ICT SECURITY POLICY

UMZIMVUBU
LOCAL MUNICIPALITY

TABLE OF CONTENTS

PURPOSE

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

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

1.3 Define the minimum-security standards for the protection of information resources.

1. ROLES AND RESPONSIBILITIES

Although precautions are taken to safeguard all the systems and data, 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 should be adhered to:

2.1 Each Departmental Head must see to it that all his or her employees take note of the Policy regarding the implementation and maintenance of data and system security.

2.2 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.

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

2.4 No information/images/data that may be offensive to any person, group or organisation may be stored on any of the official computer systems or transported across any official network or system.

2.5 As official messages sent via the e-mail system can have a major impact on the image of the Office, employees should see to it that such messages contain only authorised information and that it is in the format prescribed by the Correspondence and Publication Corporate Standards of the Office.

2.6 All the data and information on the Office's systems is the property of the Office of the municipality. The Office retains the right to access any information (e-mail etc.) that is stored on or transported across any of the resources in use and to utilise it for

whatever reason it deems necessary.

2.7 Employees must report any form of misuse of data, systems and equipment that comes to their attention to their respective managers or the Data Security Manager: IT.

3. FIREWALL

3.1 ICT will implement a firewall between the Internet and private internal network in order to create a secure operating environment for the Municipality's computer and network resources.

3.2 The firewall will (at minimum) perform the following security services:

- Access control between the trusted internal network and untrusted external networks.
- Block unwanted traffic as determined by the firewall rule.
- Hide vulnerable internal systems from the Internet.
- Hide information, such as system names, network topologies, and internal user IDs, from the Internet.
- Log traffic to and from the internal network.
- Provide virtual private network (VPN) connectivity.

3.3 Access to the Firewall is governed by password authentication so only the Firewall Administrator and the Network Administrator are permitted access to the Firewall.

3.4 Any changes to the device must be performed by either of the Firewall Administrator or the Network Administrator roles no other member of staff is authorised or capable of accessing the Firewall.

3.5 The Firewall physical device is housed in a secure area of the Municipality premises. This location is restricted through the use of secure key and may only be accessed by a restricted number of authorised technical team members.

3.6 The Firewall will provide access to the network only through a restricted number of ports. Any port that is not used to provide a connection will be disabled to prevent unauthorised access and ensure the network security is maintained.

4. COMPUTERS

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

4.2 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 should be permitted to enter the room.

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

4.4 Printers used to print sensitive documents should be placed in a location not accessible to unauthorised personnel. No sensitive information should be stored on computers located in an insecure environment.

5. NETWORK

5.1 Network devices such as routers, firewall, bridges, hubs and servers should be treated as computers and should be located in a secure environment.

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

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

6. WORKSTATIONS / NOTEBOOKS

6.1 The workstations / notebooks should not be generally available to non-employees
or unauthorised users.

6.2 Sensitive output from printers should either be destroyed or placed in a secure location. If employees work on sensitive information the visual access to the screens should be controlled.

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

6.4 Employees are not allowed to insert/remove any devices into/from any official workstation / notebook without prior authorisation (E.g. Processors, memory modules, controller cards etc.) Employees are not allowed to install any program on any official computer / workstation without the prior authorization. No sensitive or

classified information should be stored on workstations / notebooks that are not located in a secure environment.

6.5 Please note that data stored on workstations is not secured through the normal network security measures and the necessary precautions to safeguard such data should be taken. Should the current local workstation / notebook security be of any concern, additional measures can be instituted. The Centre Manager: IT can be contacted in this regard.

7. MODEMS

7.1 No modems and or related devices may be attached to and or used on any official

telephone line, computer, workstation and or network device without prior authorization.

8. OFF-LINE MEDIA

8.1 Backup media (e.g. tapes, disks or CD?s) must be secured against unauthorised use

and tampering.

9. COMPUTER RESOURCES

9.1 Critical systems (servers, domain controllers, network equipment and workstations)

should be provided with an uninterrupted power supply (UPS).

9.2 The operation and functionality of UPS?s must be tested regularly according to prescribed testing procedures.

9.3 Smoking is not allowed in areas containing computer equipment. Unauthorised access to the computer and network related resources are not allowed.

10. ACCESS MANAGEMENT

10.1 Every account must have an owner. (Someone who is responsible for account usage, password changes etc.)

10.2 A record should be maintained showing each user's profile. All modifications to user accounts should be recorded.

10.3 A new user may be registered on the system by submitting a written application with a list of services, programs and or data to which access is required. This application

has to be recommended by the applicant's supervisor and approved by the relevant Manager. After approval has been granted, the network administrator/s will register the new user.

10.4 A user account shall be created stating with employee Surname then Name order.

105. The ICT team shall receive correspondence from HR section that authorize creation/Activation of a new user account, amendments and for termination of any user account from the system. In case of changes of user employment position HR section shall inform ICT section for reallocation of user account.

11. PASSWORDS

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

11.2 Users will be forced to change passwords on the domains and servers every 31 days.

11.3 Passwords will be encrypted by the system.

11.4 The minimum password length is set to eight characters and must contain alpha as well numerical characters plus special character.

11.5 Care should be taken that passwords are not easily guessed (E.g. names, month etc.)

11.6 The use of a screensaver password is recommended.

11.7 Users will be allowed three login attempts before the account will be locked. This lock will remain in effect until opened by the Network administrator.

11.8 The last 10 previously used passwords are not allowed.

11.9 Passwords that expire must be changed immediately.

12. AUTHENTICATION

12.1 Critical systems (Payday and Munsoft) may require further authentication by means of user log-on (USER-ID and password) to the applicable system. The specific system administrator must control this.

13. TIME RESTRICTIONS

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

14. TRANSACTION LOGS

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

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

15. BACKUP

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

15.2 Critical applications and or data files should be backed up and stored off-site. The location and procedure to access the files must be available to the specific manager. 15.3 The Data Security Manager must ensure that the approved corporate backup procedures are followed.

16. EMAIL

16.1 The official e-mail system may not be misused for private purposes. Electronic mail messages are not encrypted and the e-mail

16.2 System can therefore not be used to transmit sensitive and/or classified material.

16.3 The Office retains the right to access and monitor any information sent via the e-mail system. No private information/images/data that may be offensive to any person, group or organization may be sent to any destination via the official e-mail system.

16.4 As messages sent via the official e-mail system can have a major impact on the image of the Office, employees must see to it that such messages contain only authorized information and that it is in the format prescribed by the Correspondence and Publication Corporate Standards of the Office.

17. INTERNET

17.1 The connection of any Office network to an external network (INTERNET) must be protected by appropriate security measures (e.g. firewall restrictions etc.). Internet access is provided on a limited basis for research and communication purposes only. The procedures set out in paragraph (application and authorization) must be followed to gain access to this service. No material that may be deemed offensive may be downloaded through the official systems and networks.

17.2 Due to bandwidth constraints no live streaming of video and or audio signals over the Internet will be allowed.

ICT Security Policy

18. ANTI-VIRUSES

18.1 Umzimvubu local municipality will use a single anti-virus product for anti- virus protection and that product is ESET NOD32 Antivirus. The anti-virus product is operated in real time on all servers and client computers. The Antivirus is configured for real time protection.

18.2 The anti-virus library definitions shall be updated at least once per day.

18.3 Anti-virus scans shall be done a minimum of once per week on all user controlled workstations and servers.

19. VIRUSES

19.1 Users should take care not to distribute virus infected documents, programs and or data through the network or e-mail system. All workstations/notebooks etc. should be regularly scanned for possible virus infections.

19.2 The official antivirus software should be installed on all the computers in use in the Municipalities.

19.3 All instances of virus infections should be reported. All diskettes should be scanned for possible viruses before any programs on it are executed or any data files are read or printed. Users will be informed of antivirus software updates via e-mail.

20. SECURITY MEASURES AND LIMITATION ON ACCESS

20.1 Each user must comply with all of the Municipality's access procedures, including the use of assigned user ID's and use of the licensed software made available to the employee by the Municipality. User ID's may not be shared with other persons, a user may not use e- mail accounts assigned to other individuals to send or retrieve messages.

20.2 It remains the responsibility of each user to safeguard their passwords to prevent unauthorized access. Every user must ensure that system access is signed off when they leave their desk

21. SECURITY BREACH

21.1 An information security incident information technology (IT) security incident is an event involving an IT resource at ULM that has the potential of having an adverse effect on the confidentiality, integrity, or availability of that resource or connected resources.

21.2 Resources include individual computers, servers, storage devices and media, and mobile devices, as well as the information, messages, files, and/or data stored on them. Prompt detection and appropriate handling of these security incidents is necessary to protect Umzimvumbu's information technology assets. The details of handling such an incident are detailed in the Security Breach Procedure Attached herein as ***"Annexure A"***

ICT Security Policy

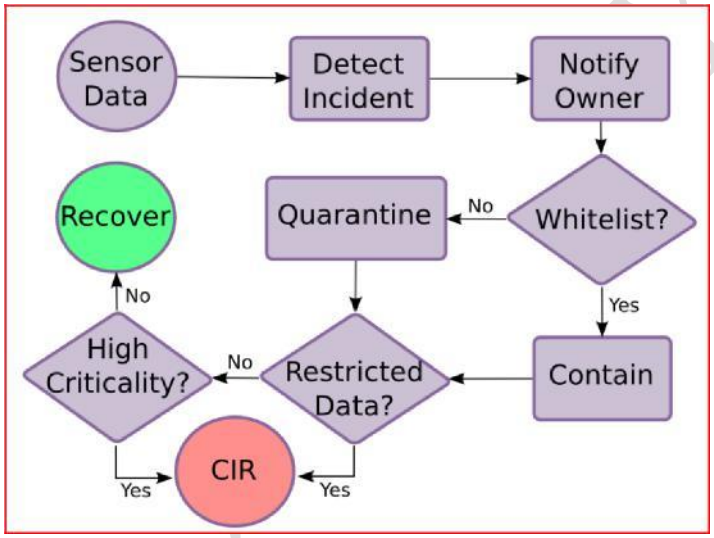
ANNEXURE A: SECURITY BREACH PROCEDURE

A1 PROCEDURE PURPOSE

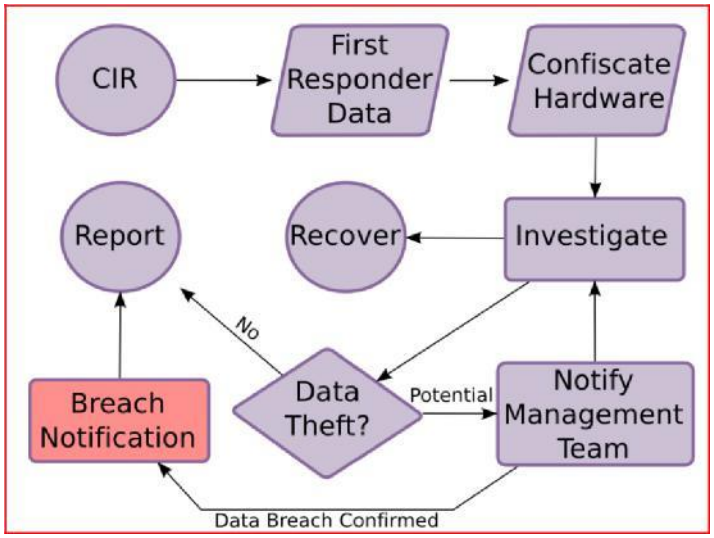
The purpose of this procedure is to provide general guidance to ULM staff who manage IT resources to enable quick and efficient recovery from security incidents; respond in a systematic manner to incidents and carry out all necessary steps to correctly handle an incident; prevent or minimize disruption of critical computing services; and minimize loss or theft of sensitive or mission critical information.

A2 OVERVIEW OF WORKFLOW

The flow-charts below are a visual depiction of the procedure described below in its most typical occurrence. This first chart covers the general incident response procedure followed by the incident handler:



If Restricted Data is present on the compromised system i.e. Payday and Munsoft data the Critical Incident Response (CIR) is followed. The CIR is summarized below.



A3. IDENTIFICATION

The identification phase of incident response has as its goal the discovery of potential security incidents and the assembly of an incident response team that can effectively contain and mitigate the incident:

- **Identify** a potential incident. The incident handler may do so through monitoring of security sensors. System owners or system administrators may do so by observing suspicious system behavior.
- **Notify**: Members of the ULM that it is suspected an IT system has been accessed without authorization. Once the IT Manager is aware of a potential incident, s/he will alert local system administrators.
- **Quarantine**: The incident IT Manager will quarantine compromised hosts at the time of notification unless they are on the Quarantine Whitelist. If they are on the Quarantine Whitelist, the IT Manager will promptly reach out to the system administrator or system owner to create a plan to contain the incident. Note that the IT Manager may notify on suspicious behavior when s/he is not confident of a compromise; in these cases they do not quarantine the host immediately, but wait 24-48 hours and quarantine only if the registered contact is unresponsive.

A4. CONTAINMENT

The containment phase represents the beginning of the CIR workflow and has the following goals:

- If the host cannot immediately be removed from the network, the IT Manager will initiate a full-content network dump to monitor the attacker's activities and to determine whether interesting data is leaking during the investigation.

- Eliminate attacker access: Whenever possible, this is done via the IT Manager performing network quarantine at the time of detection AND by the system administrator unplugging the network cable. In rare cases, the IT Manager may request that network operations staff implement a port-block to eliminate attacker access. In cases where the impact of system downtime is very high, the IT Manager will work with system administrators to determine the level of attacker privilege and eliminate their access safely.

- The IT Manager will collect data from system administrators in order to quickly assess the scope of the incident, including:

i. Preliminary list of compromised systems

ii. Preliminary list of storage media that may contain evidence

iii. Preliminary attack timeline based on initially available evidence

A5. PRESERVE FORENSIC DATA

- System administrators will capture **first responder data** if the system is turned on. The IT Manager will provide instructions for capturing this data to the individual performing that task.

I. The IT Manager or designee will capture disk images for all media that are suspected of containing evidence, including external hard drives and flash drives. The system owner should expect to have it returned within 5 business days.

II. The IT Manager will dump network flow data and other sensor data for the system.

III. The IT Manager will create an analysis plan to guide the next phase of the investigation.

This is the most time-sensitive and also the most contextually dependent phase of the investigation. The actions that need to be taken will depend on the uptime

requirements of the compromised system, the suspected level of attacker privilege, the nature and quantity of data at risk, and the suspected profile of the attacker. The most important goals of this phase are to eliminate attacker access to the system(s) as quickly as possible and to preserve evidence for later analysis.

A6. ANALYSIS

The analysis phase is where in-depth investigation of the available network-based and host-based evidence occurs. The primary goal of analysis is to establish whether there is reasonable belief that the attacker(s) successfully accessed Restricted Data on the compromised system. Secondary goals are to generate an attack timeline and ascertain the attackers' actions. All analysis steps are primarily driven by the IT Manager, who coordinates communications between other stakeholders, including system owners, system administrators, and relevant compliance officers. Questions which are relevant to making a determination about whether data was accessed without authorization include:

- Suspicious Network Traffic: Is there any suspicious or unaccounted for network traffic that may indicate data exfiltration occurred?
- Attacker Access to Data: Did attackers have privileges to access the data or was the data encrypted in a way that would have prevented reading?
- Evidence that Data was accessed: Are file access audit logs available or are file system machines intact that show whether the files have been accessed post-compromise?
- Length of Compromise: How long was the host compromised and online?
- Method of Attack: Was a human involved in executing the attack or was an automated "drive-by" attack suite employed? Did the tools found have capabilities useful in finding or exfiltration data?
- Attacker Profile: Is there any indication that the attackers were data-thieves or motivated by different goals?

A7. RECOVERY

- The primary goal of the recovery phase is to restore the compromised host to its normal business function in a safe manner.
- The system administrators will remediate the immediate compromise and restore the host to normal function. This is most often performed by reinstalling the compromised host; although if the investigation confirms that the attacker did not have root/administrator access other remediation plans may be effective.
- The system administrators will make short-term system, application, and business process changes to prevent further compromise and reduce operating risk.

A8. REPORTING

The final report serves two main purposes:

a. That a recommendation is made to the Municipal Manager and relevant Corporate Services Director as to whether the IT Manager and the responsible officials feel there is a reasonable belief that Restricted Data was disclosed impermissibly without authorization and the degree of probability that the security or privacy of the ULM has been compromised. The report must be made in sufficient time to allow notification, if appropriate, within 5 days of discovering the Breach.

b. Second, a series of mid-term and long-term recommendations are made to the owners of the compromised system, including responsible management, suggesting improvements in technology or business process that could reduce operating risk in the future.

The IT Manager will draft the final report after the investigation is complete. Preliminary reports should be avoided whenever possible since working conclusions can change substantially through the course of an investigation.

After the draft report is completed, signoff on the content of the report should be obtained from the MM. Technical personnel can offer comments now as well, but typically technical issues should be resolved by this stage. Again, a list of issues will be raised which should be resolved or acknowledged/deferred.

22. SECURITY AWANESS AND TRAINING

22.1 Security awareness emails shall be sent to all users to ensure user do not authenticate or register from any unknown websites.

22.2 ICT team shall conduct training of any new security procedure so to ensure users understand all security procedure or protocols.

23. CYBER SECURITY

Cyber security policy governs the usage of ICT resources from an end user's perspective. The cyber security policy is applicable to all the municipal employees and councilors.

23.1 Cyber security Policy elements

23.1.1 Confidential data

Confidential data is secret and valuable. Common examples are:

- Information concerning municipal employees, councilors and vendors/ service providers.
- Unpublished financial information and contractual data
- All employees are obliged to protect this data. In this policy,

23.1.2. Instructions on How to Avoid Security Breaches.

Protect Umzimvubu municipality devices.
When employees use personal digital devices to access Trust emails or accounts, they introduce security risk to municipal data/Information. Employees are required to keep municipal devices (computers and cellphones) secure by ensuring that all devices password protected. ● Ensure antivirus software is kept up to date. ● Ensure they do not leave their devices exposed or unattended. ● Log into municipal accounts and

systems through secure and private networks only. municipal employees to avoid accessing email accounts from other people's devices or lending their own devices to others. When new staff (Councilors and employees) receive Trust-issued equipment they should review the Trust's Acceptable Use of ICT security Policy, as it will contain key information relating to the safe and secure use of this equipment.

23.1.3. Keep emails safe.

Emails often host phishing attacks, scams or malicious software (e.g., trojans and worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g., "watch this video, it's amazing.") ● Be suspicious of clickbait titles (e.g., offering prizes, advice.) ● Check email and names of people they received a message from to ensure they are legitimate. ● Look for inconsistencies or give-aways (e.g., grammar mistakes, capital letters, excessive number of exclamation marks.)
- When an employee isn't sure that an email, they received is safe, they should contact ICT Team.

COMMENCEMENT OF THE POLICY

- The policy will come into effect on the date signed by ICT Governance Champion

INTERPRETATION OF THE POLICY

- All words contained in this policy shall have the ordinary meaning attached thereto, unless the definition or context indicates otherwise
- Any dispute on interpretation of this policy shall be declared in writing by any party concerned.
- The Municipal Manager shall give a final interpretation of this policy in case of written dispute.
- If the party concerned is not satisfied with the interpretation, a dispute may then be pursued with the South African Local Government Bargaining Council.

PERMANENT/TEMPORAL WAIVER OR SUSPENSION OF THE POLICY

- This policy may be partly or wholly waived or suspended by the ICT Governance Champion on temporary or permanent basis however the Municipal Manager/Council may under circumstances of emergency temporarily waive this policy subject to reporting of such waiver or suspension to Council

24. Reporting and Contact Information Questions or reports relating to this policy

- SysAid Help Desk reporting portal link: http://zaulmsq02:8080/EndUserPortal.jsp
- Email municipal ICT Team
- Telephone or callphone call for assistance

COMPLIANCE AND ENFORCEMENT

- Senior management is required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.
- Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

Any conduct that interferes with the normal and proper operation of the municipality's IT systems, which adversely affects the ability of other users to use those IT systems, or which is harmful or offensive to other users, shall constitute violation of approved IT policies.

 The municipality management reserves the right to revoke the privileges of any user at any time.

AMENDMENT AND/OR ABOLITION OF THIS POLICY

 This policy may be amended or repealed by ICT Governance Champion /Council as it may deem necessary.

DOCUMENT OWNER AND APPROVAL

The Municipality is the owner of this document. The Executive Management of the Municipality is responsible for ensuring that this policy document is reviewed regularly to ensure that it remains relevant to the organisation.

This document was approved by the Executive Management and is issued on a version controlled basis under the signature of the ICT Governance Champion.

Every page of this document must also be initialled by the Governance Champion.

_____ _____

Signature: **Date:**

_____

Position