IT DATA SYSTEM SECURITY POLICY

MUNISIPALITEIT
RICHTERSVELD
MUNICIPALITY

Council Resolution
RVN002/06/2016

Special Council Meeting:
24 June 2016

CONTENTS **PAGE**

1. INTRODUCTION

ICT data and systems security planning, for which the manager of the ICT function is responsible, is the section that deals specifically with the application and management of security, both physical and logical, for securing Richtersveld Local Municipality data and systems against unauthorised access, modification, destruction and usage. The operational security plan, for which the designated security manager is responsible, is the section that deals with ICT security issues, breaches, recovery and prevention of unauthorised access. The operational security plan is derived from the security policy and must be applied to all data, systems, infrastructure and users of Richtersveld Local Municipality ICT systems.

The purpose of the ICT Data and Systems Security Policy is to set guidelines to be adhered to by all affected environments within Richtersveld Local Municipality. It also ensures a co-ordinated synergy towards the designing and implementing of Security Plans and solutions throughout Richtersveld Local Municipality.

In terms of risk management, security planning philosophy is one of "prevention is better than cure". All reasonable, justifiable and cost effective precautionary measures should be taken to prevent the unauthorised access to data and systems of Richtersveld Local Municipality. The security policy governs access to municipal data and systems on the principle of need-to-know.

Information security requires the participation and support from all staff (including consultants, contractors, and temporaries) who will be provided with sufficient training and supporting procedures / policies to allow them to properly protect and manage Richtersveld Local Municipality information assets.

It is the responsibility of all municipal staff to report any software malfunctions, security incidents, suspected viruses, faults, weaknesses or threats observed or suspected to systems or services to the Helpdesk, Information Security Officer or manager responsible for information/system security as soon as possible to enable the volumes and costs of incidents and malfunctions to be quantified and monitored.

2. THE IMPORTANCE OF AN IT DATA AND SYSTEMS SECURITY POLICY AND PLAN

By defining an IT security policy and plan Richtersveld Local Municipality prepares itself for the possibility of unauthorised access attempts, malicious code, e-mail bourn attacks and unauthorised data and system access internally from staff. A security policy and plan is essential for the day to day operations of Richtersveld Local Municipality. Failure to prepare for the possibility of attacks on the systems and data of Richtersveld Local Municipality would result in a loss of data, systems and access to confidential and sensitive systems and information by unauthorised individuals or groups.

It is important that the ICT security plan and policy be defined within the framework of an organisation wide effort to adhere to security measures and prepare defences against system based attacks. The ICT systems are a component of the overall organisation and it must be recognised that IT provide critical support services. Without the ICT systems, many of the organisations key processes would stop and financial and /or loss of life may result.

3. COMPONENTS OF THE IT DATA AND SYSTEMS SECURITY POLICY

The data and systems security plans and policies consist of two main documents. The ICT Security policy statement and Network Security Policy that governs access to the network and connects from external networks to the internal network. Each of these documents is briefly described below.

3.1 ICT Security Policy

The ICT Security policy lays down the rules for obtaining, granting and managing access to Richtersveld Local Municipality data and systems. The policy also specifies minimum requirements for systems configurations, password composition/formats and maintenance of audit trails and reporting on security events.

The ICT Security policy is divided into the following main sections:

1. Preamble, purpose of the policy and justification or requirement for an ICT security policy.
2. The purpose of the policy in terms of the policies objectives and goals.
3. Scope of the policy, which defines the limits of the policy in term of what areas of ICT are included and which are excluded as well as why those areas are excluded.
4. General guidelines for the application of the policy and who should administer and enforce the policy.
5. A definition of information security.
6. High level information security principles that set out the principles for the formulation and application of an ICT Security policy.
7. Generally applicable policy statements that are not specific to a department or system, but can be applied in general to areas requiring security.
8. The Management Policies which specify ownership of the policy, some roles and responsibilities and security procedural requirements that must be applied and adhered to by all. The management policy statements also specify access to systems, monitoring and minimum specifications for security measures.
9. A User Policy that all users and managers of data (regardless of form – hardcopy or electronic), must apply and adhere to. Failing which disciplinary action may result.
10. Any Legal and Regulatory requirements that may apply to ICT security in municipalities.
11. Disciplinary code of practise for breaches of the policy.
12. A high level implementation plan.
13. The effective date from which the current version of the security policy will apply.
14. A compliance statement accepting the provisions of the policy and responsibilities that may apply to the user.

3.2 Network Security Policy

The Network Security Policy support the overall IT Security Policy, but deals with specific issues around the connection of networks to other networks and organisations, World Wide Web access and security measures and access control regulating who may access the network and when such access may occur. The policy also specifies what documentation should be maintained and when it should be updated and how risk should be assessed when connecting third parties to the network or allowing external access to the municipal data and communications networks.

The Network Security Policy is divided into the following main sections:

1. Purpose and objectives of the policy.
2. Background to the need for Network Security and Access control procedures.
3. Scope of the policy that sets out the extent of the reach of policy and what in included and what is excluded.
4. Terminology definitions for clarity and a common understanding of terms used in the policy.
5. The main Policy statements that set out the rules and security procedures to be applied to the network.
6. Policies governing the reporting and logging of security incidents.
7. A summary of the main responsibilities of key role players and municipal official duties.
8. A statement with regards to the application of disciplinary procedures for failure to apply the policies set out in the document.
9. The effective date from which the current version of the security policy will apply.

4. ORGANISATIONAL INVOLVEMENT IN IT SECURITY PLANNING

It very important that ICT Security planning and processes do not take place in isolation from the rest of the organisation, indeed data and systems security is the responsibility of all stakeholders in Richtersveld Local Municipality – this includes all users of the municipal systems. For this reason, ICT security planning and management normally involves users and managers from all departments as access requirements need to ensure that users have access to the data and systems required for their daily duties. The ICT Security plan should also integrate with the municipal disaster recovery and planning processes. The ICT security policies and access controls must be clearly communicated to all managers and users of the municipal ICT systems. Training on the policies must be included in the general training of staff and municipal officials and in induction training.

4.1 Who to Involve in ICT Security Planning

In order to ensure comprehensive ICT security management, policies and plans are developed, it is essential to involve the broader organisation and respective departments, key service providers and third parties involved in the provision of systems, hardware, applications, skills and other materials.

The data and systems access requirements must be defined from a departmental level and include all users, all jobs and functions within Richtersveld Local Municipality.

The ICT disaster recovery team should therefore include members from the disaster planning and management committee and heads of departments to ensure that all critical systems are included in the plan and that systems security and access requirements are correctly defined. Third parties and ICT suppliers and service providers (Telkom's, Eskom, Banks, ICT service providers, etc.), should also be included as these organisations will be responsible for supplying services and may have or require access to the municipal data stores and systems. The vendors of security products and systems are often required to provide configuration and maintenance services to Richtersveld Local Municipality. Steps must be taken to ensure that they are included in the security definition process and that they fully understand and comply with security, confidentiality and non-disclosure requirements. Any potential weaknesses or problem areas noted and it should be ensured that any risks that may exist are mitigated.

It should be noted that external organisations may be dependent on services provided by Richtersveld Local Municipality. Therefore, these organisations may request to review or be involved in the municipal ICT and data security planning process to ensure that they have full understanding of dependencies between their organisation and Richtersveld Local Municipality.

4.2 When to Involve Them

The key members of the security management department or committee should be involved in the planning process and policy definition from the start to ensure that any external ICT dependencies or requirements are fully understood and incorporated into the ICT level policies and plans. Third parties can be involved as and when required, but particularly during the negotiation of replacement systems.

4.3 Service Level Agreements and Implications

As service level agreements may be defined between the ICT department and other organisational departments, provision should be made in the Security policies and plans for their suspension or modification during an attack or security breach.

Attention should be given to externally agreed service level agreements and the impact of these data and systems security planning and enforcement. It may not be possible to meet certain service level agreements, by identifying these and discussing the implications with the respective parties beforehand, disagreements and conflicts can be avoided during the period when co-operation between parties is a key to successful management of the breach.

5. COMMUNICATING THE POLICIES

All policies, security plans and responsibilities must be communicated to the department heads, the members of the security department or committee and particularly to all resources within the ICT function. Those individuals that have specific roles and responsibilities in terms of the policies and plans must be briefed in detail on the requirements for performance that will be demanded of them during the application of controls, procedures or investigations and systems recovery processes.

All staff should be provided with training on the requirements for data and systems security and the responsibilities of each staff members to uphold the security policies and raise any suspicion of breach of the policies or systems. The objective of this training should be raise awareness for the need for data and systems security. All new joiners to Richtersveld Local Municipality must receive training on the policies upon joining in the induction program.

6. IMPLEMENTATION OF THE DRP POLICIES

Policies and plans are only effective if properly implemented. By implementation it is meant that the policies and plans are documented, communicated and fully understood by all relevant role players. Implementation is only complete when individuals with defined roles and responsibilities are fully trained to carry out the tasks and responsibilities in accordance with the policies and plans. The following sections briefly discuss the implementation of policies and plans.

6.1 Allocation of Roles and Responsibilities

Implementation of each section of the policies and plans and the tasks contained therein must be formally allocated to individuals who must formally accept the responsibility for the adherence to and implementation of the policy or activity.

6.2 Training

Once the roles and responsibilities have been allocated and accepted by the individual resources, training on the policy, procedures and plans must be provided. The training must create the capacity to implement, adhere to and monitor the respective areas of responsibility. The role players must fully understand the importance of the policies and plans and how each procedure and sub section contributes to the overall security management program. Ideally, an understanding of the overall security plan must be conveyed to each resource.

6.3 Monitoring Implementation

Once implementation in underway, all the tasks and activities must be monitored to ensure adherence to the policies and plans laid down. Corrective actions must be instituted to rectify any deviations from the policy. All audit trails and system reports should be reviewed on a daily basis to ensure that no system breaches have occurred and that non unauthorised system access has been attempted. Action plans to address any security breaches or failed access attempts must be formulated and implemented immediately upon the acknowledgement of such an event.

6.4 Testing ICT Data and Systems Plans and Policies

Once implementation is complete and all training has been provided, the IT security plans and policies must be tested to ensure that the function as expected. The security plans must be periodically tested to ensure that all security facilities and systems controls function and that no changes are required to processes and procedures. The security plans should be tested after every major system change or change in responsibilities and roles. Regular testing will uncover any weaknesses in the security plan and processes and will help to identify where the processes can be optimised and where additional training is required.

6.5 Storage of and Access to Documents

All relevant documentation, policies, procedures, plans, checklists, etc., must be stored in a safe location where it can be secured from tampering but is also easily accessible in the event of an emergency.

7. POLICY REVISIONS

7.1 When to Revise the ICT Security Policy

Policies and plans should be reviewed from time to time to ensure that they take any system and procedure changes into account. More specifically, policies and procedures should be reviewed when any of the following events occur:

- A new system is implemented.
- A major component of a system has changed or a component change would result in a different security procedure.
- A change in staff occurs or a re-allocation of responsibilities is required.
- A change of supplier takes place or a supplier contract in moved to a different vendor.
- There is a major change in the cost components and budget requirements to administer and secure a system.
- A higher level of efficiency in the security procedures is required to reduce risks to the data and systems.

7.2 Who Should Revise the ICT Security Policy and Plans?

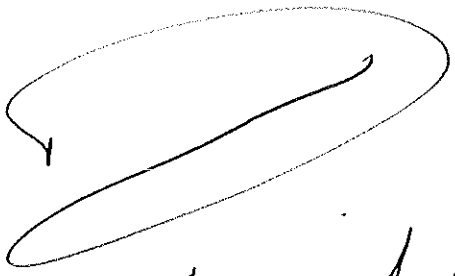
Generally, it is the responsibility of each resource in Richtersveld Local Municipality to note any problems with the security procedures and plans that may result in a security. As a matter of good practise, the ICT Security department or committee should meet at least once a year to review the organisational security policies and all sub policies and plans supporting it. The ICT manager is normally the person to initiate a revision to the ICT Security policy as the IT manager will be the first to know of system and personnel changes in the ICT domain. Outside assistance in the form of it and other security specialists may be utilised as required, with the proviso that they sign a full confidentiality and non-disclosure agreement prior to the commencement of any work.

7.3 Documenting the ICT Data and Systems Security Policy Changes

All changes to the ICT data and Systems Security documents should be briefly described on the control sheets on the cover of each policy or plan. The revision or version number should be updated and the revised document must be signed off by those duly authorised to do so. The old version should be archived immediately to prevent it from being confused with the new revision. The new revision should replace the old version in the storage location for the Security documents. The updated document should be circulated to all involved in the provision of ICT security services and each role player should sign that they have read and understood the changes to the document.

8. CONCLUSION

The ICT data and Systems Security policy and plan are essential to the ability of the organisation to administer the informational recourses or assets and to ensure proper standards exist for controlling access to the data and systems both from external and internal sources. A holistic view of data, information and systems security management should be taken when compiling Security policies and plans.



Approved 24/08/2016