***I 5** / 001*

Munisipaliteit • U-Masipala • Municipality

OVERSTRAND

OVERSTRAND MUNICIPALITY

<u>ICT INFORMATION SECURITY POLICY</u>

Approved by Council

28 March 2012

1. TABLE OF CONTENTS

1.TABLE OF CONTENTS..2

2.BACKGROUND..3

3. POLICY..3

3.1 Management and Staff Responsibilities 3

3.2 Physical Access and Utilisation 4

3.2.1 Computers 4
3.2.2 Network 4
3.2.3 Workstations / Notebooks 5
3.2.4 Modems 5
3.2.5 Off-line media 5
3.2.6 Computer resources 6

3.3 Network Access...6

3.3.1 Access Management..6
3.3.2 Passwords 7
3.3.3 Utilisation 8
3.3.4 Authentication 8
3.3.5 Time restrictions 8
3.3.6 Transaction logs 8

3.4 Backup...9

3.5 E-mail..9

3.6 Internet...9
3.7 Viruses...10

4. GENERAL..10

2. BACKGROUND

The purpose of the Information Security Policy is to:

a) Establish and maintain management and staff accountability for the protection of information resources.

b) Promulgate the policy regarding the security of data and information technology resources.

c) Define the minimum security standards for the protection of information resources.

3. POLICY

Management throughout the Municipality must enforce the following standards:

3.1 Management and Staff Responsibilities

a) Although precautions are taken to safeguard all the systems and data in the Municipality, functional Requirements make it impossible to prohibit all access to it. The owner or user of the data must therefore take the necessary precautions to ensure that the integrity, confidentiality and availability of all data, Systems and equipment are not compromised. To achieve this, the following standards must be adhered to:

b) Each Manager must see to it that all his or her employees take note of this policy.

c) Each Manager is responsible for assuring an adequate level of security for all the data and resources that form part of his or her component or team.

d) An employee may only access and or use the information that he or she is authorised to access/use.

e) All the data and information on the Municipality's systems are the property of the Municipality. The Municipality retains the right to access any information (e-mails, etc.) that is stored on or transported across any of the resources in use and to utilise it for whatever reason it deems necessary.

f) Employees must report any form of misuse of data, systems and equipment that came to their attention to their respective managers or the Department: Information Communication Technology (ICT).

3.2 Physical Access and Utilisation

3.2.1 Computers

a) In order to limit exposure to security risks, access to all computer related hardware and other resources must be controlled.

b) All the domain controllers and all other critical file servers must be kept in a secure (locked) environment and only authorised employees or supervised service representatives must be permitted to enter the room.

c) Console devices (connected to the servers or domain controllers) must be located in a secure location. Other devices such as external hard disks and tape drives must also be located in secure areas.

d) Workstations must be kept in a secure environment. Only authorised employees must be allowed to use them.

e) Printers used to print sensitive documents must be placed in a location not accessible to unauthorised personnel.

f) No sensitive information must be stored on computers located in an insecure environment.

g) Sensitive material/data must not be stored on any system without prior consultation with the Manager: ICT.

3.2.2 Network

a) Network devices such as routers, firewalls, bridges, hubs and servers must be treated as computers and must be located in a secure environment.

b) Cables, although less of an immediate security exposure than other computer devices must be placed in either secure or not readily accessible locations.

c) Employees must not make any unauthorised changes to the physical layout and connection points of the network.

d) Users must not attach any device to the network without prior authorisation from the Manager: ICT.

3.2.3 Workstations / Notebooks

a) The workstations / notebooks must not be generally available to non-employees or unauthorised users.

b) Sensitive output from printers must either be destroyed or placed in a secure location.

c) The visual access to computer screens must be controlled when employees work on sensitive information.

d) No unauthorised changes may be made to the system configuration of workstations / notebooks.

e) Employees are not allowed to insert/remove any devices into/from any official workstation / notebook without prior authorisation from the Manager: ICT (e.g. processors, memory modules, controller cards, etc.).

f) Employees are not allowed to install any program on any computer / workstation without the prior authorisation from the Manager: ICT.

g) No sensitive or classified information must be stored on workstations / notebooks that are not located in a secure environment. Data stored on workstations is not secured through the normal network security measures and the necessary precautions to safeguard such data must be taken.

3.2.4 Modems

a) No modems and or related devices may be attached to and / or used on any official telephone line, computer, and workstation and / or network device without the prior authorisation by the Manager: ICT.

3.2.5 Off-line media

b) Backup media (e.g. tapes, disks or CDs) must be secured against unauthorised use and tampering.

3.2.6 Computer resources

a) Critical systems (servers, domain controllers, network equipment and (workstations) must be provided with an uninterrupted power supply (UPS).

b) The operation and functionality of UPSs must be tested regularly according to prescribed testing procedures.

c) Smoking is not allowed in areas containing computer equipment.

d) Unauthorised access to the computer and network related resources are not allowed.

3.3 Network Access

3.3.1 Access Management

a) Every account must have a Systems Administrator who is responsiblefor account usage, password changes, etc.

b) A record must be maintained showing each user's profile. All modifications to user accounts must be recorded.

c) A new user may be registered on the system through submitting a written application with a list of services, programs and or data to which access is required. This application must be recommended by the applicant's Manager and approved by the Manager: ICT. The network administrator/s may only register the new user after approval has been granted.

d) Temporary employees (for example students and external contractors/auditors) must be registered on the system with an account expiry date. (Maximum of 30 days)

e) Only one login at any time will be allowed per user. Exceptions will only be allowed with prior authorisation by the Manager: ICT.

f) The system must not allow anybody to use the "GUEST" or "ADMINISTRATOR" logins.

g) File and directory permissions or equivalent must be granted to specific users or groups only. This will allow the user to use a file or directory in a particular way (i.e. only for reading). The network administrator must select the appropriate rights to assign to users or groups in each directory or file. Users can only use rights that have been granted in permission assignments.

h) Accounts within a group must perform a similar function and must not possess vastly different privileges. For example, an account used only for data entry should not share the same group as an account used for system management.

i) All groups must be periodically examined by the Manager: ICT to verify each member's function and privileges. Where appropriate, privileges must be adjusted.

j) A user may only perform authorised activities on the system.

3.3.2 Passwords

a) Passwords are required to gain access to all the domain controllers and file servers. No one must be allowed to access any system without a valid password.

b) Passwords must be encrypted by the system.

c) The use of a screensaver password is recommended.

d) Users must not share their passwords with anybody, except an ICT support person.

e) Password attributes:

• Character length	06 characters
• Expiration frequency	30 Days
• Password composition	Letters & numbers
• Invalid login attempts	4 unsuccessful attempts

f) Password history

A password must be unique from passwords used in the past. Users will not be allowed to use any of their previous passwords.

g) Timeout = Logout

Have idle sessions disconnect from network resources after a specified period of inactivity. (10 minutes.)

3.3.3 Utilisation

Users may not leave workstations unattended while still logged onto systems. If a user has been logged onto the Novell server and there has been no activity on that workstation for a period of 10 (ten) minutes, such connection will be electronically terminated.

The facility to use “shared directories” must only be utilised for official purposes. Private information may not be made available on the network through “shared” directories and/or resources such as CD-ROMs and/or files. To prevent unauthorised access to information shared in through the use of shared directories, users must always implement password control over the information.

3.3.4 Authentication

Critical systems (such as Human Resources and Financial) must require further authentication by means of user log-on (ID and password) to the applicable system. The specific system administrator must control the further authentication.

3.3.5 Time restrictions

Time restrictions must be set on the domain controllers and file servers that carry the Human Resources, Financial and other critical information. All the users must be granted access only from 07:00 to 18:00 from Monday to Friday. Exceptions to the above must only be allowed with prior authorisation from the Manager: ICT.

3.3.6 Transaction logs

a) The domain controller and file server error logs must be followed up regularly by the network administrator.

b) All transaction logs must be followed up regularly by the network administrator.

3.4 Backup

a) It is the responsibility of the specific user to ensure that his/her data is backed up regularly. Files containing static information must be protected from unauthorised modification.

b) Critical applications and or data files must be backed up and stored off- site. The location and procedure to access the files must be available to the specific Manager.

c) The Manager: ICT must ensure that the approved corporate backup procedures are followed.

3.5 E-mail

a) The official e-mail system may not be misused for private purposes.

b) Electronic mail messages are not encrypted and the e-mail system must therefore not be used to transmit sensitive and/or classified material.

c) The Municipality retains the right to access and monitor any information sent via the e-mail system.

3.6 Internet

a) The connection of any network to an external network (INTERNET) must be protected by appropriate security measures (e.g. firewall restrictions, etc.).

b) Internet access must be provided on a limited basis for research and communication purposes only. The procedures set out in paragraph 2.3.1 (application and authorisation) must be followed to gain access to this service.

c) No access (other that that officially authorised) to the INTERNET via the Municipality's infrastructure (network, telephones etc.) shall be allowed.

d) Employees are not allowed to download and execute software from the Internet without the appropriate authorisation by the Manager: ICT.

e) Due to bandwidth constraints no live streaming of video and / or audio signals over the Internet shall be allowed.

3.7 Viruses

a) Users must take care not to distribute virus infected documents, programs and or data through the network or e-mail system.

b) All workstations/notebooks, etc. must be regularly scanned for possible virus infections.

c) The official anti virus software must be installed on all computers in use in the Municipality.

d) All instances of virus infections must immediately be reported to the Manager: ICT

e) All discs and memory sticks must be scanned for possible viruses before any programs on it are executed or any data files are read or printed.

f) Any ICT related training needs must be submitted to the Manager: ICT.

4. GENERAL

a) An effective level of awareness and training is essential to a proper information security program and Managers must ensure that all employees are made aware of the official security policy of the Municipality.

b) As some of the technical aspects of the security policy may change due to the systems installed as well as external threats, regular amendments to this document must be considered and issued by the Manager: ICT in consultation with the ICT Steering Committee.

Policy Section	Information Communication Technology
Current Update	28 March 2012
Previous Review	N/A
Approval by Council	25 August 2010