ICT USER ACCESS MANAGEMENT POLICY

TABLE OF CONTENTS

1. INTRODUCTION....4
2. LEGISLATIVE FRAMEWORK....4
3. OBJECTIVE OF THE POLICY....5
4. AIM OF THE POLICY....5
5. SCOPE....5
6. BREACH OF POLICY....6
7. ADMINISTRATION OF POLICY....6
8. DELEGATION OF RESPONSIBILITY....6
9. NEW USER REGISTRATION....6
10. TERMINATED USER REMOVAL....7
11. USER PERMISSION/ROLE CHANGE REQUEST....8
12. GENERAL USER ACCESS RIGHTS ASSIGNMENT....9
13. NETWORK USER ACCESS RIGHTS ASSIGNMENT....9
14. OPERATING SYSTEM ACCESS RIGHTS ASSIGNMENT....10
15. APPLICATION USER ACCESS RIGHTS ASSIGNMENT....10
16. DATABASE USER ACCESS RIGHTS ASSIGNMENT....10
17. REVIEWING USER ACCESS AND PERMISSIONS....11
18. USER AND ADMINISTRATOR ACTIVITY MONITORING....11
19. ANNEXURE A: IMPLEMENTATION ROADMAP....12
20. ANNEXURE B: USER ACCESS MANAGEMENT FORM EXAMPLE 13
21. ANNEXURE C: OPERATING SYSTEM SECURITY SETTINGS....14
22. ANNEXURE D: AUDIT/EVENT LOG REVIEW TEMPLATE....16
23. ANNEXURE E: REFERENCES....17

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.

Terminology	Definition
Personal Identification Number	A number allocated to an individual and used to validate electronic transactions.
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.

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; and
- User and administrator activity monitoring.

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 user access request form. The template for this type of request can be found attached to this policy in Annexure B.

9.3 User access requests must be obtained from HR on registration of a new employee. The form must be sent to the service provider/line manager for access requirements to be requested. Once the requirements have been requested and signed off by the departmental manager, the form must be sent to the ICT department for approval following which the activation of the employee based on the specified requirements will be completed. The form must then be sent back to HR for record keeping purposes. Records of user access granted must be stored for a minimum of 10 years.

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. Should shared accounts be required to fulfil a business function, this account must be approved and documented by the Risk Management Committee.

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

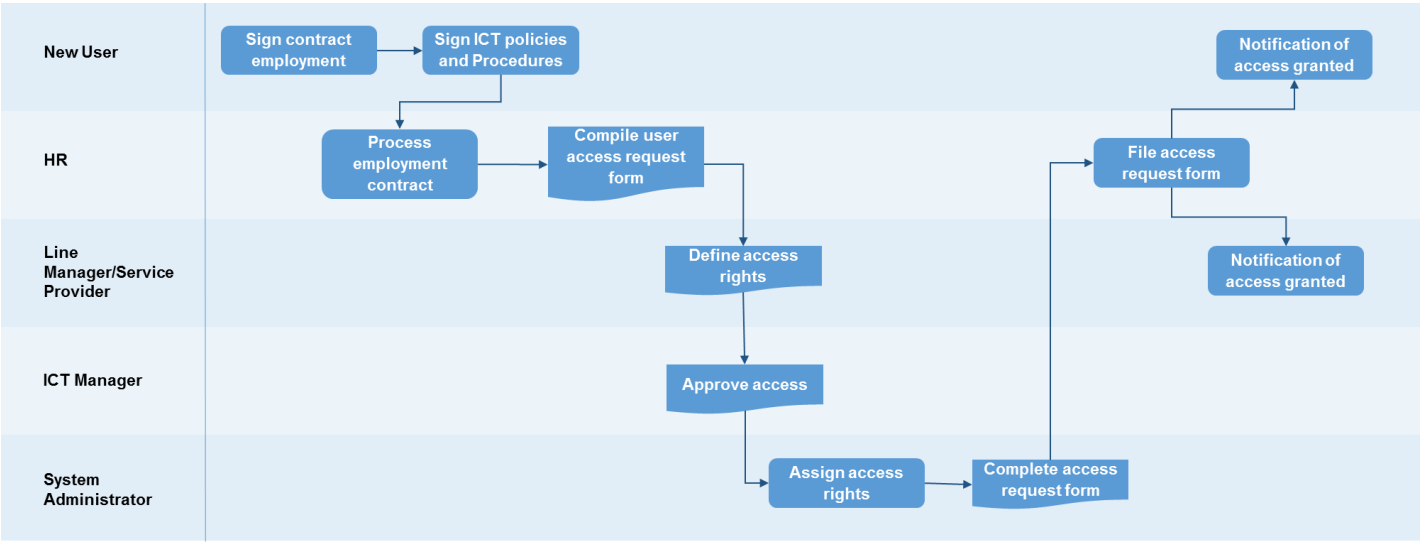

Figure 1: New user registration process

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. Access must be disabled immediately, with accounts being removed after 6 months once authorisation has been obtained by line manager.

10.3 Terminated user requests must be obtained from HR on the termination of an employee. The template for this type of request can be found attached to this policy in Annexure B. The form must be sent to the service provider/line manager for access revocation to be signed off. Once access revocation has been signed off, the form must be sent to the ICT department for approval and deactivation of employee based on specified requirements. The form must then be sent back to HR for record keeping purposes. Records of user access removal must be stored for a minimum of 10 years.

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

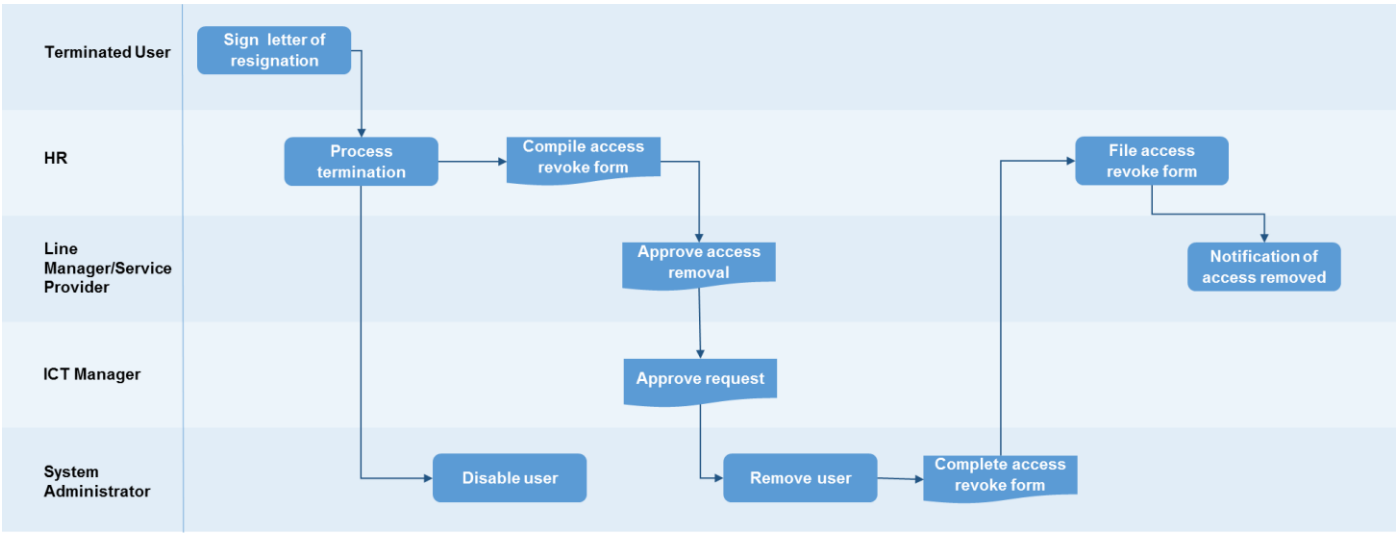

Figure 2: User termination process

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 Access must only be granted once approval has been obtained by the respective line manager.

11.4 User access change requests must be obtained from HR on change of an employee's role or permissions. The template for this type of request can be found attached to this policy in Annexure B. The form must be sent to the service provider/line manager for access requirements to be signed off. Once the access requirements have been signed off, the form must then be sent to the ICT department for approval and adjustment of employee's access rights based on specified requirements. The form must then be sent back to HR for record keeping purposes. Records of user access granted and removed must be stored for a minimum of 10 years.

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.

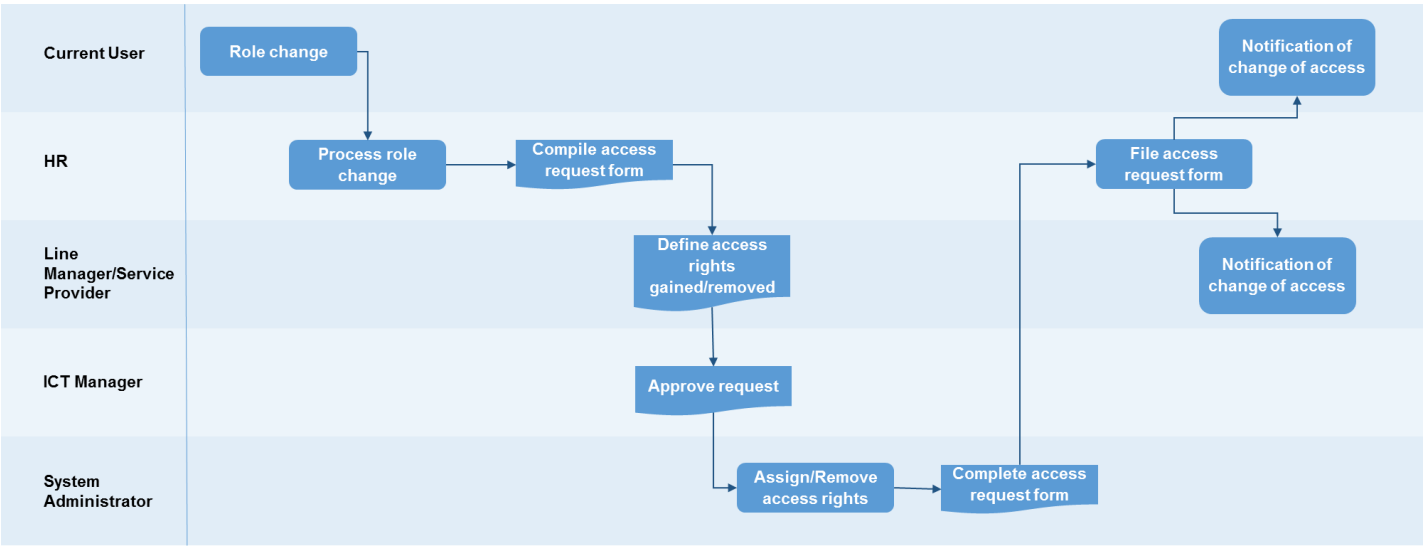

Figure 3: User permission/role change request process

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.

12.4 Access rights must be assigned to a group/role. A user must then be assigned to that group. Access rights must not be assigned to individual users.

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 Best practice states that RAS access must only be granted to employees who require remote access to a system in order to administer the environment.

13.5 Best practice states that VPN access must only be granted to employees who:

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

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

13.6 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.

13.7 RAS/VPN access must be monitored and audit logs reviewed every quarter (3 months) by system administrators.

13.8 All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes. Records of RAS/VPN access reviews must be stored for a minimum of 10 years.

13.9 The ICT Manager must approve all hardware and software, owned by Municipal employees and service providers/vendors, if it is to be used for official purposes (BYOD).

13.10 The ICT team must ensure that all mobile devices must be protected with a PIN.

14. OPERATING SYSTEM ACCESS RIGHTS ASSIGNMENT

14.1 Each system administrator must be given their own accounts within the administrator group. Should shared accounts be required to fulfil a business function, then this account must be approved and documented by the Risk Management Committee.

14.2 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 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 (e.g. sysadmin server role, db_owner database role, sa built-in login etc.) 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 The ICT Steering Committee must approve all instances where Municipal employees have edit or execute access to databases.

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 every quarter (3 months) by system administrators.

17.2 On a monthly basis, HR must send a list of all terminated employees for that month to the ICT department. This list must be used to ensure that all terminated users have had their access revoked. Should one or more terminated users still have access to the environment, and investigation into the finding must be conducted.

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. Records of user access review must be stored for a minimum of 10 years.

18. USER AND ADMINISTRATOR ACTIVITY MONITORING

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

18.2 Once a month, system administrators and application owners must review audit and event logs for suspicious and malicious activities. A template for the reviewing of audit logs can be found in Appendix D of this Policy.

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 All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes. Records of user activity monitoring must be stored for a minimum of 10 years.

19. ANNEXURE A: IMPLEMENTATION ROADMAP

No	Action	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	Identify all current access management procedures																		
2	Assess appropriateness of current procedures																		
3	Adjust and document changes to procedures																		
4	Educate employees of changes in procedures																		
5	Implement newly defined or adjusted procedures																		

20. ANNEXURE B: USER ACCESS MANAGEMENT FORM EXAMPLE

Name: _____ Date: ___/____/____

Designation: _____

Requested by: _____

New	Termination	Change

General PC Use

E-mail	☐
VPN	☐
RAS	☐
Finance Application	☐
HR Application	☐
Comms Application	☐
_____ (other)	☐

Administrative rights:

The following section must be completed if access is being requested for a service provider/vendor:

Period of access: _____

Reason for request:

	HR Manager	Line Manager	ICT Manager	System Administrator
Signature:	_____	_____	_____	_____
Date:	___/____/____	___/____/____	___/____/____	_____/_____/_____

21. ANNEXURE C: OPERATING SYSTEM SECURITY SETTINGS

Security Configuration	Setting
Password Policy - General User Accounts	
Minimum password length	8 characters
Maximum password age	30 days
Password history	6 passwords remembered
Password complexity	Enabled
Password Policy - Administrative/Super User Accounts	
Minimum password length	12 characters
Maximum password age	30 days
Password history	12 passwords remembered
Password complexity	Enabled
Account Lockout Policy - General User Accounts	
Account lockout duration	60 minutes
Account lockout threshold	3 attempts
Account lockout counter threshold	30 minutes
Account Lockout Policy - Administrative/Super User Accounts	
Account lockout duration	60 minutes
Account lockout threshold	3 attempts
Account lockout counter threshold	60 minutes
Audit Policy	
Account logon events	Failure
Account management	Success, Failure
Logon events	Failure
Policy change	Success, Failure
Privilege use	Success, Failure
System events	Failure
Event Logs	

Application Log: Maximum log size (KB)	32 768
Application Log: When maximum event log is reached	Overwrite events as needed
Security Log: Maximum log size (KB)	81 920
Security Log: When maximum event log is reached	Overwrite events as needed
System Log: Maximum log size (KB)	32 768
System Log: When maximum event log is reached	Overwrite events as needed
Additional Settings	
Screen saver	Enable
Screen saver: Wait	10 minutes
On resume, display logon screen	Enabled
Accounts: Rename administrator account	Not Administrator or admin
Accounts: Rename guest account	Not Guest
Accounts: Guest account status	Disabled
Windows Firewall: Firewall state (Domain)	Enabled (1)
Windows Firewall: Firewall state (Private)	Enabled (1)
Windows Firewall: Firewall state (Public)	Enabled (1)

22. ANNEXURE D: AUDIT/EVENT LOG REVIEW TEMPLATE

Reviewer:			
Month/Year	____/20___		
System/Application	**Day of review**	**Signature**	**Notes**
Active Directory			
Exchange			
Member Server 1			
Member Server 2			
Member Server 3			
Member Server 4			
Finance Application			
HR Application			
Comms Application			
Document Management System			

ICT Manager

Signature: _____

Date: ___/____/20__

23. ANNEXURE E: REFERENCES

BS ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls. (2013). Geneva: BSI Standards Limited.

Control Objectives for Information Technology (COBIT) 5. (2012). Illinois: ISACA.

Minumum Information Security Standards. (1996, December 4). Cabinet.