be adopted for the effective implementation throughout the organisation.

12.8 Encryption

Encryption is a technique that can be used to protect the confidentiality of information. It should be considered for the protection of sensitive or critical information.

Based on a risk assessment, the required level of protection should be identified taking into account the type and quality of the encryption algorithm used and the length of the cryptographic keys to be used.

12.9 Digital signatures

1) Digital signatures provide a means of protecting the authenticity and integrity of electronic documents, for example to verify who signed a document and to check whether the contents of the document have been altered.

2) Digital signatures can be applied to most forms of documents being processed electronically and can be implemented using a cryptographic techniques based on a uniquely related pair of keys where one is used to create a signature (the private key) and the other to check the signature (the public key).

3) Self-evidently, great care must be taken to protect the confidentiality of the private key, since anyone having access to this key can sign documents, thereby in effect forging the signature of

the owner of that key. In addition, protecting the integrity of the public key is important. This protection is provided by the use of a public key certificate (see below).

4) Non-repudiation services

Non-repudiation services should be used where it might be necessary to resolve disputes about occurrence or non-occurrence of an event or action, e.g. a dispute involving the use of a digital signature on a document. They can help to establish evidence to substantiate whether a particular event or action has taken place, e.g. denial of sending a digitally signed instruction using electronic mail.

5) Key management

Protection of cryptographic keys

The management of cryptographic keys is essential to the effective use of cryptographic techniques. Any compromise or loss of cryptographic keys may lead to a compromise of the confidentiality, authenticity and/or integrity of information. A management system should be in place to support the organisation's use of the two type of cryptographic techniques, which are:

secret key techniques, where two or more parties share the same key and this key is used to encrypt and decrypt information. This key has to be kept secret since anyone having access to it is able to decrypt all information encrypted with this key, or to introduce unauthorized information; and

public key techniques, where each user has a key pair, a public key (which can be revealed to anyone) and a private key (which has to be kept secret). Public key techniques can be used for encryption and to produce digital signatures.

6) Standards, procedures and methods

A key management system should be based on an agreed set of standards, procedures and secure methods for:

generating keys for different cryptographic systems and different applications;

7) generating and obtaining public key certificates;

distributing keys to intended users, including how keys should be activated when received;

storing keys, including how authorized users obtain access to keys;

changing or updating of keys, including rules on when keys should be changed and how this will be done;

8) dealing with compromised keys;

revoking keys, including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves the organisation (in which case keys should also be archived);

archiving keys, e.g. for information archived or backed up;

destroying keys; and

9) logging and auditing of key management related activities.

In order to reduce the likelihood of compromise, keys should have defined activation and deactivation dates so they can only be used for a limited period of time. This period of time should be dependent on the circumstances under which the cryptographic control is being used and the perceived risk.

10) Procedures may need to be considered for handling legal requests for access to cryptographic keys, e.g. encrypted information may need to be made available in an unencrypted form as evidence in a court case.

11) In addition to the issue of securely managed secret and private keys, the protection of public keys should be considered. There is a threat of someone forging a digital signature by replacing a user's public key with their own. This problem is addressed by the use of a public key certificate. These certificates should be produced in a way that uniquely binds information related to the owner of the public/private key pair to the public key. It is therefore important that the management process that generates these certificates can be trusted. This process is normally carried out by a certification authority which should be a recognized organisation with suitable controls and procedures in place to provide the required degree of trust.

12) The content of Service Level Agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services.

13) Security of system files

a) Objective: To ensure that IT projects and support activities are conducted in a secure manner, access to system files must be controlled.

b) Maintaining system integrity should be the responsibility of the user function or development group to whom the application system or software belongs.

c) Control of operational software

Control must be exercised over the implementation or deployment of software on operational systems. To minimise the risk of corruption of operational systems, the following controls must be implemented:

d) the updating of the operational program libraries shall only be performed by the nominated librarian upon appropriate authorization;

operational system libraries shall contain only executable code;

e) executable code shall not be deployed to operational systems until evidence of successful testing and user acceptance is obtained, and the corresponding program source libraries have been updated;

f) automatic program version incrementing must be provided for in the development environment and version checking must be incorporated into the executable;

g) an audit log should be maintained of all updates to operational program libraries; and

previous versions of software must be retained as a contingency measure.

h) Vendor supplied software used in operational systems must be maintained at a level supported by the vendor. Any decision to upgrade to a new release should take into account the security of the release, i.e. the introduction of new security functionality or the number and severity of security problems affecting this version. Software patches should be applied when they can help to remove or reduce security weaknesses.

Physical or logical access should only be given to suppliers for support purposes when necessary, and with management approval. The supplier's activities must be monitored.

i) Protection of system test data

Test data should be protected and controlled. System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data. The use of operational data bases containing personal information must be avoided. If such information is used, it should be depersonalized before use. The following controls should be applied to protect operational data, when used for testing purposes:

the access control procedures, which apply to operational systems, should also apply to test application systems;

there should be separate authorizations each time operational information is copied to a test application system;

operational information should be erased from a test application system immediately after the testing is completed; and

the copying and use of operational information should be logged to provide an audit trail.

j) Access control to program source library

In order to reduce the potential for corruption of computer programs, strict control must be maintained over access to program source code libraries, as per the following:

program source libraries must not be held on operational systems;

access to program source libraries must be restricted to development staff only;

programs under development or maintenance must not be held on operational systems;

updating of program source libraries and the issuing of program sources to developers must preferably be completely automated;

program listings should only be printed when absolutely necessary and disposed of securely when no longer required;

k) audit logs must be maintained automatically of all accesses to program source libraries;

old versions of programs must be automatically archived by the development environment as part of the process of source library updating; and

maintenance and copying of program source libraries must be subject to strict change control procedures.

12. 9 Security in development and support processes

Objective: To maintain the security of application system software and information.

Project and support environments must be strictly controlled. Managers responsible for application systems must also be responsible for the security of the project or support environment and formal change control procedures must be followed.

12.10 Change control procedures

1. In order to minimize the risk of corruption of information systems, strict controls must be maintained over the implementation of changes. Developers must only be given access to those parts of the system necessary for their work, and that work must be subject to formal change control procedures.

2. Changing application software can impact the operational environment. Wherever possible, application and operational change control procedures should be integrated. This process should include:

a) maintaining a record of agreed authorization levels;
b) ensuring changes are submitted by authorized users;
c) reviewing controls and integrity procedures to ensure they will not be compromised by the changes;
d) identifying all computer software, information, data base entities and hardware that require amendment;
e) obtaining formal approval for detailed proposals before work commences;
f) ensuring that the authorized user accepts changes prior to any implementation;
g) ensuring that implementation is carried out so as to minimize business disruption;

h) ensuring that the system documentation set is updated on the completion of each change and that the old documentation is disposed of or archived;
i) maintaining version control for all software updates;
j) maintaining a record of all change requests;
k) ensuring that operating documentation and user procedures are changed as necessary to be appropriate; and
l) ensuring that the implementation of changes takes place at the right time and is not disturbing the business process involved.

12.11 Technical review of operating system changes

1. Periodically, it is necessary to change/upgrade operating systems, e.g. when new software releases or patches are available. When changes occur, application systems should be reviewed carefully to ensure that there is no adverse impact on operation or security. This process should cover:

a) review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes;
b) ensuring that the annual support plan and budget will cover reviews and system testing resulting from operating system changes;
c) ensuring that appropriate fallback plans are in place should the upgrade fail for whatever reason and reversion to the current release be necessary;
d) ensuring that notification of operating system changes is provided in time to allow appropriate reviews to take place before implementation; and
e) ensuring that appropriate changes are made to business continuity plans.

2. Restriction on changes to software packages

2.2 Modifications to software packages should be discouraged and allowed only in exceptional circumstances. Where there is a valid business justification for modifying a software package, the following points must be considered:

a) the risk of built-in controls and integrity processes being compromised;

b) the ability of the vendor to support such modifications in the future, i.e. to support multiple versions of the package;
c) the cost of having the vendor modify the package;
d) the degree of dependence on the vendor for future maintenance and support on the modified package, and the cost thereof;
e) the time involved in the vendor making the changes, and the time to respond to future support requirements;
f) the possibility of having the vendor incorporate the modifications as standard features of the software; and
g) the impact on the municipality if it becomes dependent on the modified software and the vendor either reneges on support agreements, goes out of business or demands exorbitant support fees.

If package modification is deemed essential, arrangements should be made to kept a copy of the current source code in escrow.

3. Covert channels and Trojan code

3.3 A covert channel can expose information by some indirect and obscure means. It may be activated by changing a parameter accessible by both secure and insecure elements of a computing system, or by embedding information into a data stream. Trojan code is designed to affect a system in a way that is not authorized and not readily noticed and not required by the recipient or user of a program. Covert channels and Trojan code rarely occur by accident. Where covert channels or Trojan code are a concern, the following should be considered:

a) buying programs only from reputable sources;
b) where possible, buying the source code so that the code may be verified;
c) using only thoroughly evaluated products;
d) where possible, inspecting all source code before operational use;
e) controlling access to, and modification of, source code once installed; and
f) using staff of proven trustworthiness to work on key systems.

4. Outsourced software development

4.4 Where software development is outsourced, the following points must be considered:

a) licensing arrangements, code ownership and intellectual property rights;
b) certification of the quality and accuracy of the work carried out;
c) escrow arrangements in the event of failure of the third party;
d) rights of access for audit of the quality and accuracy of the work done;
e) contractual requirements for the quality of code; and
f) testing before installation to detect Trojan code.

13. COMMUNICATIONS AND OPERATIONA MANAGEMENT

13.1 Operational procedures and responsibilities

Objective: *To ensure the correct and secure operation of information processing facilities.*

Responsibilities and procedures for the management of all information processing facilities should be established, including the development of appropriate operating instructions and incident response procedures. Segregation of duties must be implemented to reduce risk of negligent or deliberate system misuse.

13.1.1 Documented operating procedures

Operating procedures shall be documented and maintained. Changes shall be formally authorized by management. The procedures shall specify the detailed instructions for the execution of each job, including:

(a) processing and handling of information;
(b) scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;

(c) instructions for handling errors or other exceptional conditions, which might arise during job execution;

(d) support contacts in the event of unexpected operational or technical difficulties;

(e) special output handling instructions, such as special stationery or the management of confidential output;

(f) procedures for secure disposal of output from failed jobs;

(g) system restart and recovery procedures for use in the event of system failure; *and*

(h) procedures for system housekeeping activities, such as computer start-up and close-down procedures, back-up, equipment maintenance and cleaning.

13.1.2 Operational change control

a) Changes to information processing facilities and systems must be controlled. Inadequate control of changes is a common cause of system or security failures. A formal procedure, the *System Request*, is in place and well-established in the municipality.

b) All changes, whether to application systems, infrastructure, user profiles, hardware, *etc.* are controlled by this procedure. Formal sign-off is required and monitored at every stage. System Requests are managed by the *System Request Manager* application and the relevant data is stored in a data base for the purpose. Hard-copies are filed sequentially on *SysReq Number* when User Acceptance sign-off has been obtained.

13.1.3 Incident management procedures

1. The *System Incident Report* procedure is in place to record unexpected events that occur during normal operations. The same procedure shall be used to document security incidents. In addition, the following controls must be considered and implemented as appropriate and required:

(a) procedures should be established to cover all potential types of security incident, including:

(i) information system failures and loss of service;

(ii) denial of service;

(iii) errors resulting from incomplete or inaccurate business data;

(iv) breaches of confidentiality.

(b) in addition to normal contingency plans (designed to recover systems or services as quickly as possible) the procedures should also cover:

(i) analysis and identification of the cause of the incident;

(ii) planning and implementation of remedies to prevent recurrence, if necessary;

(iii) collection of audit trails and similar evidence;

(iv) communication with those affected by or involved with recovery from the incident; *and*

(v) reporting the action to the appropriate authority.

(c) audit trails and similar evidence should be collected and secured, as appropriate, for:

(i) internal problem analysis;

(ii) use as evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings, *e.g.* under computer misuse or data protection legislation, *and*

(iii) negotiating for compensation from software and service suppliers.

(d) action to recover from security breaches and to correct system failures must be formally controlled. The procedures must ensure that:

(i) only clearly identified and authorized staff are allowed access to live systems and data;

(ii) all emergency actions taken are documented in detail;

(iii) emergency action is reported to management and reviewed in an orderly manner; *and*

(iv) the integrity of business systems and controls is confirmed with minimal delay.

13.1.3.1 Segregation of duties

1. Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Separating the management or execution of certain duties or areas of responsibility, in order to reduce opportunities for unauthorized modification or misuse of information or services, must be considered and implemented where required.

2. In addition, controls such as monitoring of activities, audit trails and management supervision must be implemented where justified. Security audit must remain independent.

3. Areas of single responsibility where a single person can perpetrate fraud without being detected must be identified. The initiation of an event must be separated from its authorization. The following controls must be considered and implemented where appropriate:

(a) it is important to segregate activities that require collusion in order to defraud, *e.g.* raising a purchase order and verifying that the goods have been received, *and*

(b) where there exists the possibility of collusion, controls must be devised and implemented that increase the number of persons involved, thereby reducing the risk of conspiracy.

13.1.3.2 Separation of development and operational facilities

The separation of development and production facilities is important for proper segregation of the roles involved. Rules for the transfer of software objects (both source and executable) from development to operational status must be defined and documented.

Development and testing activities can cause serious problems, *e.g.* unwanted modification of files or system environment, or system failure. The appropriate level of separation between development, testing and production environments must be determined, implemented, maintained and reviewed regularly.

It is advisable to separate development and testing environments where appropriate, so that a stable environment can be maintain wherein to conduct meaningful testing.

Development staff must not be allowed access to the production environment *unless absolutely unavoidable* (*e.g.* need to effect an urgent repair to corrupted data), and even then only under strict control and supervision. The following controls must therefore be implemented:

(a) development and operational software must run on different computer processors wherever possible;

(b) development and testing activities should be separated as far as possible;

(c) compilers, Editors and other system utilities must not be accessible from operational environments;

(d) different log-in procedures must be used in the development and operational environments, *i.e.* the same username/password combination must not allow access to both environments; *and*

(e) development staff should only have access to operational systems on a strict needs basis and such access must be controlled as for any other user.

13.1.3.3 External facilities management

The use of external contractors to provide and/or manage processing facilities may introduce potential security exposures, such as the possibility of compromise, damage, or loss of data. Such risks must be identified in advance and appropriate controls agreed with the contractor, and incorporated into the Service Level Agreement.

In particular, the following need to be addressed:

(a) obtaining the approval of business application owners;

(b) implications for business continuity plans;

(c) security standards must be agreed, together with the process for measuring compliance;

(d) allocation of specific responsibilities and procedures to effectively monitor all relevant security activities; *and*

(e) responsibilities and procedures for reporting and handling security incidents.

13.1.4 System planning and acceptance

***Objective**: To minimise the risk of system failures.*

Planning and preparation are essential to ensure the availability of adequate capacity and resources. Projections of future capacity requirements should be made regularly to reduce the risk of system overload. The operational requirements of new systems should be established, documented and tested prior to their acceptance and use. Upgrades and enhancements of a capital nature must be planned in line with the municipality's 3-year Budget cycle.

13.1.4.1 Capacity Planning

Capacity demands should be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available. These projections must take into account new business and system requirements and current trends in the municipality's information processing.

The main application servers require particular attention because costs and lead times tend to be significant. Key resources must be monitored regularly and trends analyzed

13.1.4.2 System acceptance

Acceptance criteria for new information systems, upgrades and new versions must be established, and suitable tests conducted prior to acceptance. Such criteria must be clearly defined, agreed, documented and tested. The following controls should be considered:

(a) performance and computer capacity requirements;

(b) error recovery and restart procedures, and contingency plans;

(c) preparation and testing of routine operating procedures to defined standards;

(d) agreed set of security controls in place;

(e) effective manual procedures;

(f) business continuity arrangements;

(g) evidence that installation of the new system will not compromise existing systems, particularly at peak processing times;

(h) evidence that consideration has been given to the effect that the new system will have on the overall security of the organisation; *and*

(i) training in the operation or use of the new system.

13.1.5 Protection against malicious software

Objective: *To protect the integrity of software and information.*

Increasingly, it is necessary to take special precautions to detect and prevent the introduction of malicious software (or "*malware*"). Information processing facilities are vulnerable to the introduction of malicious software such as computer viruses, network worms, Trojan horses and logic bombs. Users must be made aware of the dangers of unauthorized software, particularly where such software is easily downloadable from the internet.

13.1.5.1 Controls against malicious software

Detection and prevention controls to protect against malicious software, and appropriate user awareness procedures must be implemented. Protection against malicious software must be based on security awareness, appropriate system access and change management controls. The following controls should be applied:

(a) enforcement of the provisions of the *Computer Facilities Usage Directive* (CFUD) regarding compliance with software licenses and installation of software;

(b) installation and regular update of anti-virus and anti-spyware detection and repair software;

(c) conducting regular reviews of the software and data content of systems supporting critical business processes. The presence of any unapproved files or unauthorized amendments must be formally investigated;

(d) checking of any files on electronic media of uncertain or unauthorized origin, or files received over untrusted networks, for viruses before use;

(e) checking any electronic mail attachments and downloads for malicious software before use;

(f) management procedures and responsibilities to deal with the virus protection on systems, training in their use, reporting and recovering from virus attacks;

(g) appropriate business continuity plans for recovering from virus attacks, including all necessary data and software backup and recovery arrangements; *and*

(h) procedures to verify all information relating to malicious software, and ensure that warning bulletins are accurate and informative. Managers must ensure that qualified sources, *e.g.* reputable journals, reliable internet sites or anti-virus software vendors, are used to differentiate between hoaxes and real viruses. Staff should be made aware of the problem of hoaxes and what to do on receipt of them.

13.1.6 Housekeeping

***Objective**: To maintain the integrity and availability of information processing and communication services.*

Routine procedures must be in place to carry out the agreed backup strategy, taking backup copies of data and rehearsing timely restoration, logging events and faults and, where appropriate, monitoring the equipment environment.

13.1.6.1 Information backup

Backup copies of essential business information and software must be taken regularly. Adequate backup facilities must be provided to ensure that all business information and software can be recovered following a disaster or media failure. Backup arrangements for individual systems must be regularly

tested to ensure that they meet the requirements of the business continuity plans. The following controls should be considered:

(a) the appropriate level of backup information, together with complete records of the backup copies and documented restoration procedures, must be stored at a remote location, at a sufficient distance to escape any damage from a disaster at the main site. At least three generations or cycles of backup information must be retained;

(b) backup media requires an appropriate level of physical and environmental protection consistent with the standards applied at the main site. The controls applied to media at the main site should be extended to cover the backup site. Note: at present, off-site backup is located at the South End Fire Station;

(c) where practicable, backup media should be regularly checked and tested to ensure they can be relied upon for emergency use when necessary. A policy of planned media replacement after a predetermined number of cycles must be implemented, so that media are replaced well within the relevant planned service life; *and*

(d) restoration procedures should be checked and tested regularly to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

13.1.6.2 Operator logs

Operators must maintain logs of their activities, to include as appropriate:

(a) system starting and finishing times;

(b) system errors and corrective action taken;

(c) confirmation of the correct handling of data files and computer output; *and*

(d) the name of the person logging the entry.

This is in addition to system logs produced by the relevant operating system.

13.1.6.3 Fault logging

Faults must be reported to the relevant authority and corrective action taken. In the case of corporate application systems, faults occurring during End-of-Day processing shall be dealt with in accordance with the System Incident Report procedure. Users must log fault calls with the Service Desk. All faults reported must be dealt with appropriately within acceptable timescales dictated by the business impact of the fault. Management must:

(a) review fault logs to ensure satisfactory resolutions have been reached; *and*

(b) review corrective measures to ensure controls have not been compromised, and that the action taken is fully authorized.

13.1.7 Network management

Objective: *To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.*

13.1.7.1 Network controls

A range of network controls is necessary to achieve and maintain security in computer networks. Network controllers must implement controls to ensure the security of data in networks, and the protection of connected services from unauthorized access. In particular, the following controls must be enforced:

(a) operational responsibility for networks must be separated from computer operations;

(b) responsibilities and procedures for the management of remote equipment, including equipment in user areas, must be established and communicated;

(c) Where necessary, special controls must be established to safeguard the confidentiality and integrity of data passing over public networks, and to protect the connected systems. Special controls may also be required to maintain the availability of the network services and computers connected; *and*

(d) management activities should be closely coordinated both to optimize the service to the business and to ensure that controls are consistently applied across the information processing infrastructure.

13.1.8 Media handling and security

Objective: *To prevent damage to assets and interruptions to business activities, media should be controlled and physically protected.*

Appropriate operating procedures must be in place to protect documents, computer media (tapes, disks, and cassettes), input/output data and system documentation from damage, theft and unauthorized access.

13.1.8.1 Management of removable computer media

Procedures for the management of removable computer media such as tapes, disks, cassettes and printed reports must be established. The following controls should be considered and implemented as appropriate:

(a) if no longer required, the previous contents of any re-usable media that are to be disposed of, must be erased or the media rendered physically incapable of being read;

(b) authority to remove media from the municipality's premises should be controlled and limited. All such removals must be logged in a register kept for the purpose, stating the date, time, type of media, label or description of content, destination and name and Man Number of the person removing the media; *and*

(c) all media must be stored in a safe, secure environment, in accordance with the manufacturer's specifications and the security requirements of the municipality.

13.1.8.2 Disposal of media

Media must be disposed of securely and safely when no longer required or when the number of usage cycles has exceeded the prescribed limit. Appropriate steps must be taken to prevent leakage of sensitive information through careless disposal of media. The following controls must be implemented, as appropriate:

(a) media containing sensitive information must be disposed of securely and safely;

(b) items that might require secure disposal, such as:

(i) paper documents;

(ii) voice or other recordings;

(iii) carbon paper;

(iv) reports;

(v) one-time-use printer ribbons;

(vi) magnetic tapes;

(vii) removable disks, diskettes or cassettes;

(viii) optical storage media (CDs/DVDs) – all forms, including manufacturer software distribution media;

(ix) program listings;

(x) test data; *and*

(xi) system documentation.

Where paper documents are to be disposed of in bulk via external contractors, care must be taken to ensure that there are suitable safeguards in place to prevent compromising of sensitive information. Wherever possible, such media must be securely (cross-cut) shredded.

Disposal of sensitive items should be logged in a register kept for the purpose.

Note that the provisions of the Archives Act may have a bearing on disposal of media, particularly reports and the assistance of the Archives Officer should be sought when formulating the relevant disposal procedures.

13.1.8.3 Information handling procedures

Procedures for the handling and storage of information must be developed and implemented in order to adequately protect such information from unauthorized disclosure or misuse. Procedures should be drawn up for handling information consistent with its classification in documents, computing systems, networks, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities, use of fax machines and any other sensitive items, *e.g.* blank cheques and other pre-printed stationery. The following controls should be implemented as appropriate:

(a) handling and labeling of all media;

(b) access restrictions to identify unauthorized personnel;

(c) maintenance of a formal record of the authorized recipients of data;

(d) ensuring that input data is complete, that processing is properly completed and that output validation is applied;

(e) protection of spooled data awaiting output to a level consistent with its sensitivity;

(f) storage of media in an environment that accords with manufacturers' specifications;

(g) keeping the distribution of data to a minimum;

(h) clear marking of copies of data for the attention of the authorized recipient; *and*

(i) review of distribution lists and lists of authorized recipients at regular intervals.

13.1.8.4 Security of system documentation

System documentation may contain a range of sensitive information, *e.g.* descriptions of applications processes, procedures, data structures and authorization processes. The following controls should be implemented as necessary:

(a) system documentation should be stored securely;

(b) the access list for system documentation should be kept to a minimum and authorized by the application owner; *and*

(c) system documentation held on a network, or supplied via a network, should be appropriately protected.

13.1.9 Exchanges of information and software

Objective: *To prevent loss, modification or misuse of information exchanged between organisations.*

Exchanges of software between the municipality and external organisations must be controlled and compliant with relevant legislation. Exchanges should be done on the basis of formal agreements with procedures and standards implemented to protect information and media in transit. The business and security implications associated with electronic data interchange, electronic commerce and electronic mail must be considered.

13.1.9.1 Information and software exchange agreements

Agreements, preferably formal and reduced to writing in a Service Level Agreement (SLA) are required for the exchange of information (whether electronic or manual) between the municipality and external bodies. The security content of such an agreement should reflect the sensitivity of the information involved. Agreements on security should include:

(a) management responsibilities for controlling and notifying transmission, dispatch and receipt;

(b) procedures for notifying sender, transmission, dispatch and receipt;

(c) minimum technical standards for packaging and transmission;

(d) courier identification standards;

(e) responsibilities and liabilities in the event of loss of data;

(f) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of labels is immediately understood and that the information is appropriately protected;

(g) information and software ownership and responsibilities for data protection, software copyright compliance and similar considerations;

(h) technical standards for recording and reading information and software; *and*

(i) any special controls that may be required to protect sensitive items, such as cryptographic keys.

13.1.9.2 Security of media in transit

Information can be vulnerable to unauthorized access, misuse, tampering or corruption during physical transport, for instance when sending media via the postal service or courier. The following controls should be considered and implemented as necessary when transporting computer media between sites:

(a) Reliable transport or couriers should be used;

(b) Packaging should be sufficient to protect the contents from physical damage likely to arise during transit and in accordance with manufacturers' specifications;

(c) Special controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification. Examples include:

  (i) use of locked containers;

  (ii) delivery by hand;

  (iii) tamper-evident packaging (which reveals attempts to gain access);

  (iv) in exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes; *and*

  (v) use of digital signatures and confidentiality encryption.

13.1.9.3 Electronic commerce security

Electronic commerce can involve the use of electronic data interchange (EDI), electronic mail and on line transactions across public networks such as the internet. Electronic commerce is vulnerable to a number of network threats which may result from fraudulent activity, contract dispute and disclosure or modification of information. Therefore, appropriate controls must be applied to mitigate the risks. Security considerations include the following:

(a) *Authentication*. What level of confidence can be placed on the claimed identities of the parties to a transaction?

(b) *Authorization*. What level of confidence can be placed on the claimed authority to conduct a transaction?

(c) *Contract and tendering processes*. What are the requirements for confidentiality, integrity and proof of dispatch and receipt of key documents and the non-repudiation of contracts?

(d) *Order transactions*. How is the confidentiality and integrity of order, payment and delivery address details, and confirmation of receipt, provided?

(e) *Vetting*. What degree of vetting is appropriate to check payment information supplied by the customer?

(f) *Settlement*. What is the most appropriate form of payment to guard against fraud?

(g) *Ordering*. What protection is required to maintain the confidentiality and integrity of order information, and to avoid the loss or duplication of transactions?

(h) *Liability*. Who carries the risk for any fraudulent transactions?

13.1.9.4 Security of electronic mail

Electronic mail is increasingly being used for routine business communications, replacing traditional forms of communication such as telex, facsimile transmission and letters. Electronic mail differs from

traditional forms of business communication by, for example, its speed, message structure, degree of informality and vulnerability to unauthorized access.

(a) Security risks

Consideration must be given to the need for controls to reduce risks created by electronic mail. These include:

(i) vulnerability of messages to unauthorized access or modification or denial of service;

(ii) vulnerability to error, *e.g.* incorrect addressing or misdirection, and the general reliability and availability of the service;

(iii) impact of a change of communication media on business procedures, *e.g.* the effect of increased speed of dispatch or the effect of sending formal messages from person to person rather than organisation to organisation;

(iv) legal considerations, such as the potential need for proof of origin, dispatch, delivery and acceptance;

(v) implications of publishing externally accessible staff lists; *and*

(vi) controlling remote user access to electronic mail accounts.

(b) Policy on electronic mail

The municipality is in the process of drawing up a clear policy regarding the use of electronic mail. From an Information Security Management perspective, the policy will have to address:

(i) attacks on electronic mail, *e.g.* viruses, interception;

(ii) protection of electronic mail attachments;

(iii) guidelines on when *not* to use electronic mail;

(iv) employee responsibility not to compromise the municipality, *e.g.* sending defamatory electronic mail, use for harassment, unauthorized purchasing;

(v) use of cryptographic techniques to protect the confidentiality and integrity of electronic messages;

(vi) retention of messages which, if stored, could be discovered in case of litigation;

(vii) compliance with the provisions of the Archives Act governing retention and disposal of messages; *and*

(viii) additional controls for vetting messaging which cannot be authenticated.

13.1.9.5 Security of electronic office systems

Policies and guidelines should be prepared and implemented to control the business and security risks associated with electronic office systems. These provide opportunities for faster dissemination and sharing of business information using a combination of: documents, computers, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities and fax machines.

Consideration given to the security and business implications of interconnecting such facilities should include:

(a) vulnerabilities of information in office systems, *e.g.* recording phone calls or conference calls, confidentiality of calls, storage of faxes, opening mail, distribution of mail;

(b) policy and appropriate controls to manage information sharing, *e.g.* the use of corporate bulletin boards;

(c) excluding categories of sensitive business information if the system does not provide an appropriate level of protection;

(d) restricting access to diary information relating to selected individuals;

(e) the suitability, or otherwise, of the system to support business applications, such as communicating orders or authorizations;

(f) categories of staff, contractors or other parties allowed to use the system and the locations from which it may be accessed;

(g) restricting selected facilities to specific categories of user;

(h) identifying the status of users, *e.g.* employees of the municipality or contractors in directories for the benefit of other users;

(i) retention and backup of information held on the system; *and*

(j) fallback requirements and arrangements.

13.1.9.6 Publicly available systems

Care must be taken to protect the integrity of electronically published information to prevent unauthorized modification which could harm the reputation of the municipality. Information on a publicly available system, *e.g.* information on a web server accessible via the internet, may need to comply with laws, rules and regulations in the jurisdiction in which the system is located. There should be a formal authorization process before information is made publicly available.

Software, data and other information requiring a high level of integrity, made available on a publicly available system, should be protected by appropriate mechanisms, *e.g.* digital signatures. Electronic publishing systems, especially those that permit feedback and direct entry of information, should be carefully controlled so that:

(a) information is obtained in compliance with any data protection legislation;

(b) information input to, and processed by, the publishing system will be processed completely and accurately in a timely manner;

(c) sensitive information will be protected during the collection process and when stored; *and*

(d) access to the publishing system does not allow unintended access to networks to which it is connected.

13.1.9.7 Other forms of information exchange

Procedures and controls should be in place to protect the exchange of information through the use of voice, facsimile and video communications facilities. Information could be compromised due to lack of

awareness, policy or procedures on the use of such facilities, *e.g.* being overheard on a mobile phone in a public place, answering machines being overheard, unauthorized access to dial-in voice-mail systems or accidentally sending facsimiles to the wrong person.

Business operations could be disrupted and information could be compromised if communications facilities fail, are overloaded or interrupted. Information could also be compromised if these are accessed by unauthorized users.

A clear policy statement of the procedures staff is expected to follow in using voice, facsimile and video communications should be established. This should include:

(a) reminding staff that they should take appropriate precautions, *e.g.* not to reveal sensitive information by avoiding being overheard or intercepted when making a phone call by:

  (i) people in their immediate vicinity particularly when using mobile phones;

  (ii) wiretapping and other forms of eavesdropping through physical access to the phone handset or the phone line; *and*

  (iii) people at the recipient's end.

(b) reminding staff that they should not have confidential conversations in public places or open offices and meeting places with thin walls;

(c) not leaving messages on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialing;

(d) reminding staff about the problems of using facsimile machines, namely:

  (i) unauthorized access to built-in message stores to retrieve messages;

  (ii) deliberate or accidental programming of machines to send messages to specific members; *and*

  (iii) sending documents and messages to the wrong number either by misdialing or using the wrong stored number.

13.1.10 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Term	Definition
IPsec Concentrator:	A device in which VPN connections are terminated.

Revision History

Date	Revisions

Mamphekgo K.K

The Speaker

22-05-2016

Date