
# Rustenburg Local Municipality

## Cyber Security Policy

## 1. INTRODUCTION

1.1 This Cyber Security Policy is a formal set of rules by which users who are given access to the organisation's Information Technology (IT) Systems and assets must abide.

1.2 The Cyber Security Policy serves several purposes. The main purpose is to inform users, employees, contractors and other authorized users of their obligatory requirements for protecting the ICT assets of the organisation. The Cyber Security Policy describes the ICT assets that we must protect and identifies many of the threats to those assets.

1.3 The Cyber Security Policy also describes the user's responsibilities and privileges. What is considered acceptable use? What are the rules regarding Internet access? The policy answers these questions, describes user limitations and informs users there will be penalties for violation of the policy. This document also contains procedures for responding to incidents that threaten the security of the organisation's computer systems and network.

## 2. PURPOSE OF POLICY

2.1 The main purpose is to inform the municipal users:
employees, contractors and other authorized users of their obligatory requirements for protecting the technology and information assets of the Municipality.
The Cyber Security Policy describes the technology and information assets that users must protect and identifies many of the threats to those assets.

a) To protect the Information Communication Technology Infrastructure, Services and stored data from unauthorised access, use, disclosure, disruption, modification and destruction. It is concerned with ensuring integrity, availability, confidentiality and safety of data and services; and ensures controls are proportionate to risk.

b) Rustenburg Local Municipality recognises the importance of Cyber security. It is committed to ensuring all Municipal activities involving information technology are an appropriately defended against Cyber security threats.

c) The Municipality recognises that successful implementation of Cyber security relies on having a well-informed user community combined with effective management procedures. This overarching policy is supported by a Cyber Security framework which includes supplementary policies and guidelines on specific topics; operational practices; action plans; technology controls and monitoring and assurance activities.

d) The Municipality is committed to the appropriate use of Information Technology

e) and Services to support its operations, data processing, administrative, and service functions. The IT Acceptable Use policy defines acceptable behaviour expected of users of municipal ICT Infrastructure and Services.

## 3. APPLICATION & SCOPE

a) This policy represents the Rustenburg Local Municipality position and takes precedence over other relevant policies which may be developed at a local level.

b) All Users should be aware of this policy, their responsibilities and legal obligations. All Users are required to comply with the policy and are bound by law to observe applicable statutory legislation.

## 4. WHAT ARE WE PROTECTING

4.1 It is the obligation of all users of the organisation's systems to protect the technology and information assets of the Municipality. This information must be protected from unauthorized access, theft and destruction. The technology and information assets of the organisation are made up of the following components:

a. Computer hardware, CPU, disc, Email, web, application servers, PC systems, application software, system software, etc.

b. System Software including: operating systems, database management systems, and backup and restore software, communications protocols, and so forth.

c. Application Software: used by the various departments within the organisation. This includes custom written software applications, and commercial off the shelf software packages.

d. Communications Network hardware and software including: routers, routing tables, hubs, modems, switches and firewalls.

## 5. CLASSIFICATION OF INFORMATION

5.1 User information found in computer system files and databases shall be classified as either confidential or non-confidential. The organisation shall classify the information controlled by them. Senior manager is required to review and approve the classification of the information and determine the appropriate level of security to best protect it.

## 6. CLASSIFICATION OF COMPUTER SYSTEMS

| Security Level | Description | Example |
|---|---|---|
| RED | This system contains confidential information – information that cannot be revealed to personnel outside of the Municipality. Even within the Municipality, access to this information is provided on a "need to know" basis.<br><br>The system provides mission-critical services vital to the operation of the business. Failure of this system may have life threatening consequences and/or an adverse financial impact on the business of the Municipality. | Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information. |
| GREEN | This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network. | User department PCs used to access Server and application(s). Management workstations used by systems and network administrators. |
| WHITE | This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services. | A test system used by system designers and programmers to develop new computer systems. |

| | | |
|---|---|---|
| BLACK | This system is externally accessible. It is isolated from RED or GREEN systems by a firewall. While it performs important services, it does not contain confidential information. | A public Web server with non-sensitive information. |

**7. LOCAL AREA NETWORK (LAN) CLASSIFICATIONS**

7.1 A LAN will be classified by the systems directly connected to it. For example, if a LAN contains just one RED system and all network users will be subject to the same restrictions as RED systems users. A LAN will assume the Security Classification of the highest level systems attached to it.

**8. THREATS TO SECURITY**

8.1 EMPLOYEES

8.1.1 One of the biggest security threats is employees. They may do damage to your systems either through incompetence or on purpose. You must layer your security to compensate for that as well. You mitigate this by doing the following.

a) Only give out appropriate rights to systems. Limit access to only business hours.

b) Don't share accounts to access systems. Never share your login information with co-workers

c) When employees are separated or disciplined, you remove or limit access to systems.

d) Advanced – Keep detailed system logs on all computer activity.

e) Physically secure computer assets, so that only staff with appropriate need can access.

**8.2 AMATEUR HACKERS AND VANDALS.**

a. These people are the most common type of attackers on the internet. The probability of attack is extremely high and there is also likely to be a large number of attacks. There are usually crimes of opportunity. There amateur hackers are scanning the internet and looking for well-known security holes that have not been plugged. Web servers and electronic mail are their favourite targets. Once they find a weakness they

will exploit it to plant viruses, Trojan horses, or use the resources of your system for their own means. If they do not find an obvious weakness they are likely to move on to an easier target.

**8.3 CRIMINAL HACKERS AND SABOTEURS.**

a. The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow and foothold into the network.

**9. USER RESPONSIBILITIES**

**9.1 The following responsibilities apply:**

***9.1.1 Information Technology Manager***

9.1.1.1 The Information Technology Manager has the following responsibilities:

a) carriage of the Municipal Cyber Security Policy and supporting framework;
b) ensuring effectiveness of Cyber security measures through monitoring programs;
c) ensuring effectiveness of disaster recovery plans with a program of testing;
d) authorise complementary operational procedures to support this policy;
e) authorising the isolation or disconnection of any equipment or IT Network Infrastructure from the Municipal network which poses a severe and unacceptable risk; and reporting to appropriate governance bodies including the Risk, and Performance Audit Committee.

***9.1.2 IT Security Specialist***

9.1.2.1 The IT Security Specialist has the following responsibilities:

a) monitor and operate processes required by the cyber security policies and framework;
b) continuous development and improvement of cyber defences;
c) continuous monitoring and review of practices and defences; and

d) conduct education activities to ensure awareness of cyber security threats and defences.

### *9.1.3 Risk and Performance Audit Committee*

9.1.3.1 The Risk Committee and Performance Audit Committee has the following responsibilities:

a) monitor cyber security risks and controls by reviewing the outcomes of cyber risk

b) management processes and monitor emerging risks; and

c) oversee the adequacy of cyber security capability and controls.

### *9.1.4 IT Personnel*

9.1.4.1 IT personnel with responsibility for managing any ICT infrastructure services, IT personnel whom manage any IT infrastructure services have the following responsibilities:

a) Develop, operate and manage the IT infrastructure services according to municipal Cyber a) Security policies;

b) Regularly monitor and assess the related cyber security controls to ensure ongoing effectiveness; and Immediately report all security incidents and breaches to the Cyber Security IT Security specialist or IT Manager.

### *9.1.5 Users of IT infrastructure and Services*

9.1.5.1 Individual Users have responsibility to:

a) Use IT infrastructure and Services according to IT policies at all times;

b) Be aware of the security requirements of the IT infrastructure and Services they use, and take every precaution to safeguard their access to these systems against unauthorised use; and

c) Immediately report any known or suspected security incidents and breaches to IT Division.

## 9.2 ACCEPTABLE USE

9.2.1 User accounts on organisation computer systems are to be used only for business of the organisation and not to be used for personal activities. Unauthorized use of the system may be in violation of the law, constitutes theft and can be punishable by law. Therefore, unauthorized use of the organisation computing system and facilities may constitute grounds for either civil or criminal prosecution.

9.2.2 Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Furthermore, they are prohibited from making unauthorized copies of such confidential information and or distributing it to unauthorised persons outside of the Municipality.

9.2.3 Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to organisation systems for which they do not have authorization.

a. Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from the employees' manager and/or the organisation IT designee.

b. Users shall not download unauthorized software from the Internet onto their PCs or workstations.

c. Users are required to report any weaknesses in the organisation computer security, any incidents of misuse or violation of this policy to their immediate supervisor.

**10. USE OF THE INTERNET**

a) The organisation will provide Internet access to employees and contractors who are connected to the internal network and who has a business need for this access. Employees and contractors must obtain permission from their supervisor and file a request with the Security Administrator.

b) The Internet is a business tool for the Municipality. It is to be used for business-related purposes such as: communicating via electronic mail with suppliers and business partners, obtaining useful business information and relevant technical and business topics.

c) The Internet service may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature for “chain letters” or any other purpose which is illegal or for personal gain.

## 11. USER CLASSIFICATION

a) All users are expected to have knowledge of these security policies and are required to report violations to the Security Administrator. Furthermore, all users must conform to the Acceptable Use Policy defined in this document. The Municipality has established the following user groups and defined the access privileges and responsibilities.

## 12. MONITORING USE OF COMPUTER SYSTEMS

12.1 The organisation has the right and capability to monitor electronic information created and/or communicated by persons using organisation computer systems and networks, including e-mail messages and usage of the Internet. It is not the organisation policy or intent to continuously monitor all computer usage by employees or other users of the organisation computer systems and network. However, users of the systems should be aware that the organisation may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and employees’ electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and organisation policies.

### 12.2 Access Control

a) A fundamental component of our Cyber Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access.

b) The application and database systems can limit the number of applications and databases available to users based on their job requirements.

## 13 USER SYSTEM AND NETWORK ACCESS – NORMAL USER IDENTIFICATION

13.1 All users will be required to have a unique logon ID and password for access to systems. The user's password should be kept confidential and MUST NOT be shared with management & supervisory personnel and/or any other employee whatsoever. All users must comply with the following rules regarding the creation and maintenance of passwords:

a) Password must not be found in any English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard "hacker tools".

b) Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the terminal.

c) Password must be changed every 30 days.

d) User accounts will be locked after 3 failed login attempts.

e) Logon IDs and passwords will be suspended after 30 days of no usage.

13.2 Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting or modifying a password file or any computer systems is prohibited.

13.3 Users will not be allowed to logon as a System Administrator. Users who need this level of access to production systems must request a Special Access account as outlined elsewhere in this document.

13.4 Employee Logon IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the organisation office.

13.5 Supervisors/Managers shall immediately and directly contact the Municipality IT Manager to report change in employee status that requires terminating or modifying employee logon access privileges.

13.6 Employees who forget their password must call the IT department to get a new password assigned to their account. The employee must identify himself/herself by government issued ID to the IT department.

13.7 Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee's password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

**14. SYSTEM ADMINISTRATOR ACCESS**

a) System Administrators, network administrators, and security administrators will have full access to host systems, routers, hubs and firewalls as required to fulfil the duties of their job.

b) All system administrator passwords will be DELETED immediately after any employee who has access to such passwords is terminated, fired, or otherwise leaves the employment of the Municipality.

c) SPECIAL ACCESS Special access accounts are provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts are monitored by the organisation and require the permission of the user's organisation's IT Manager. Monitoring of the special access accounts is done by entering the users into a specific area and periodically generating reports to management. The reports will show who currently has a special access account, for what reason, and when it will expire. Special accounts will expire every day and will not be automatically renewed without written permission.

**15. CONNECTING TO THIRD-PARTY NETWORKS**

a) This policy is established to ensure a secure method of connectivity provided between the Municipality and all third-party organisations and other entities required to electronically exchange information with the organisation.

b) "Third-party" refers to vendors, consultants and business partners doing business with the organisation, and other partners that have a need to exchange information with the

organisation. Third-party network connections are to be used only by the employees of the third-party, only for the business purposes of the organisation. The third-party organisation will ensure that only authorized users will be allowed to access information on the organisation's network. The third-party will not allow Internet traffic or other private network traffic to flow into the network.

c) This policy applies to all third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet the requirements outlined in this document, they will be re-designed as needed.

d) All requests for third-party connections must be made by submitting a written request and be approved by the organisation.

**16. CONNECTING DEVICES TO THE NETWORK**

a) Only authorized devices may be connected to the organisation network(s). Authorized devices include PCs and workstations owned by the organisation that comply with the configuration guidelines of the organisation. Other authorized devices include network infrastructure devices used for network management and monitoring.

b) Users shall not attach to the network: non-organisation computers that are not authorized, owned and/or controlled by the organisation.

NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g. thumb drives, USB's and writable CD's.

**17. REMOTE ACCESS**

a) Only authorized persons may remotely access the organisation network. Remote access is provided to those employees, contractors and business partners of the organisation that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connection can be remote PC to the network or a remote network to Municipality network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID.

## 18. UNAUTHORIZED REMOTE ACCESS

18.1 The attachment of (e.g. hubs) to a user's PC or workstation that is connected to the organisation LAN is not allowed without the written permission of the organisation. Additionally, users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

### *18.2 Penalty for Security Violation*

a) The organisation takes the issue of security seriously. Those people who use the technology and information resources of organisation must be aware that they can be disciplined if they violate this policy. Upon violation of this policy, an employee of organisation may be subject to discipline up to and including discharge. The specific discipline imposed will be determined by a case-by case basis, taking into consideration the nature and severity of the violation of the Cyber Security Policy, prior violations of the policy committed by the individual, state and federal laws and all other relevant information. Discipline which may be taken against an employee shall be administrated in accordance with any appropriate rules or policies and the organisation Policy Manual.

b) In a case where the accused person is not an employee of organisation the matter shall be submitted to the CAE. The CAE may refer the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violator.

### *18.3 Security Incident Handling Procedures*

18.3.1 This section provides some policy guidelines and procedures for handling security incidents. The term "security incident" is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the organisation network. Some examples of security incidents are:

a) Illegal access of an organisation computer system. For example, a hacker logs onto a production server and copies the password file

b) Damage to the organisation computer system or network caused by illegal access. Releasing a virus or worm would be an example.

c) Denial of service attack against the organisation web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.

d) Malicious use of system resources to launch an attack against other computer outside of the organisation network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

18.3.2 Employees, who believe their computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to their manager immediately. The employee shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.

## 19. Policy Review and Maintenance

a) The Policy shall be reviewed and updated after 24 months after council approval, or as a need arises, to ensure that the policy remains aligned with changes to relevant laws, policies, contractual obligations and best practice.