

WEST RAND DISTRICT MUNICIPALITY



ICT SECURITY POLICY

<u>COUNCIL APPROVAL</u>	<u>DATE</u>	<u>SIGNATURE</u>

INDEX

1.	Introduction.....	1
1.1	Definitions	1
1.2	Purpose	2
1.3	Scope.....	2
1.4	Roles and Responsibilities.....	3
2.	Management Approval.....	Error! Bookmark not defined.
2.1	Prior Management Approval	Error! Bookmark not defined.
3.	Information Integrity	4
3.1	Information Reliability	4
3.2	Virus Checking	4
3.3	Push Technology.....	4
3.4	Spoofing Users.....	4
3.5	User Anonymity	4
3.6	Web Page Changes	5
4.	Information Confidentiality	5
4.1	Information Exchange	5
4.2	Posting Materials.....	5
4.3	Message Interception.....	5
4.4	Security Parameters	5
5.	Public Representations	6
5.1	External Representations	6
5.2	Appropriate Behavior	6
5.3	Prohibited Behaviour.....	6
5.4	PERSONAL LAPTOPS	7
6.	passwords and authentication.....	7
7.	Removal of Postings	9
7.1	Disclosing Internal Information	9
7.2	Inadvertent Disclosure.....	9
8.	Intellectual Property Rights	10
	Copyrights	10
9.	Access Control & environmental control.....	10
9.1	User Authentication	10
9.2	physical access.....	10
9.3	Server room Environmental control	11
9.4	Internet Service Providers	11
9.5	Establishing Network Connections	11

9.6	Establish New Business Channels	12
10.	Internet Policy: Personal Use.....	12
10.1	Personal Use.....	12
10.2	Blocking Sites.....	12
11.	Privacy Expectations	13
11.1	No Default Protection.....	13
11.2	Monitoring.....	13
11.3	Logging	13
12.	Reporting Security Problems	13
12.1	Notification Process.....	13
12.2	False Security Reports	14
12.3	Testing Controls.....	14
12.4	Handling Information About Security	14
12.5	Public Representations	14
12.6	Severity.....	14
12.7	Disciplinary Action	15
12.8	Incident Reporting.....	15
13.	Internet Monitoring.....	15
14.	Emails	15
14.1	West Rand District Municipality Email Disclaimer	15
14.2	Email Policy Statements	16
15.	Antivirus Procedures	16
16.	Server Update and Patch Management	17
16.1	NOTIFICATION WINDOW.....	17
16.2	Patch Management Risk	18
16.3	Server Interruption	18
16.4	Standard Troubleshooting Expectations.....	18
16.5	Preferred Patch Schedule	18
17.	database security.....	19
18.	Policy Revision	19

1. INTRODUCTION

Section 59(a) of the Municipal Finance Management Act 56 of 2003 places the onus on each individual within the WRDM to take responsibility for the effective, efficient, economical and transparent use of financial resources within the municipal entity. ICT security policies are risk management strategies that establish acceptable use of company emails, internet, patches/updates, antivirus software, user accounts, computer accounts and physical security shielding an employer from legal liability and protecting network security and productivity. Information and Communication Technology security minimizes the likelihood of these problems and provides a means of managing the remainder of the risk and ensuring Corporate Governance.

The Information and Communication Technology security policy provides an approach to information security that is consistent with the WRDM's accepted business strategy. Information must be protected at all stages of its life-cycle, from the moment it is created or received through processing, communication, transportation and storage, and dissemination to others. Every employee, contractor and consultant at the WRDM has an obligation to appropriately protect information in accordance with the classification and Information and Communication Technology security policies as set out in this policy.

1.1 DEFINITIONS

The definitions are described in the table below

TERM	DEFINITION
User ID or User Account	A name, number, set of initials, etc. which is combined with a password and identifies uniquely a person authorized to use a system.
Password	A secret code used to verify that an individual using a user ID is the actual or authorized owner of the said user Id.
Passphrase	Is a sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.
PC or Computer Equipment	Includes desktop computers, printers, fax machines and any other item that is connected to WRDM's system and/or network.
Junk-Mail or Spam Mail	Mail which is general and not work related, aimed at advertising, selling, etc.
Portable computer / laptop / notebook	Generic expression for all movable computers.
Virus, Trojan Horse, worm or email bomb	A potential disruptive and dangerous program.
A breach of security	Where a stated organizational policy or legal requirement regarding information security has been contravened.
ICT	Stands for Information and Communication Technology.
FTP	File transfer protocol

UUCP	Unix to Unix copy – referred to remote execution of code and file transfer
HTTP / HTTPS	Hypertext transfer protocol / Hypertext transfer protocol secure
Cybercrime or Hacking	The criminal act of illegal access to the computer in order to intercept data, unlawfully acquiring passwords, cyber fraud, cyber extortion and theft of incorporeal property.
Spoofing attack	The act of disguising or impersonation in order to obtain information by pretending to be legit.

1.2 PURPOSE

Use of ICT equipment and infrastructure by employees and councillors of WRDM is permitted and encouraged where such use supports the goals and objectives of the business.

This policy ensures that the WRDM ICT security policy attains the following:

- Provide the high level policy for information security at the WRDM.
- Promote awareness among all councillors, employees, contractors and consultants on the value of information, the risk involved in working with or handling proprietary information and the need to protect information.
- Provide for consequences in the event of non-compliance.
- Define the information owners and users responsible for protecting information.
- Preserve rights and remedies in the event of security breach.

The role of protecting the WRDM's assets is a vital part of the WRDM ICT security policy and requires clearly defined duties and a reporting infrastructure. Information owners grant users access to the business systems, according to their business requirements and other relevant criteria. Information and Communication Technology (ICT) department are the custodians of information and are responsible for daily administration of controls that are specified by the information owners. In response to the risks, this policy describes West Rand District Municipality (WRDM) officials policy regarding ICT security. All suspected and actual security breaches shall be investigated and the necessary disciplinary action shall be taken.

1.3 SCOPE

This document sets out the ICT security policy of West Rand District Municipality, and applies to all employees, councillors, contractors and temporary staff who use the ICT infrastructure with West Rand District Municipality computing or networking resources as well as those who represent themselves as being connected. All ICT users are expected to be familiar with and comply with this policy. This allow all parties involved to protect the information properly.

1.4 ROLES AND RESPONSIBILITIES

1.4.1 ICT Manager

- Oversee regular check on data networks servers.
- Development, implement and enforce ICT policies.
- Conduct regular system reviews.
- Conduct user access reviews
- Ensure information security and backup management.

1.4.2 Network Administrator

- Installing and configuring computer networks and systems.
- Ensure configurations and running of anti-virus system.
- Ensure configuration and running of patch management.
- Ensure configuration and applying group policy.
- Conduct regular system reviews

1.4.3 ICT Technicians

- Installation of PC hardware
- Check and maintain computer hardware and software.
- Install configure and manage software and their functions.
- Develop and maintain local networks.
- Maintain helpdesk logged tickets.

1.4.4 Internal audit

- To assess business processes within ICT
- To assess the efficacy of risk management efforts
- To evaluate internal controls and provide improvement recommendations
- To assess governance risk and compliance within ICT.

1.4.5 Enterprise risk management

- To oversee implementation and quarterly review of risk management progress
- To ensure risk management assessments are performed on a regular basis
- To review the risk register and ensure its adequately updated
- To oversee and monitor the adequacy of risk mitigation controls

1.4.6 ICT Steering committee

- To ensure timeous review of the ICT security policy
- To advise on amendments and implementation of the policy
- To recommend reviewed ICT policies to serve at other committees of council prior to approval

2. INTERNET ACCESS

2.1 INTERNET AND EMAIL ACCESS

Access to the internet and electronic mail is provided by default to all authenticated users.

3. INFORMATION INTEGRITY

3.1 INFORMATION RELIABILITY

All information taken off the internet should be considered unverified until confirmed by credible source. There is no quality control process on the internet, and considerable amounts of the information, is outdated and inaccurate, and in some instances even deliberately misleading.

3.2 VIRUS CHECKING

All files downloaded from non-West Rand District Municipality resources via the internet will be screened with virus detection software.

3.3 PUSH TECHNOLOGY

Automatic updating of software or information on West Rand District Municipality's computers via background "push" internet technology is prohibited unless the involved vendor's system has first been tested and approved by the internet group within ICT, similarly, autorun will be disabled for all executable files in order to limit exposure to malicious programs.

3.4 SPOOFING USERS

Before employees release any internal West Rand District Municipality information, enter into any contracts, or order any products via public networks, the identity of the individuals and organization's contact must be confirmed. Identity confirmation is ideally performed via digital signatures or digital certificates, but in cases where these are not available other means such as letters of credit, third party references, and telephone conversations must be used.

3.5 USER ANONYMITY

Misrepresenting, obscuring, suppressing or replacing a user's identity on the internet or any West Rand District Municipality electronic communications systems is forbidden. The user name, electronic mail address, organization affiliation and related information included with messages or postings must reflect the actual originator of the messages or postings. If users

have a need to employ remailers or other anonymous facilities, they must do so on their own time, with their own information systems, and with their own internet access accounts. Use of anonymous FTP long-ins, anonymous, HTTP (web) browsing, and other access methods established with the expectation that users would be anonymous are not permissible.

3.6 WEB PAGE CHANGES

Employees may not establish new internet web pages dealing with West Rand District Municipality business, or make modifications to existing web pages dealing with West Rand District Municipality business, the WRDM website content management is the responsibility of the communications officer, this includes creating new web pages, uploading documents and any other content on the website.

4. INFORMATION CONFIDENTIALITY

4.1 INFORMATION EXCHANGE

West Rand District Municipality software, documentation and all other types of internal information must not be sold or otherwise transferred to any party for any purposes other than business purposes expressly authorized by management. Exchanges of software and/or data between West Rand District Municipality and any third party may not proceed unless a written agreement has first been signed and approved by management. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

4.2 POSTING MATERIALS

Employees must not post unauthorised West Rand District Municipality material on any publicly accessible platforms.

4.3 MESSAGE INTERCEPTION

Wiretapping and other types of message interception are straightforward and frequently encountered on the internet. Accordingly, West Rand District Municipality secret, proprietary or private information must not be sent over the internet unless it has first been encrypted by approved methods. Unless specifically known to be in the public domain.

4.4 SECURITY PARAMETERS

Credit card numbers, telephone calling card numbers, fixed log-in passwords, and other security parameters that can be used to gain access to goods or services, must not be sent over the internet in readable form. The SSL encryption is an acceptable internet encryption standards.

5. PUBLIC REPRESENTATIONS

5.1 EXTERNAL REPRESENTATIONS

Employees and/or councillors may indicate their affiliation with West Rand District Municipality in mailing lists, chat sessions, and other offerings on the internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an electronic mail address. In either case, whenever employees and/or councillors provide an affiliation, they must also clearly indicate the opinions expressed are their own, and not necessarily those of West Rand District Municipality.

5.2 APPROPRIATE BEHAVIOUR

To avoid libel, defamation of character, and other legal problems, whenever any affiliation with West Rand District Municipality is included with an internet message or posting, “flaming” or similar written attacks are strictly prohibited. Likewise, employees and/or councillors must not make threats against another user or organization over the internet. All internet messages intended to harass, annoy or alarm another person are similarly prohibited.

- Do keep your use of the internet to a minimum;
- Do check that any information you access on the internet is accurate, complete and current;
- Do check the validity of the information found;
- Do respect the legal protections to data and software provided by copyright and licenses;
- Do inform the ICT department immediately of any unusual occurrence.

5.3 PROHIBITED BEHAVIOUR

The following behaviour by an employee or councillor is considered unacceptable:

- Download text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity.
- Download inappropriate content from internet sites.
- Download software from the internet and install it upon the Organization’s computer equipment.
- Use the organisation’s computers to make unauthorized entry into any other computer or network.

- Disrupt or interfere with other computers or network users, services, or equipment. Intentional disruption of the operation of computer systems and networks is a crime under the Computer Misuse and cybercrime Act of 2024.
- Represent yourself as another person (Imposter or impersonator).
- Use Internet access to transmit confidential, political, obscene, threatening or harassing materials.
- Use of organization communications systems to set up persona businesses or send chain letters.
- Forwarding of organization confidential messages to external locations.
- Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, exist or racist, or might be considered as harassment.
- Accessing copyrighted information in a way that violates copyright legislation (Copyright Act of 1976, Section 107).
- Breaking into the organisation's or another organisation's systems or unauthorised use of a password/mailbox.
- Broadcasting unsolicited personal views on social, political, religious or other non-business related matters.
- Transmitting unsolicited commercial or advertising material.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of computer virus or malware into the municipal network.

5.4 PERSONAL LAPTOPS

The use of personal laptops and desktops on the West Rand District Municipality local area network is prohibited, should an extreme need arise to prompt such use of a personal laptop or desktop, the device will need to be cleared by ICT and adhere to all policies e.g.: the machine will need to be formatted, the name to adhere to WRDM standard naming convention, Municipality antivirus must be installed and licensed, Municipality office suite must be installed and licensed, the laptop will need to be joined to the WRDM domain, group policy will be enforced.

6. PASSWORDS AND AUTHENTICATION

6.1 SYSTEM PASSWORD SETTING SUMMARY

The WRDM's systems shall be configured to adhere with the below password security parameters.

SETTING	PARAMETER
Password history size	12 months
Account lockout duration	30 minutes
Invalid logon attempts	3
Password change	30 days

Password length	6 – 8 characters
-----------------	------------------

Users must follow good practice when managing their user IDs, PINs or passwords.
Good end user practices in the selection and use of PIN and passwords are essential.

All users are required to adopt the following practises when setting and managing their PIN and passwords:

- Select PINs and passwords that conform to the WRDM's minimum standard. Don't use a weak password just because it's easier to remember.
- Only reveal your user ID if requested by an authorised person; e.g. system administrators or helpdesk personnel trying to resolve a support issue.
- Keep all PIN and passwords confidential;
- Don't give your password to ANYONE. Don't give it to your manager, your spouse, your friend, the VC, your mother, or any other authority!
- Don't write down your user ID or password: remember it. It's better to have your password reset because you forgot it than to have it stolen
- Change PIN and passwords whenever there is any indication of possible system or PIN or password compromise;
- Change PIN or passwords for privileged accounts, e.g. those that access system utilities, every 30 days;
- Change initial PIN or passwords at the first logon;
- Do not include PIN or passwords in any automated logon process, e.g. stored in a macro or function key.
- You are responsible for ANY activity using your account user ID and password.
- Don't let anyone observe you entering your password. Cover your keyboard when logging in if someone is watching you, or ask them to turn away.
- If your password has been changed or reset and you didn't request it or change it, please let ICT know.
- Password change or reset will be authorised by the use of signed Employee Access form

The following strategies will help users to generate a password that is easy to remember, is hard to guess and complies with the WRDM's policy.

- Use a mixture of upper and lower case and punctuation e.g. Keep Out!
- String several words or parts of words together e.g. it's Cold
- Choose a phrase, perhaps a line from a poem or song and form passwords by concatenating words from the phrase along with digits and/or punctuation. e.g.

Tw1nLit* (from twinkle, twinkle, little star), Yat550ml (from you are the sunshine of my love).

- Invent phrases like car registration plates e.g. one4you!

6.2. AUTHENTICATION

Physical identity of users must be authenticated before providing them with account and password details. Authentication through a username and password will be required before a user can access the West Rand District Municipality local area network either through an ethernet or wireless connection.

7. REMOVAL OF POSTINGS

It is the responsibility of the employee to not send messages to internet discussion groups, electronic bulletin boards, or other public forums, which include an implied or explicit affiliation with West Rand District Municipality. Messages in this category include (a) political statements; (b) religious statements; (c) cursing or other foul language; and (d) statements viewed as harassing others based on race, creed, color, age, sex, physical handicap or sexual orientation.

7.1 DISCLOSING INTERNAL INFORMATION

Employees and/or councilors must not publicly disclose internal West Rand District Municipality information via the internet that may adversely affect West Rand District Municipality's customer relations, or public image unless the approval of the executive director has first been obtained. Such information includes business prospects, performance analyses and the like. Responses to specific customer electronic mail messages are exempted from this policy.

7.2 INADVERTENT DISCLOSURE

Care must be taken to properly structure comments and questions posted to mailing lists, public news groups and related public postings on the internet. Before posting any material, employees and/or councilors should keep in mind that several sparse pieces of information can be pieced together to form a picture revealing confidential information which could then be used against West Rand District Municipality. Although it may seem to be different than the prevailing internet culture of openness, to avoid this mosaic picture problem, employees and councilors should be reserved rather than forthcoming with internal WRDM information.

8. INTELLECTUAL PROPERTY RIGHTS

COPYRIGHTS

West Rand District Municipality strongly supports strict adherence to software vendor's license agreements. When at work, or when West Rand District Municipality computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Likewise, participating (download, copying, distribution) in pirate software and similar activities are prohibited. Employees and/or councilors should assume that all materials on the internet are copyrighted unless specific notices state otherwise.

9. ACCESS CONTROL & ENVIRONMENTAL CONTROL

9.1 USER AUTHENTICATION

All users wishing to establish a real-time connection with West Rand District Municipality internal computers via the internet or telephonically must authenticate themselves on the network protected by a firewall and/ or access control server also known as active directory before gaining access to West Rand District Municipality's internal network.

9.2 PHYSICAL ACCESS

Access to the server room shall be strictly controlled and restricted to authorized ICT personnel, ICT contractors and service providers only. Access to the server room shall be protected by a reinforced wooden covered steel door with a key. A server room access register is to be signed by all parties entering the server room. The key shall be kept at a safe location where it would have to be requested and signed for together with the server room access register by the party requesting access to the server room and an accompanying technician. No eating, drinking or smoking is allowed in the server room.

9.2.1 LOGICAL ACCESS

Logical access to all application system in the WRDM will be acquired by means of an access form provided by ICT, which will be authorized by relevant signatories prior to access being granted, user access and logs reviews will be conducted regularly on application systems to ensure security and integrity of the system

9.2.2 USER ACCESS REVIEWS

All user access to critical systems eg: financial and payroll systems shall be reviewed regularly by ICT to ensure that access and account privileges are in line with job function.

9.3 SERVER ROOM ENVIRONMENTAL CONTROL

Environmental control equipment in the server room enable proactive monitoring of conditions in the server room. Monitored conditions include temperature, humidity, power outages, smoke detectors, uninterrupted power supply and generator.

The WRDM's server room is equipped with Air conditioners, Fire suppression system, Uninterrupted power supply connected to an external generator and smoke detectors.

All environmental control equipment is to be serviced as per schedule below to ensure optimum operation of the equipment and security for information processing equipment like servers, switches and routers:

Air conditioners – annually

Interrupted power supply – annually

Fire suppression system and smoke detectors – annually

Generator - annually

9.4 INTERNET SERVICE PROVIDERS

All internet (except on 3G or LTE) activity must pass through West Rand District Municipality firewalls / network infrastructure so that access controls and related security policies can be applied.

9.5 ESTABLISHING NETWORK CONNECTIONS

Employees and/or councilors may not establish internet or other external network connections that could allow non-West Rand District Municipality users to gain access to West Rand District Municipality systems and information.

9.6 ESTABLISH NEW BUSINESS CHANNELS

Employees and/or councilors are prohibited from using new or existing internet connections to establish new business channels. These channels include electronic data interchange (EDI) arrangements, electronic malls with on-line shopping, on-line database services, etc.

10. INTERNET POLICY: PERSONAL USE

10.1 PERSONAL USE

West Rand District Municipality management encourages employees and/or councilors who have been granted internet access to explore the internet, but if this exploration is for personal purposes, it must be done on personal, not company time. Likewise, games, news groups, radio, music and other non-business activities must be performed in personal, not company time.

Use of West Rand District Municipality computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as no West Rand District Municipality business activity is pre-empted by the personal use.

Employees must not employ the internet or other internal information systems in such a way that the productivity of other employees and/or councilors is eroded; examples include chain letters and broadcast charitable solicitations.

Browsing of distasteful material such as erotica, discriminatory sites that advocate racial supremacy, material that is forbidden and sites that are not in alignment with the ideals or image of Council, are prohibited.

10.2 BLOCKING SITES

West Rand District Municipality routinely prevent users from connecting with certain non-business web sites. Employees and/or councilors using West Rand District Municipality computers who discover they have connected with a web site that contains sexual explicit, racist, violent or other potentially offensive material must immediately disconnect from that site. The ability to connect with a specific web site does not in itself imply that users of West Rand District Municipality systems are permitted to visit that site.

11. PRIVACY EXPECTATIONS

11.1 NO DEFAULT PROTECTION

Employees and/or councilors using West Rand District Municipality information system and/or the internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, employees and/or councilors should not send information over an unsecured internet connection if they consider it to be confidential or private (eg: public wifi, open wifi)

11.2 MONITORING

Continuous monitoring and scanning is carried out on all inbound and outbound internet traffic to ensure secure information exchange.

11.3 LOGGING

West Rand District Municipality routinely maintains logs, security logs, application logs, warning logs and system access logs for regular review.

12. REPORTING SECURITY PROBLEMS

12.1 NOTIFICATION PROCESS

If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, then ICT must be notified immediately.

If any unauthorized use of the information systems has taken place, or is suspected of taking place, ICT must likewise be notified immediately.

Similarly, whenever passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen or disclosed, ICT must be notified immediately.

Because it may indicate a computer virus infection or similar security problem, all unusual systems behaviours, such as missing files, frequent system crashes, misrouted messages and the like must also be immediately reported. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

12.2 FALSE SECURITY REPORTS

The internet has been plagued with hoaxes alleging various security problems. Many of these hoaxes take the form of chain letters, which request that the receiving party send the message to other people.

Employees and/or councilors in receipt of information about the system vulnerabilities should forward it to ICT, who will then determine what if any action is appropriate. Employees and/or councilors must not personally redistribute system vulnerability information.

12.3 TESTING CONTROLS

Employees and/or councilors must not “test the doors” (probe) security mechanisms at either West Rand District Municipality or other internet sites. Likewise, the possession of tools for cracking information security is prohibited.

12.4 HANDLING INFORMATION ABOUT SECURITY

Users must promptly report all information security alerts, warnings, suspected vulnerabilities and the like, to ICT. Users are prohibited from utilizing Council systems to forward such information to other users, whether the other users are internal or external.

12.5 PUBLIC REPRESENTATIONS

No media advertisement, internet home-page, electronic bulletin board posting, electronic mail message, voice mail message, or any other public representation about West Rand District Municipality may be issued unless the Municipal Manager has first approved it.

12.6 SEVERITY

Identified unauthorized access incidents or attempts to West Rand District Municipality systems or information shall be assessed in terms of their severity for the purpose of disciplinary action decisions. Factors determining severity may include (without excluding other considerations):

- The extent of actual or potential financial loss; and/or
- The extent of actual or potential operational impact; and/or
- Whether such access was cognitive or accidental; and/or

- Whether any law, contract or other standard was breached.

12.7 DISCIPLINARY ACTION

Where it is believed that an employee / councilor has failed to comply with this policy, he/she will face relevant disciplinary procedures.

12.8 INCIDENT REPORTING

All breaches of security, inadequate processes, or incidents that may indicate or result in a threat to or weakness in security must be reported immediately to ICT.

13. INTERNET MONITORING

West Rand District Municipality accepts that the use of internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business. While it is understood that acceptable personal use of internet resources is allowed as long as it does not impact productivity, all of the organisation's internet resources are primarily provided for business purposes.

14. EMAILS

The Municipal Manager will be accountable for all the overall email and messaging policy of the West Rand District Municipality. All messages distributed via West Rand District Municipality system are the property of the West Rand District Municipality. All West Rand District Municipality employees and/or councillors shall have no expectations of privacy in anything they store, send or receive on West Rand District Municipality's email system.

Communication to "All WRDM" staff must be sent from the directorate responsible for that communication and with expertise on the particular subject / content within the communication. eg: Health related communication, must be sent from MHS, ICT related communication, must originate from ICT, Finance related communication must originate from Finance etc, in all cases, "Reply to all" is strictly prohibited.

14.1 WEST RAND DISTRICT MUNICIPALITY EMAIL DISCLAIMER

All outgoing email shall be subject to the following disclaimer:

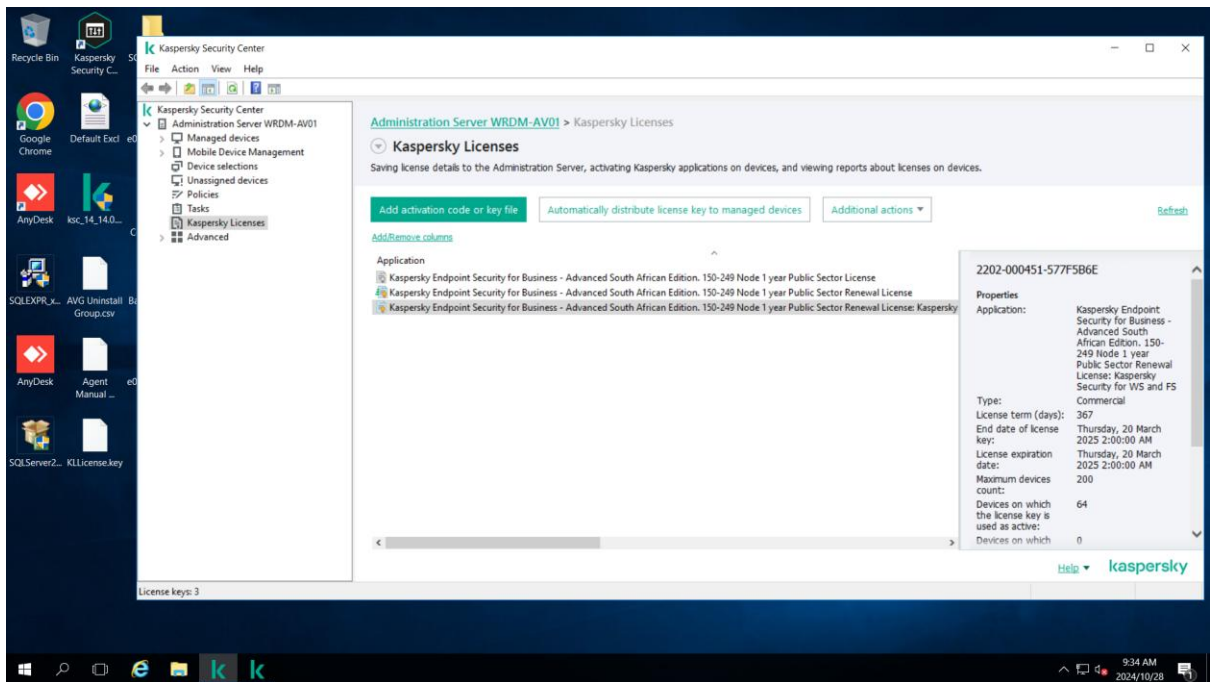
“This message may contain confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this email. Please notify the sender immediately by email if you have received this email by mistake and delete this email from your system. Email transmission cannot be guaranteed to be secured or error free as information could be intercepted, corrupted, lost, destroyed, arrive late, incomplete or contain viruses. The sender therefore does not accept liability for any errors or omissions in the content of this message, which arise as result of email transmission. The West Rand District Municipality does not take responsibility for West Rand District Municipality user’s personal views.”

14.2 EMAIL POLICY STATEMENTS

- Reasonable private use of the West Rand District Municipality email and messaging infrastructure is permitted but this is subject to strict control. Abuse of this privilege may be regarded as misconduct.
- The West Rand District Municipality will audit the West Rand District Municipality infrastructure. The West Rand District Municipality messaging infrastructure audit will be triggered by the following events:
 - West Rand District Municipality suspects that the West Rand District Municipality messaging infrastructure is abused or over utilised by private email;
 - Messaging irregularities are suspected;
 - Messaging virus attacks are suspected;
 - West Rand District Municipality email contents filtering rules are violated;
 - Through using email, West Rand District Municipality users will be deemed to have read, understood and agreed to the policies relating to West Rand District Municipality email systems.

15. ANTIVIRUS PROCEDURES

The Kaspersky server is based at West Rand District Municipality where the admin console is run. The entire computer clients include West Rand District Municipality, West Rand Development Agency, 107 EOC and all the fire stations, which Kaspersky obtains connection to this server.



The update is set as per below on the server and are performed manually using the antivirus server:

All computers are installed with Kaspersky antivirus software before dispatched to employees. This includes West Rand District Municipality, West Rand Development Agency and all satellite offices. The update is done manually using the proxy settings as per below:

The remote setting to get the connection to the Kaspersky server (Kaspersky admin console) settings is set as per below

16. SERVER UPDATE AND PATCH MANAGEMENT

16.1 NOTIFICATION WINDOW

Users will receive notice one week in advance before server upgrades, performance patches, application updates and hotfixes are downloaded and installed on the systems listed above.

The advance notice is provided so the ICT department may inform all users of the scheduled downtime and maintenance period. The ICT department will be the single point of contact for notifying the West Rand District Municipality users that server patch maintenance will occur.

16.2 PATCH MANAGEMENT RISK

It is a best business practice to download and install server operating system application performance patches and security updates. The ICT department recommends downloading and installing patches as they are made available. However, only the user can properly balance its business needs and objectives with the benefit of rapid patch management and the resultant risk that new patches and updates may introduce incompatibilities or errors. Patching servers against known issues upon patch release ensures organizations address known issues and close application and operating system vulnerabilities as they are discovered as a measure to combat evolving cybercrime.

16.3 SERVER INTERRUPTION

Routine patch management cycles typically require that servers be rebooted. Occasionally multiple restarts are required. In non-virtualized and most physical server environments, while patches are installed and servers are restarted, critical services, application data, email and other files, services and programs may prove unavailable.

16.4 STANDARD TROUBLESHOOTING EXPECTATIONS

The process of downloading and installing updates and patches requires sometimes making significant changes to the underlying operating system and/or critical business applications. Patch deployment can break a previously properly functioning server. Following the installation of new patches and any necessary restarts, an ICT Administrator will perform tests to ensure server functionality returns to proper operation. If trouble is encountered, the ICT Administrator may require physical access to the server room.

16.5 PREFERRED PATCH SCHEDULE

The patches and updates are scheduled to auto download and install at 12:00 PM every Wednesday, from update server WRDM-SCCM02

Windows Components/Windows Update			hide
Policy	Setting	Comment	
Configure Automatic Updates	Enabled		
Configure automatic updating:			3 - Auto download and notify for install
The following settings are only required and applicable if 4 is selected.			
Install during automatic maintenance			Disabled
Scheduled install day:			4 - Every Wednesday
Scheduled install time:			12:00
Policy	Setting	Comment	
Specify intranet Microsoft update service location	Enabled		
Set the intranet update service for detecting updates:			http://wrdm-sccm02.wrdm.gov.za:8530
Set the intranet statistics server:			http://wrdm-sccm02.wrdm.gov.za:8530
(example: http://IntranetUpd01)			
Policy	Setting	Comment	
Turn on recommended updates via Automatic Updates	Enabled		

17. DATABASE SECURITY

Database security is essential on systems that utilize database to store and process data, best practice method outlined below must be followed when implementing or maintaining database system where applicable.

- 17.1. Production databases are configured to capture, record and alert on key data and database activities including, but not limited to view access to confidential or personal information, data manipulation activities (e.g. insert, delete & change), security activities (e.g. creation/deletion of users), high-risk database activities (e.g. turn audit on/off), and suspicious or abnormal activities.
- 17.2. Production databases requiring password authentication must utilize authentication lookup against approved WRDM authentication services (i.e. Active Directory, Radius) with an exception of systems that do not allow for directory services integration.
- 17.3. Database vulnerability assessments must be conducted to identify, analyse and manage security risks related to critical and high risk database vulnerabilities.
- 17.4. Changes to database system must follow the organization's Change Management processes, including changes being tested and authorized before implementation in production systems

18. POLICY REVISION

The policy will be revised biennial.