EDEN

DISTRICT MUNICIPALITY
UMASIPALA WESITHILI
DISTRIKSMUNISIPALITEIT

ICT USER ACCESS MANAGEMENT POLICY

Council Approved: 05/12/2017

Council Resolution Nr: C.5

TABLE OF CONTENTS

Glossary of Abbreviations

Abbreviation	Definition
BYOD	Bring Your Own Device
COBIT	Control Objectives for Information and Related Technology
HR	Human Resources
ICT	Information and Communication Technology
ID	Identifier
ISO	International Organization for Standardisation
ODBC	Open Database Connectivity
PIN	Personal Identification Number
RAS	Remote Access Service
VPN	Virtual Private Network

Glossary of Terminologies

Terminology	Definition
Administrative rights	Access rights that allow a user to perform high level/administrative tasks on a device/application such as adding users, deleting log files, deleting users.
Bring Your Own Device	The practice of allowing employees to use their own devices, such as cell phones, tablets, laptops, or other devices for work purposes.
Business case	A formal requirement in order for a specific business function to perform its required task.
Clear text	Clear text refers to a message that has not been encrypted in anyway and can be intercepted and read by anyone.
COBIT	A best practice framework created by ISACA for Information Technology Management and IT Governance.
Dormant account	A user account that has not been accessed or used for 60 days or more.
Line manager	Each department (HR, Finance, ICT, etc.) should have a manager employed to perform managerial tasks.
Personal Identification Number	A number allocated to an individual and used to validate electronic transactions.

Terminology	Definition
Principle of least privilege	A user or a program must be able to access only the information and resources that are necessary for its legitimate purpose.
Remote Access Service	A service which allows for a user to connect to a remote machine from any network point, as long as the targeted device resides on the network.
Segregation of duties	The principle of dividing a task up based on varying levels of authority in order to prevent fraud and error by requiring more than one person to complete a task.
VPN	A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organisation's network.
Wi-Fi	Wi-Fi is a wireless networking technology that allows computers and other devices to communicate over a wireless signal.

1. INTRODUCTION

Information security is becoming increasingly important to the Municipality, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that ICT systems, data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

2. LEGISLATIVE FRAMEWORK

The policy was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.

The following legislation, amongst others, were considered in the drafting of this policy:

- Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
- Copyright Act, Act No. 98 of 1978;
- Electronic Communications and Transactions Act, Act No. 25 of 2002;
- Minimum Information Security Standards, as approved by Cabinet in 1996;
- Municipal Finance Management Act, Act No. 56 of 2003;
- Municipal Structures Act, Act No. 117 of 1998;
- Municipal Systems Act, Act No. 32, of 2000;
- National Archives and Record Service of South Africa Act, Act No. 43 of 1996;
- Promotion of Access to Information Act, Act No. 2 of 2000;
- Protection of Personal Information Act, Act No. 4 of 2013;
- Regulation of Interception of Communications Act, Act No. 70 of 2002; and
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

The following internationally recognised ICT standards were leveraged in the development of this policy:

- Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014;
- Control Objectives for Information Technology (COBIT) 5, 2012;
- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls; and
- King Code of Governance Principles, 2009.

3. OBJECTIVE OF THE POLICY

The objective of the policy is to define the user access management control measures for the Municipality's ICT systems, information and infrastructure where it would apply to both the Municipal users and Service Providers. This policy seeks to further ensure that it protects the privacy, security and confidentiality of the Municipality's information.

The main objective of this policy is to provide the Municipality with best practice User Access Management controls and procedures to assist the Municipality in securing their user access management procedure.

4. AIM OF THE POLICY

The aim of this policy is to ensure that the Municipality conforms to standard user access management controls in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and that risks associated to the management of user access are mitigated. This policy supports the Municipality's Corporate Governance of ICT Policy as approved by Council.

5. SCOPE

The ICT User Access Management Policy has been developed to guide and assist municipalities to be aligned with internationally recognised best practice User Access Management controls and procedures. This policy further recognizes that municipalities are diverse and therefore adopts the approach of establishing principles and practices to support and sustain the effective control of user access management in the Municipality.

The policy applies to everyone in the municipality, including its service providers/vendors. This policy is regarded as being crucial to the operation and security of ICT systems of the Municipality. Municipalities must develop their own User Access Management controls and procedures by adopting the principles and practices put forward in this policy.

The policy covers the following elements of user access management:

- New user registration;
- Terminated user removal;
- User permission/role change request;
- User access rights assignment for networks, operating systems, databases and applications;
- Reviewing user access permissions;
- User and administrator activity monitoring; and
- Resetting of passwords

Aspects relating to ICT security and operating system security controls are contained in the ICT Security Controls and ICT Operating System Security Controls policies.

6. BREACH OF POLICY

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the Municipality and evaluated on its level of severity. Appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy. Actions include, but are not limited to:

- Revocation of access to Municipal systems and ICT services;
- Disciplinary action in accordance with the Municipal policy;
- Civil or criminal penalties e.g. violations of the Copyright Act, Act No. 98 of 1978; or
- Punitive recourse against the service provider/vendor as stated in the service provider/vendor's SLA with the Municipality.

7. ADMINISTRATION OF POLICY

The ICT Manager or delegated authority within the municipality is responsible for maintaining this policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and recommended changes must be approved by Council

8. DELEGATION OF RESPONSIBILITY

In accordance with the ICT Governance Policy, it is the responsibility of the Municipal Manager to determine the delegation of authority, personnel responsibilities and accountability to Management with regards to the Corporate Governance of ICT.

9. NEW USER REGISTRATION

9.1 A formalised user registration process must be implemented and followed in order to assign access rights.

9.2 All user access requests must be formally documented, along with the access requirements, and approved by authorised personal by making use of the electronic process on the Collaborator system.

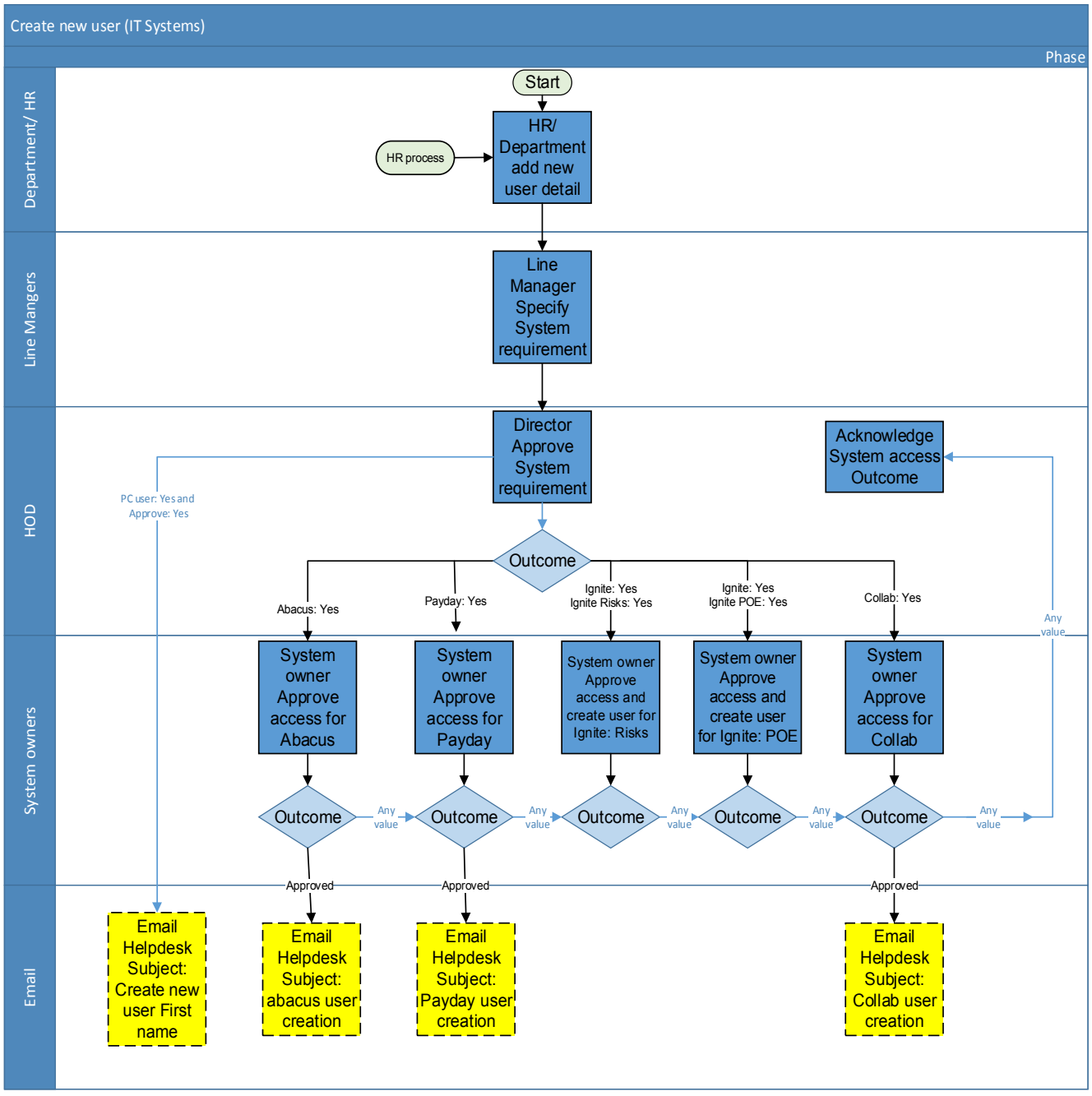
9.3 User access requests must be originated from HR on registration of a new employee. The electronic form must be sent to the line manager for access requirements to be requested. Once the requirements have been requested and approved by the departmental manager, the electronic form must be sent to the system owner for approval where after the electronic request will be sent to the ICT department for the activation of the employee based on the specified requirements on the specific systems.

9.4 User access must only be granted once approval has been obtained.

9.5 All users must be assigned unique user IDs in order to ensure accountability for actions performed.

9.6 The diagram below depicts the formal new user registration process to be followed.

Figure 1: New user registration process



10. TERMINATED USER REMOVAL

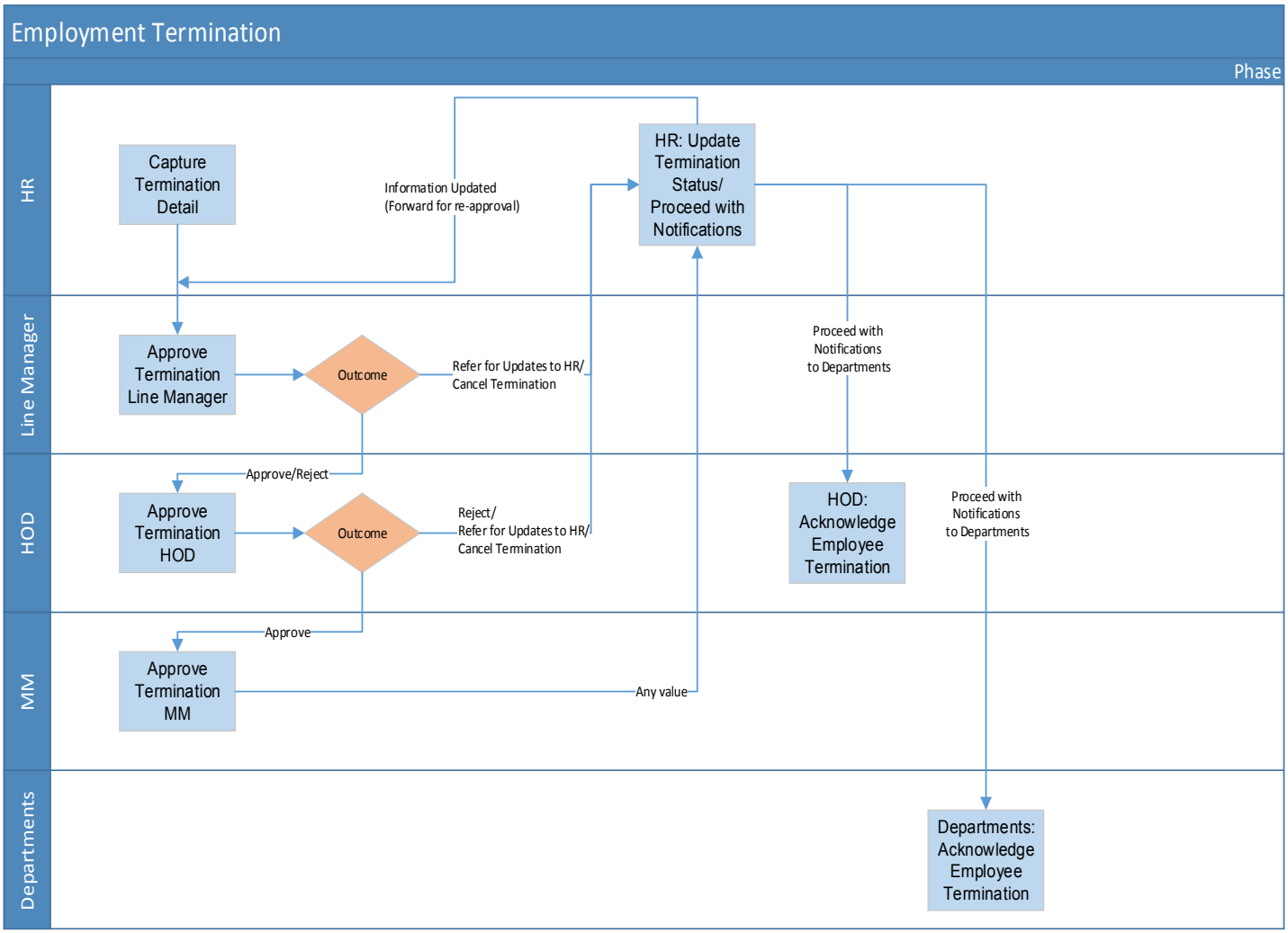
10.1 A formalised user termination process must be implemented and followed in order to revoke access rights.

10.2 All user termination requests must be formally documented and approved by duly authorised personnel by making use of the electronic process on Collaborator. Access must be disabled immediately, with Active Directory accounts being removed after 30 days. System user access will be treated in accordance with supplier system best practices.

10.3 Terminated user requests must be originated from HR on the termination of an employee. Once access revocation has been approved, the electronic form must be sent to the ICT department for deactivation of employee based on specified requirements.

10.4 The diagram below depicts the formal user termination process to be followed.

Figure 2: User termination process



11. USER PERMISSION/ROLE CHANGE REQUEST

11.1 A formalised user access management process must be implemented and followed in order to adjust user access rights.

11.2 All user access change requests must be formally documented, along with their access requirements, and approved by duly authorised personnel.

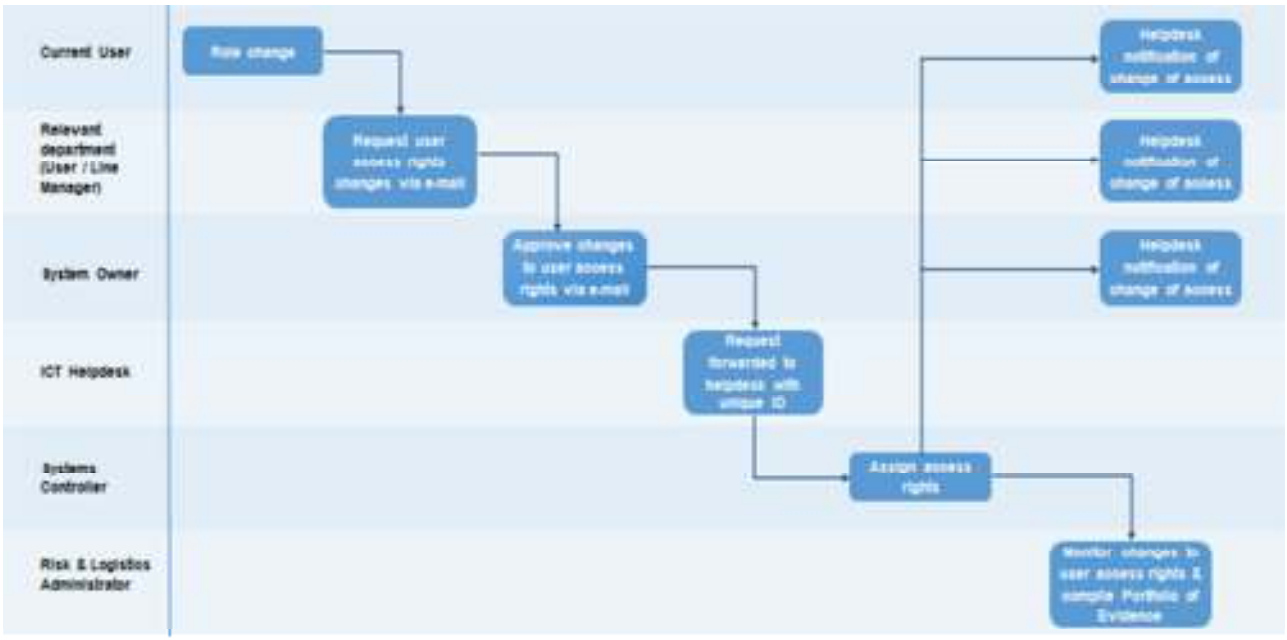
11.3 The change request must only be granted once approval has been obtained by the respective system owner.

11.4 The approved user access change request must be obtained from the system owner on change of an employee's role or permissions. The user / line manager in the relevant department must send the request via e-mail to the system owner for approval. Once the access requirements have been approved, the system owner must then send the approved e-mail request to the ICT helpdesk for adjustment of the employee's access rights based on specified requirements. The ICT helpdesk request for the changes to the employee's access rights will be kept for record keeping purposes.

11.5 User access rights that are no longer required must be removed immediately.

11.6 The diagram below depicts the formal user permission/role change request process to be followed.

Figure 3: User permission/role change request process



12. GENERAL USER ACCESS RIGHTS ASSIGNMENT

12.1 Access rights include, but are not limited to:

(a) General office applications (E-mail, Microsoft Office, SharePoint, etc.);

(b) Department specific applications and/or databases;

(c) Network Shares;

(d) Administrative tasks;

(e) RAS/VPN Access;

(f) Wi-Fi; and

(g) BYOD

12.2 Access must follow a “principle of least-privilege” approach, whereby all access is revoked by default and users are only allowed access based on their specific requirements.

12.3 The levels or degrees of access control to classified information must be restricted in terms of legislative prescripts.

13. NETWORK USER ACCESS RIGHTS ASSIGNMENT

13.1 Access to the Municipality’s network must only be allowed once a formal user registration process has been followed.

13.2 Access to Wi-Fi must only be provided to users who require access to the network throughout the Municipality, to fulfil their business function.

13.3 RAS/VPN access must only be granted to users who require the service to fulfil their business function.

13.4 VPN access must only be granted to employees and approved third party support services who:

(a) Work remotely (Not at the office);

(b) Work overtime, or not within regular office hours.

13.5 It is the responsibility of the ICT Steering Committee to ensure all users must be made aware of the security risks and obligations associated with RAS/VPN access.

13.6 RAS/VPN access must be monitored and audit logs reviewed on a daily basis.

13.7 All reviews must be formally documented. Documentation must be kept for record keeping purposes.

14. OPERATING SYSTEM ACCESS RIGHTS ASSIGNMENT

14.1 Each system administrator must be given their own accounts within the administrator group.

14.2 Where possible, the default administrator account must be renamed and a password must be randomly generated and sealed in an envelope and kept in a safe.

14.3 Where possible, the default guest account must be removed or renamed and disabled.

15. APPLICATION USER ACCESS RIGHTS ASSIGNMENT

15.1 Segregation of duties must be practiced, in such a way that application administrators cannot perform general user tasks on an application. This is to prevent any fraudulent activity from taking place.

15.2 Applications administrators must remain independent of the department utilising the application, with the exception of the ICT department.

16. DATABASE USER ACCESS RIGHTS ASSIGNMENT

16.1 The ICT Manager must limit full access to databases to ICT staff who need this access. Municipal employees who use applications may not have these rights to the application's databases.

16.2 The ICT Manager must ensure that Municipal employees who access databases directly (e.g. through ODBC) only have read access.

16.3 If a Municipal employee requires read and write access to a database to fulfil a business function, approval must be obtained from the ICT Manager. The request and approval must be kept for record keeping purposes.

16.4 The ICT Manager must review database rights and permissions on a quarterly basis (every 3 months). Excessive rights and permissions must be removed.

17. REVIEWING USER ACCESS AND PERMISSIONS

17.1 User access and user permissions must be reviewed and signed off on a monthly basis by the relevant System Owner.

17.2 On a monthly basis, HR must send a list of all user movement for that month to the ICT department. This list must be used to ensure that all users access have been modified accordingly. Any discrepancies must be addressed immediately.

17.3 On a monthly basis, the ICT Manager must review all users with administrative access to the environment and assess their rights for appropriateness. Should a user be found with excessive rights, a user access change request must be performed.

17.4 All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes.

18. USER AND ADMINISTRATOR ACTIVITY MONITORING

18.1 User and administrator activity must be monitored through audit and event logging.

18.2 Logs must be reviewed for suspicious and malicious activities by system administrators.

18.3 Dormant accounts should be disabled and a request to remove the access should be performed in line with section 11.User Permission/Role Change Request.

18.4 Any suspicious and malicious activities must be reported to the ICT Manager immediately.

19. RESETTING OF PASSWORDS

19.1 If a user suspects that his/her password has been compromised, they must reset their passwords immediately or a formal request must be sent to the Systems Controller.

19.2 The new temporary password must be communicated directly to the user, on validation of their identity

19.3 The user must be forced to change their temporary password on first log on.

19.4 All documentation must be kept for record keeping purposes.