Molemole Municipality

IT-05-03
Information and Network Security Policy

Document Name:	**Information and Network Security Policy**
Policy Number:	IT-05-03
Version:	001

Document Information

Policy	Information and Network Security
Version	001
Policy Code	IT-05-03
File Name	MOL-IT-05-03-001 Information and Network Security.doc
Manual	IT Policies and Procedures Manual
Section	05 Security
Applicability	This is applicable to all users and person maintaining information, communications and systems.
Situations	This policy applies to all situations in which information is required to be protected in terms of its storage, access and transmission.
Changes	V001 : Initial Version
Policy Owner	IT Manager
Policy Enforcer	IT Manager

Contents

1. Overview

1.1. General Purpose

Information and information resources are valuable assets of Molemole Municipality and they form an important part of the operation and management of the municipality.

This and other policies have been put into place in order to protect these and to promote integrity, security, reliability and privacy of the entire information infrastructure including the information and data it contains, the network, the computers and other access devices.

1.2. Background to this Policy

Information security is fundamental to all activities and capabilities within the scope of the operations of IT services. This applies within the scope of the municipality as much as it does to other government institutions and to private business.

This is a core ICT policy, and it contains a number of situations that require security to be controlled within the scope of information access and the utilisation of networks.

The benefits of implementing this policy will include improved control of the information critical to the success of the municipality as well as compliance with national and international standards and best practices.

1.3. Creation of this Policy

This policy is informed by the following:

- General risks to the municipality arising from threats to a secure IT infrastructure – in terms of risks to confidentiality, integrity of available of the information and systems.
- Legislative and associated requirements.
- General principles associated with good practice in information security.

2. Scope

2.1. This policy is concerned with the broader aspects of information and network security.

2.2. The scope includes the following:

- Responsibilities for Information Security
- Organisational Security
- Identification and Control of Information Assets
- Personnel Authorisation
- Document Classification and Management
- Communication and Operations Management
- Access Control
- Computer Security
- Cryptographic Controls
- Physical Security
- Security Incident Management

2.3. This policy is supported by more specific policies that deal with particular situations including:

- IT-01-03 Register of IT Assets
- IT-02-01 Acceptable Use Policy
- IT-03-01 Email Use Policy
- IT-03-02 Internet Use Policy
- IT-03-03 Email Disclaimer
- IT-03-04 Website Disclaimer
- IT-04-01 Data, Information and Records Policy
- IT-04-02 Information Sensitivity Policy
- IT-05-01 Physical Access Security Policy
- IT-05-02 UserID and Password Policy

- IT-05-51 Network Access Acceptance

2.4. This policy must be communicated to all personnel who are responsible for managing IT security implementation within the municipality. It is imperative that the IT security personnel employ this policy to the full as part of their responsibilities.

2.5. Where necessary the IT security personnel must communicate the relevant elements of this policy to the entire user base of the municipality.

3. Purpose of this Policy

3.1. This policy provides the principles and practices to protect the information assets of the municipality. The elements of this policy play a part in protection from threats, business continuity, minimisation of business impact, as well as maximisation of return on investments and business opportunities.

3.2. The purpose of this policy is to provide a set of controls suitable for the achievement of the characteristics of information security as identified in the definition below.

4. Applicability

4.1. This Policy is applicable to all situations involving the implementation and enforcement of information security controls to meet the purpose of this policy. These situations are identified in the scope as outlined above.

5. Definitions for this Policy

5.1. This policy document also defines the following specific items:

- **Information Security** : this is defined as the preservation of confidentiality, integrity and availability of information.

- **Confidentiality** : ensuring that information is accessible only to those authorised to have access.

- **Integrity** : safeguarding the accuracy and completeness of information and processing methods.

- **Availability**: ensuring that authorised users have access to information and associated assets when required.

6. References for this Policy

6.1. This policy is informed by the following reference documents, as well as by other best practices which extend the practical implementation of these generic best practices.

COBIT V4.0

6.2. COBIT provides many control objectives which support the development of information security policies. These include the following:

- DS5 : Ensure System Security.
- P09: Assess and Manage Risks (concerning security risks).
- AI1/AI2 : Security within Applications.
- DS12 : Manage the Physical Environment : including physical security measures.

ISO 177999: IT Code of Practice for Information Security Management

6.3. This is a core reference for the creation of a customised policy for information security. The ISO 17799 is designed to support the extraction of suggested controls as required.

6.4. Some institutions have adopted the ISO 17799 as-is, with minimal changes, however this is not the intended usage of this code of practice.

MISS: Minimum Information Security Standards (NIA)

6.5. The MISS is used as the basis for implementation of security in government institutions in terms of the requirements imposed by the NIA.

6.6. Much of the MISS is outlined in the Information Sensitivity Policy, and this Information and Network Security Policy builds on the Information Sensitivity Policy.

Electronic Communications and Transactions Act (25 of 2002)

6.7. The introduction to this Act reads :

- To provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy for the Republic; to promote universal access to electronic communications and transactions and the use of electronic transactions by SMMEs;

- to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-government services; and to provide for matters connected therewith.

6.8. This entire Act is critical for the creation of ICT Policies in both government institutions and in the private sector. The treatment of this is at a high-level in order to identify the places in which policies must consider the applicable sections.

Other Relevant Legislation

- Promotion of Access to Information Act (2 of 2000)

- National Archives and Records Service of South Africa Act (43 of 1996 / amended)

- Municipal Financial Management Act (56 of 2003)

- Promotion of Administrative Justice Act (3 of 2000)

SANS Security Guidelines

6.9. SANS offers a range of templates for specific security policies. Where appropriate these have informed the development of this policy.

7. Organisational Security

Management Information Security Forum

7.1. Due to the high level of importance of information security to the municipality as a whole, it is required that a management forum be established as a permanent part of the organisation of the municipality and is constituted by the Municipal Manager.

7.2. The composition of the Information Security Forum must include representatives from all key units as identified by the Municipal Manager and the IS Manager.

7.3. The Information Security Forum is responsible for the implementation of this Information and Network Security policy and will make its own decisions on how these must be conducted. These must include:

- Establishing roles and responsibilities as required.
- Monitoring significant changes in the exposure of information assets to major threats.
- Approving all initiatives that are designed to enhance information and network security.
- Determining the methods for ongoing risk assessment and security classification.
- Implementation of internal communications to promote awareness of information security and its impact on the effectiveness and efficiency of the municipality in carrying out its goals – in order to ensure commitment from all units and departments within the municipality.
- Integration of the information security policies with all information management within the scope of the IS Department.
- Establishment of specific controls and monitoring and evaluating the effectiveness and efficiency of these controls.
- Defining and maintaining the Security Incident Classification Scheme.
- Reviewing all information security incidents.

Information Security Officer

7.4. An Information Security Officer is the responsible person for the implementation of this information and network security policy, as well as all other related policies.

7.5. This manager will be appointed from within the IS department, and will report into the Information Security Forum.

7.6. In situations in which other managers are responsible for particular IT services and information they will report into the Information Security Manager in terms of the implementation of this policy.

7.7. The Information Security Manager, and all other managers as identified who have responsibilities for particular areas of information security, are responsible for the following:

- Identification of all assets in terms of the Register of IT Assets Policy (IT-01-03).
- Specification of the security implementation for each specific IT Asset in terms of this policy.
- The implementation of the security policies and procedures for each specific IT Asset.
- This requires clear identification of the responsibilities for security implementation as well as clear authority lines. These must be documented in terms of the Register of IT Policy and Security Roles as outlined in this document.

Security of Third Party Access

7.8. All third parties who may require access to the physical sites that are part of the information infrastructure as well as access to the information resources such as databases, networks and systems, must have such access rights clearly identified in contractual agreements.

7.9. This includes all contractors who are present on-site for various periods of time as per their contracts which may give rise to security weaknesses.

7.10. These third parties include the following:

- Hardware support staff

- Software maintenance and support staff
- Trainers
- Cleaners, caterers, security guards and related services
- Students and learnerships
- Temporary and casual personnel who are not considered as employees
- All consultants

7.11. Each contractor who is needed to be on-site must have specific security controls identified in the Service Level Contract or other contract with the contractor. The SLA must be created in terms of the guidelines provided in IT-12-01 Contract Management Guidelines.

Security in Outsourcing Contracts

7.12. Within outsourcing arrangements the municipality delegates responsibility for all or some of the IT services to an external organisation. In such arrangements, outsourcing contracts will be established to manage and control the arrangement.

7.13. As a part of such contracts the contractors will need access to secure information and services and the contracts must include provision for the following:

- Ensuring that all parties are aware of the security policies.
- How confidentiality of information is to be maintained.
- How integrity of the assets are to be maintained and how this will be tested.
- What access to information assets is to be provided.
- How availability will be maintained, including special provisions for situations of loss during disasters.
- Physical security for equipment, including municipal-owned and contractor-owned equipment.
- How security audits will be conducted.

7.14. The outsourcing contract must be created using the guidelines provided in IT-12-01 Contract Management Guidelines.

8. Identification and Control of Information Assets

8.1. All information security is performed in terms of identified information assets. All information assets must be identified clearly in an up-to-date Register of Information Assets as outlined in policy IT-01-03 Register of Information Assets.

8.2. All information maintained by the municipality is subject to classification in terms of the Information Sensitivity Policy IT-04-02. That policy also identifies the responsibility of the municipality in terms of communicating public information, and protecting private and sensitive information.

9. Personnel Security and Authorisation

9.1. All personnel who are part of or interact with the IT services could be the causes of human error, fraud, theft or abuse of the information assets.

9.2. Security considerations must be addressed at the earliest possible time, such as at the time of recruitment for employees, and at the time of contractual negotiations for contracted staff.

9.3. Staff and contractors who will have access to sensitive information, as identified in the Information Sensitivity Policy IT-04-02, must undergo specified security screening in addition to standard recruitment procedures.

9.4. Employment contracts and all third party contracts (IT-12-01 Contract Management Guidelines) must include a provision for confidentiality of information.

Employment Contracts and Contracting Agreements

9.5. Security and other checks must be included into the recruitment process and the results of these considered in the selection and appointment of new employees as well as the continuation of an existing employment contractor. These checks must include the following:

- Character references : business and personal references
- Completeness and accuracy of the CV
- Confirmation of all qualifications
- Identity check on the person
- Credit checks in cases in which this is applicable
- Police records where appropriate

9.6. For those employees with high levels of authority, these checks must be conducted at regular intervals as part of their conditions of employment.

9.7. These checks must also be conducted when employees change jobs in which their access to information changes.

9.8. These checks must be carried out as required for individual contractors and consultants in situations in which the contractual agreement is insufficient. This could include agreements with employment agencies providing temporary, contract or part-time staff.

Supervision

9.9. Sufficient supervision must be provided by management to new staff, as well as to temporary and contract staff in terms of the implementation of this information and network security policy.

9.10. Managers must be aware of personal situations of their staff which may impact and affect their performance and may in turn pose a potential threat to the municipality. For example, evidence of financial difficulties poses a potential threat for fraud.

User Training

9.11. All users of all IT services must be trained adequately to operate and use the IT services and all IT resources effectively and efficiently.

9.12. The requirements for such training are given in the Guidelines on IT Training (IT-10-01).

10. User Administration, Access Control and Personal Communications

10.1. Access to information resources must only be provided to authenticated and authorised users.

10.2. All users must have an authorised user code and strong password.

10.3. All access to sensitive IT services and sensitive information must automatically be logged in an audit trail.

10.4. The policies and procedures for the allocation of user codes and rights, as well as the management of user rights, are provided in policy IT-05-02 UserID and Password Policy.

10.5. Access to all network services requires acceptance of the Network Access Acceptance (IT-05-51).

10.6. Email Disclaimer is required as part of all email communications (IT-05-01).

11. Access Control Security

11.1. This section of the information security policy provides a set of specific policies for a range of situations that the municipality is required to control. All these policies concern the external access to the network.

Network Access Control

11.2. Access to IT services from both internal and external network facilities must be controlled adequately. This will ensure that users who use the IT services through the networks do not compromise the security of the IT services.

11.3. The path from each user workstation to the networked services needs to be controlled in terms of the needs for security in specific IT services and for specific users.

11.4. This must be accomplished through a variety of means such as:

- Dedicated telephone numbers for access to specific services.
- Automatically connecting ports to specific applications.
- Preventing unlimited network roaming for specific users.
- Usage of firewalls to control access between internal services and network users at a fine level.

11.5. Users within the municipal offices must access the network through cable connections from their desktop computers.

11.6. Laptop computers must use either cable connections or wireless connections through established security access protocols and codes.

11.7. All users must have a valid user code and password and must use secure authentication methods to access the network. The policy IT-05-02 UserID and Password Policy must be used to allocate and revoke user codes and to ensure adequate controls on password selection.

Wireless Communication Policy

11.8. All wireless infrastructure devices that are connected to the municipal network or which reside at the municipal site and which provide connectivity to any network endpoint, such as laptops, desktops, mobile phones or PDAs are subject to the following specific conditions of usage:

- They must abide by the Wireless Communication Standard identified below.
- Must be installed by an approved support team.
- Must use approved authentication protocols and infrastructure.
- Must use approved encryption methods.
- Must have a hardware addressed (MAC) that can be registered and tracked.
- Must not interfere with any other wireless access devices maintained by the municipality or other organisations.

11.9. Access is only provided on completion and approval of the Wireless Access Request Form (IT-05-56 Request for Wireless Access).

Wireless Communication Standard

11.10. All wireless devices that connect to the municipal network or which provide access to sensitive information as per the Information Sensitivity Policy must:

- Use an authentication protocol which is one of EAP-FAST (Extensible Authentication Protocol Fact Authentication via Secure Tunnelling), PEAP (Protected Extensible Authentication Protocol) or EAP-TLS (Extensible Authentication Protocol Translation Layer Security).
- Use TKIP (Temporary Key Integrity Protocol) or AES (Advanced Encryption System) protocols within a minimum key length of 128 bits.
- Enable WiFi Protected Access Pre-Shared Key (WPA-PSK), EAP-FAST, PEAP or EAP-TLS.
- When enabling WPA-PSK configure a complex shared secret key of at least 20 characters on the wireless client and the wireless access point.
- Disable broadcast of the SSID.
- Change the default SSID name.
- Change the default login and password to the wireless device.

Remote Access Policy

11.11. Remote Access in this context means dial-in, ISDN or VPN or any other means of creating a connection between user and the municipal network from sites outside of the fixed network of the municipality.

11.12. This policy applies to all situations in which a user can access the municipal network using remote access facilities.

11.13. This does not apply to access to the public municipal Internet sites for which no access is provided to the municipal network.

11.14. Remote access is only available to authorised users and is always provided for a limited period. Following the expiry of the limited period the user is required to re-apply.

11.15. Users who require remote access must apply using the appropriate form (IT-05-62 Request for Remote Access).

11.16. All users who have been granted remote access must give the same consideration to this form of network access as they have in terms of on-site connections within the municipal offices, and all policies applicable to on-site connections are also applicable to remote access connections. This includes all acceptable use policies.

11.17. All employees and third parties granted remote access must ensure that no unauthorised users make usage of this remote access. If such authorised users believe that their remote access has been used by others they are required to report this immediately to the Information Security Manager.

11.18. The users must never store their remote access codes to the remote access services on their personal computers, and this also includes the facilities for computers to remember the logon codes and passwords.

11.19. The user must never provide their user code, password or other credentials to others in any form.

11.20. Users who are connected to the municipal network using remote access facilities must not be connected to other networks at the same time.

11.21. All computers that have access to the municipal network via remote access must ensure that they have up-to-date anti-virus software installed and activated at all times.

11.22. Remote access must always require strong passwords (as identified in the UserID and Password Policy), one-time passwords or a public/private key system with a strong passphrase.

11.23. Users will be disconnected automatically from the network after 30 minutes of inactivity.

11.24. The user is directly responsible for all contraventions of this policy.

Dial-up Access

11.25. Dial-in facilities are only provided on an as-needed basis in situations in which other forms of remote access, such as VPN, are not possible.

11.26. All dial-in users are required to re-register for these services every 6 months.

11.27. All modems used for dial-in access must be SABS approved and this includes modems integrated into laptops as well as external modems.

11.28. Only GSM Cellular telephones are allowed to be used to connect to the network and not analog and non-GSM cellular phones. This is because of the threat of scanning by unauthorised parties.

11.29. Dial-up access may be needed to provide remote support in the eventuality that other forms of remote access are unavailable.

VPN Access

11.30. When VPN access is provided, it is the responsibility of the users to have their own Internet access arranged through an Internet Service Provider, and they are responsible for their own fees for these services.

11.31. The following additional considerations apply to users accessing the municipal network remotely via VPN:

- When a user accesses the municipal network via a VPN connection all other network access for the user will be dropped. This will include general Internet access.
- Dual tunnelling is not permitted, and only one network connection is allowed to be used while using the VPN.
- VPN facilities will be managed by the municipality IS Department.
- No VPN connection will be allowed to last more than 24 hours.

- Computers which require connection to the VPN and which are not municipal-owned or under the control of the municipality IT Department must be checked in advance to ensure that they comply with this policy.

- Only VPN clients officially sanctioned by the IS Department may be used to access the municipal network through the VPN.

Firewall Policies

11.32. All network traffic between the internal IT services and the outside must pass through the firewall which must include both logical and physical controls.

11.33. The firewall must be immune to penetration.

11.34. Traffic must be exchanged at the level of the application layer only.

11.35. The following must be observed in the configuration of the firewall:

- Combines control measures at both the application and transportation layer.

- Enforces protocol discontinuity at the transportation layer.

- Must be configured according to the "minimal art philosophy".

- Must employ strong authentication for management of its components.

- Must hide the internal structure of the network.

- Provides an audit trail of all communications to or through the firewall system and will generate alarms when suspicious activity is detected.

- Will defend itself from a direct attack through active monitoring of traffic and through pattern recognition technology.

Operating System Access Control

11.36. This policy covers access to servers and other shared IT services other than application systems.

11.37. All internal servers deployed at the municipality must have a well-defined responsibility for system administration. This will generally be the IS

Department but this responsibility may be delegated as required to other municipal departments if this is appropriate.

11.38. No department may operate a publicly accessible server without the permission and monitoring of the IS Department. This of specific concern in the case of Internet Servers.

11.39. All servers must be registered with the IS Department, even if they are run and operated by other departments and units. For each server the following information must be available at all times, recorded in the Register of IT Assets:

- Hardware description in detail : including make and model, memory type and size, disk type and capacity, processors and their configuration, and any other components that have been installed.
- Server location : where it is located, such as room, cabinet, rack, position.
- Server connectivity : how this server is connected with other servers.
- Operating system and version.
- Specific patches applied.
- All security software included, such as anti-virus and monitoring software.
- Primary function of the server, as well as its key applications.
- Whether this is a live production server, or a testing/staging server.

11.40. This information must be kept up to date at all times.

11.41. All configuration changes for production servers must follow appropriate change management procedures.

11.42. General Configuration Guidelines include the following:

- Any specific services that are not needed to support the functions that the server is required to perform must be disabled.
- Access to specific services on each server must be logged and protected through appropriate access-control methods

- All security patches and other patches must be installed as soon as is possible, unless these interfere with existing business operations.

- Trust relationships between servers, which allow authentication credentials to be shared, must be used only to the extent that other forms of inter-server communications are not possible.

- Do not use the root account, or similar super user accounts, when a less privileged account can perform the same function.

- Where possible, use different security accounts for each service.

- The password to the root password and other passwords and account names for services must be protected at all times and also must be available as required. These must be stored in a locked safe for which the keys are available only to specific identified personnel.

- All servers must be located within access-controlled and protected server room facilities which are controlled in accordance with the policy IT-05-01 Physical Access Security. Server facilities must never be operated in areas that are not controlled, such as open working areas.

11.43. All servers must be monitored as follows:

- All security events and related sensitive events must be logged as audit trails.

- These security audit logs and other system logs must be reviewed on a daily basis by the Information Security Manager to identify potential and actual threats. For example, multiple logon failures on key security accounts.

- Any threats must be brought to the immediate attention of the IS Manager for further decisions on appropriate action.

- Security audit logs and associated server logs must be kept for at least 2 years, with as much as possible of the logs being kept online.

Application Access Control

11.44. Each application system must have its own access control capabilities to ensure that only authorised users are able to access the application.

11.45. Each application system must exploit single-sign-on (SSO) capabilities where possible, to avoid multiple user accounts being maintained for individual users.

11.46. Each application system must maintain its own access control to specific functions and capabilities and to ensure that individual users can be allocated and de-allocated permissions.

11.47. All logon events and other key security events must be logged at the application level. Where appropriate these events can be logged into the server application logs.

12. Operating Systems Security

12.1. All computers are controlled by a range of systems software including operating systems, email servers, internet servers and database servers. Security weaknesses are commonly discovered in these components and patches are provided by the vendors in order to remedy these weaknesses.

12.2. When security weaknesses are detected this information can be used to gain access or to gain control of computers by bypassing the security controls.

12.3. It is essential that all patches provided by the vendors (such as Microsoft, Oracle and others) are applied immediately that they are available. Where possible automatic updates must be enabled on all servers to support the implementation of patches on a timer basis, and the timer must be set to check for new patches at least once per day.

12.4. In situations in which there is no suitable automatic patching mechanism, then a specific person must be allocated by the IS Manager to check every day for updates and then to apply these manually. A report must be prepared every day on all patches applied.

12.5. Serious security notifications may require rebooting of the servers and this may result in disruption of the IT Services and in extreme cases may result in locking down the servers until specific problems are resolved. In such a case it is not possible to communicate with the users through normal methods and an alternative method of user notification must be provided, such as through SMSs on mobile phones.

13. Cryptographic Controls

13.1. Cryptographic systems and techniques must be used for the protection of information that is considered to be sensitive or at risk and for which other controls do not provide adequate protection.

Encryption Keys

13.2. All decryption keys to be lodged with IS including the information concerning the types of encryption used. This to be done for each situation in which encryption is used.

Decryption Directions (RIC 21/29/30).

13.3. A designated judge may, on request, issue a decryption direction which requires the decryption key and related assistance to be provided for the decryption of specific information as identified in the direction.

13.4. The municipality needs to ensure that such a direction can be complied with by implementation of a suitable policy on key management and encryption.

Cryptography Providers

13.5. All cryptographic services and products must be provided by one of the providers maintained in the registry identified in s29 of the ECT Act.

14. Physical Security

Physical Access

14.1. It is essential to implement a comprehensive and practical physical security policy.

14.2. This is required to help prevent unauthorised access, damage and interference in business premises and information.

14.3. This is outlined in the policy Physical Security and Access Authorisation IT-05-01.

Environmental Controls

14.4. Equipment must be maintained in suitable environmental conditions to support optimal operation of the equipment. This specifically applies to data centres and server rooms.

14.5. Controls must be in place to minimise threats arising from:

- Theft
- Fire
- Explosives
- Smoke
- Water (or the lack of water)
- Dust
- Vibration
- Chemicals
- Break in electrical supply
- Electromagnetic radiation

14.6. Existing South African legislation provides for non-smoking in the workplace and this is of additional concern in or near computer environment. No smoking must be allowed in any area in which computing facilities are present.

14.7. There must be no drink or food allowed in any of the central IT services including server rooms, data centres and training rooms. It is also recommended that this practice be applied by users in their own offices.

Power Supply

14.8. Servers and other centralised IT services must be protected from breaks in electricity supply.

14.9. This must be accomplished by a combination of support structures including:

- Battery backup to support the first few seconds (30 seconds) of a total break.
- UPS facilities for longer delays as required.
- Backup generators to support up to 5 days of operation.

14.10. It is essential that the fuel supply for the generators is available in a safe environment and that this itself does not represent a fire risk.

14.11. Generators must be tested on a regular basis, as well as the fuel supply. Records must be maintained of these tests.

14.12. Emergency shut down of equipment must be possible from emergency exits to facilitate rapid power down in the time of emergency.

14.13. Emergency lighting must be available in all critical locations.

14.14. Lightening protection must be provided for all buildings housing critical IT infrastructure.

14.15. Cleaning staff and others who have access to server rooms must have their own power points for the usage by cleaning machines. They must not have access to the power points for the key IT equipment.

Cabling Security

14.16. All cables for power, networks and external communications must be protected against intentional or accidental damage, as well as from interception.

14.17. Some guidelines for this are the following:

- All cabling moves outside of public areas and remains invisible where possible.
- Power cables must be segregated from network cables.
- Access to conduits and control boxes must be controlled.
- Alternative routings must be provided for cables where this is critical.
- Regular sweeps must be conducted to detect unauthorised devices that may be intercepting the transmissions on the cabling.

15. Security Threats and Incident Management

15.1. Security incidents must be reported to the Information Security Manager as quickly as possible and it is the responsibility of the Information Security Manager to acknowledge receipt as soon as possible and to immediately analyse the incident in order to decide on the most appropriate action.

15.2. Security incidents include any and all violations of the elements of this policy and all related security and IT policies and procedures. The Information Security Forum must create and maintain a Security Incident Classification Scheme, and also identify the suitable responses for each class of incident.

15.3. The classification scheme must be based upon a variety of characteristics of the security incidents, such as their impacts, their causes, and the elements in the IT services that are affected:

- Software / hardware / network faults
- Suspected threats – including viruses and intentional destruction
- Cyber crime incidents
- Violations of acceptable use policies

15.4. The Information Security Manager is always the owner of each incident, and is delegated the authority to handle each incident by the Information Security Forum.

15.5. Depending upon the severity of the incident, some or all of the Information Security Forum may be required to assist the Information Security Manager in decision-making.

15.6. All security incidents notified must be used to increase the knowledge of security weaknesses and responses.

15.7. If there is a need to implement the interception of messages, or the inspection of private data stored, then the Information Security Forum must approve this explicitly in writing.

15.8. A lockdown process must be defined by the Information Security Forum and implemented by the Information Security Manager if the security incident warrants this lockdown.

16. System Development and Maintenance

16.1. This section only concerns the security implementation within systems development and not the entire systems development life cycle.

User Rights to Application Systems

16.2. It is essential that every system developed and/or implemented implements best practice in information and network security. This is the essence of a “single-sign-on” (SSO) approach.

16.3. Individual systems must not implement their own user authentication procedures, but must use the municipal security systems. This provides a centralised point of control of user access.

16.4. Individual systems must maintain their own user right management processes, to support fine levels of access rights required.

16.5. Each individual system must support a user administrator role which manages the specific user rights available within individual systems.

16.6. Access rights to individual systems must be logged and records maintained of all changes to user rights.

Data Integrity and Validation

16.7. Databases must be structured to support as much data integrity as possible, so that incorrect data is not able to be stored. This must include at least:

- Primary key and unique keys.
- Foreign keys and referential integrity.
- Required data fields.
- Data types appropriate to the data stored (for example, not using text fields to hold dates and numbers).
- Check constraints to restrict data values in specific fields (such as M/F in gender fields).
- Business rule constraints, in which specific business rules prevent storage of data (such as for purchases beyond a credit limit).

16.8. Where possible, data must be modified through stored procedures in database systems and not by accessing the tables (or other storage units) directly. This has the benefit of preventing changes that have not been considered and also allowing flexibility in the changes to the database design.

16.9. All data entered by a user into an application system must be controlled through data validation checks, even if the same checks are already installed within the database. These must include the following:

- Out of range checks
- Invalid characters in data
- Missing / incomplete data
- Upper and lower bounds
- Unauthorised access by specific users

Data Change Auditing

16.10. Where possible, all application systems must maintain an "eternal log" of all changes made in the entire history of the application. This must indicate who made each change and when the changes were made as well as containing the details of each data change.

17. Procedure: Reporting and Responding to Security Incidents

Purpose

17.1. The purpose of this procedure is to have a formal process for centralising responses to security incidents.

Trigger

17.2. This is triggered by any situation or event that may threaten any part of the information security.

17.3. A security incident is any violation or suspected violation of any element of the Information and Network Security Policy or any related policies.

17.4. This is done as soon as possible after the incident is noted. Timing is always critical when dealing with security incidents and threats.

Requestor

17.5. The Requestor is any person with access to the information network or physical areas of the IT infrastructure that identifies a problem. In effect this applies to everyone within the scope of the municipality.

17.6. At all times the individuals concerned must adopt the principle of "safe rather than sorry" in situations in which there is uncertainty. It is essential to err on the side of caution by raising false incidents that can be clarified rather than failing to raise true incidents because of incomplete information.

17.7. It is noted that every very serious security breach was noticed by someone at some time and that in many cases the threat and impact can be reduced by early action.

17.8. Either the Information Security Manager or an assigned delegate must be on call throughout the times that the IT services are available. This will be 24 hours a day, 7 days per week for the municipality, since on-line access is provided continuously and intentional security violations are more likely to occur after normal business hours.

Responsibility

17.9. Every security incident is owned by the Information Security Manager or their delegate.

17.10. The Information Security Forum must be convened if there is a need for immediate escalation. An attempt must be made to inform the IS Manager immediately no matter where s/he is and what his/her situation. In the absence of the IS Manager, the Deputy IS Manager and the IS Security Manager must be directly involved.

Steps

Seq	Activity	Who	Duration
1	A situation or event is noted that poses a potential threat to any part of the security of the information assets of the municipality. Requestor gathers as much immediate evidence as possible to substantiate the threat.	Requestor	
2	Requestor reports this to the Support Desk, who immediately notifies the IS Security Manager. The Support Desk gathers as much information from the Requestor as possible.	Support Desk	
3	The IS Security Manager identifies the key personnel required to assist and they are briefed on the event. The IS Security Manager requests an urgent report on the incident within a specific time frame. This must include a search of the Lessons Learned Log from previous incidents to detect patterns and also to detect prior solutions. Any similar situation for which there is a prior solution must be applied immediately.	IS Security Manager	
4	The incident report is provided to the IS Security Manager and they decide on whether to continue with the threat monitoring or to ignore the incident.	IS Security Manager	
5	If the decision is to continue, then the incident is tracked and problems are addressed on a case by case basis. There are no general rules.	IS Security Manager	
6	Once the incident has been dealt with, the IS Security Manager is responsible for recording the problem and its resolution into the Lessons Learned Log for the benefit of future incidents and threats.	IS Security manager	
7	The incident is closed.	IS Security Manager	

Forms and Registers

17.11. The standard logging system of the Support Desk is used. There is no other Form to be completed. It is expected that completion of a form will waste valuable time in response to potentially critical threats.

Practice Notes

17.12. Timing is essential in these situations since it is not possible to determine immediately whether this is a very large threat or a non-threat. All situations reported must be dealt with as though they are at the top level of threat until proven otherwise.

17.13. There will possibly be a host of false alarms but this must never detract from the seriousness given to each and every incident.

17.14. In practical terms this will be carried out by the Support Desk and other experts within the IS Unit and not by the Requestor. The Requestor's primary responsibility is reporting the initial incident.

17.15. The types of threats and incidents will include the following:

- Telephonic or SMS threat or other written or verbal threat against any of the information assets or people in the IS Unit.
- Loss of service for reasons unknown.
- Suspicion of data loss or changes not planned.
- Virus warnings or other malicious code.
- Threats concerning the physical space such as loss of access to key spaces.
- External threats that may impact on the internal operation such as riots near the municipal offices.

17.16. Any form of communication is acceptable as a notification to the Information Security Manager including fax, email, telephone, voice mail.

17.17. The telephone numbers and email addresses for reporting incidents must be available at all times that this procedure is required to be operational.

17.18. Fallback numbers are required to be provided in cases in which the primary security person is not available.

17.19. It is very important that there is confirmation of the notification of the security incident and where possible this must be provided by a return email or fax, or by the provision of a security incident number.

17.20. The Information Security Manager must give feedback to the person notifying the incident as soon as possible in terms of acknowledging receipt of the incident notification.

17.21. The Information Security Manager on receipt of a security incident notification will immediately carry out the following actions:

- Classify the incident using the Security Incident Classification Scheme.
- Confirm the incident.
- Determine the initial impact and priority for response.
- Plan an initial response.
- Depending upon the severity, invoke the escalation procedures and inform the Information Security Forum to take over the authority for handling the incident.
- Determine whether interception of messages is required to be implemented and seek the appropriate approval from the Information Security Forum.

17.22. The Information Security Manager must then carry out the plan, and include internal and external personnel as required.

17.23. All Security Incidents must be logged into a Security Log and this must contain all of the relevant information:

- The date and time.
- The person reporting the incident and their contact details.
- The complete details of the incident.
- The plan used to deal with this.
- Analysis of the approach and how this can be used to improve best practices.
- The performance of the response as evaluated and whether this meets standards and guidelines.

Performance of Response to Security Incidents

17.24. Each type of incident is different therefore it is important to establish a set of norms and standards on how quickly and effective the response has been to each incident.

17.25. Threats due to serious virus infections can bring down an entire organisation.

Lockdown

17.26. If the incident is serious then a lock down may be recommended for the municipal IT infrastructure. This can be done by the Information Security Manager without the authority of the Information Security Forum if the incident warrants this.

17.27. The lockdown must include consideration of the following:

- physical lockdown, in which access to sites is only for specific individuals.
- access lockdown, in which all access into the network is shut off, except possibly for support access points.
- security key lockdown, in which key access accounts have their passwords changed immediately.
- application lockdown, in which specific applications are shut down.

Enforcement

17.28. This is required to be enforced by the IS Security Manager.

Review and Audit

17.29. This process must be reviewed every 12 months, or after any serious security incident.

18. Forms / Registers

Form: Acceptance of Responsibility for IT Policy and Security Role (IT-01-62)

18.1. This form must be signed by all personnel who have a role within the IT Security Organisation structure, including members of the Information Security Forum, the Information Security Manager and all other personnel with assigned roles.

18.2. The following information must be provided on this form:

- The Role.
- The Name of the Employee who is assigned this Role.
- The starting date of the role.
- (The ending date if this role is no longer held by this person).
- The summary of the key responsibilities (with reference to the policies and procedures).
- Who the Role reports to, and the nature of this reporting process.

Register of IT Policies and Security Roles (IT-01-51)

18.3. This Register is maintained by the Information Security Forum. It contains a list of all of the Roles and identifies the specific personnel who hold this role, as well as their assigned delegates who can stand-in, in the event that the role-holder is unavailable.

18.4. This Register must be maintained and be up-to-date at all times and be available.

18.5. This Register will contain the list of all personnel who have completed the Form: Acceptance of Responsibility for Information Security Role, as well as keeping the original signed forms as completed by the personnel. The register must contain the following information:

- The Role.
- The Person Assigned.
- The starting date and ending date of the assignment.

- The Delegate for the person.
- Contact details as required.
- Classification of the type of incident.
- A detailed incident report.
- The response to the incident, including the success.
- The impact in terms of losses and costs of recovery.
- Lessons learned to improve the security policy, procedures and infrastructure.

Security Incident Log

18.6. This is a log containing all of the relevant information as required within the security incident policy and procedure.

19. Review

19.1. This policy will be reviewed every 12 months.

20. Audit Guidelines

20.1. This policy is large and contains many areas which are of critical concern to the implementation of secure IT Services. As a result, a set of basic guidelines are provided which can inform audits, including self-audits within the IS Department, as well as those conducted by the Internal Audit department. It is expected that external audits will contain a materially similar set of audit guidelines.

20.2. These audit guidelines identify specific checks that can be provided in order to identify gaps that must be remedied following audits.

Communication of IT Security Policy

20.3. This policy and related policies have been communicated to all relevant people, they are understood by these personnel and are being enforced by the people identified as enforcers.

Register of IT Assets

20.4. A complete list of current IT Assets is provided in the Register of IT Assets.

20.5. This indicates the current status of each of the IT Assets as well as the security restrictions required to be applied to each.

User Management

20.6. Procedures are in place for new user accounts and for maintaining user accounts.

20.7. These procedures are being used for access to the municipal network, as well as for all systems which have their own security codes.

20.8. The personnel who are responsible for enforcing these procedures are fully knowledgeable about their responsibilities.

Log On

20.9. At logon time to the municipal network there is a message to the user that by continuing they agree to comply with the Acceptable User Policies (as provided by IT-05-51 Network Access Acceptance).

20.10. Procedures for external access to the municipal network are in place and are being applied in practice.

Access Control

20.11. Users are not allowed access to individual subsystems unless they have logged on as an authorised user of the municipal network.

Firewalls

20.12. The guidelines for implementing and configuring firewalls meet the policy statements in this policy.

Malicious Software Protection

20.13. All software acquired by the municipality is checked for virus contamination prior to installation and usage.

20.14. Critical software is protected by digital signature which is verified prior to loading.

20.15. Users understand the problems associated with malicious software and know what steps to take in the event of infestation.

20.16. All external data being used on a municipal computer or the IT services is checked for contamination prior to being used.

Security Incident Handling Procedure

20.17. All incidents are reported correctly.

20.18. Incident Reports are prepared in accordance with the procedure.

20.19. Incident Reports are complete and are available to support queries as Lessons Learned Logs when new incidents arise.

20.20. The response to security incidents is correct in terms of the deployment of resources and the identification of the threat.

21.Review and Audit

20.1. This policy will be reviewed after three years from the date of approval or should a need arise.

20.2. The enforcement of this policy will be audited as follows:

- Random monitoring of email messages and users
- Non-random monitoring of users in situations in which there is reasonable suspicion of transgression. For example, on the evidence of high email usage.

* * * END OF DOCUMENT * * *

a) **Date of Approval by Council** 29/05/2025

b) **Signed on behalf of Council** ________________