



Policy: Logical Access Management Policy

**Reference Number:
8/7/2/1/6/9/Logical Access Management**

**Version: 3.0
Date:15/12/2021**

Contents

1	Document Version Control	3
2	Policy Overview	5
3	Applicability	5
3.1	Intended Audience	5
4	Responsible Office	5
5	Policy Statement	5
6	Related Policy Detail	5
6.1	User Enrolment, Provisioning and De-provisioning	5
6.2	Management of Privileged Access Rights	6
6.3	Role-Based Access	7
6.4	System Accounts	8
6.5	Remote Access	8
6.6	Authentication Management	9
6.7	Operational Technology Systems	10
6.8	Access Review	11
6.9	Audit Logging	12
6.10	Cloud and Federated Access	12
7	Enforcement	13
8	Exception Handling	13
9	Glossary	13
10	References	14

1 Document Version Control

Changes:

DATE	AUTHOR	VERSION NUMBER	REVISION DETAILS
11/10/2018	Louis van Dyk	0.1	First draft
16/11/2018	Deidre Marais	0.5	User access management – 4.1.2 was changed to supervisor. Retention period was removed. Related standards and procedures were added to policy sections.
03/04/2019	Louis van Dyk	1.1	Change applicability section 3 to include external service providers and consultants
03/06/2019	Louis van Dyk	1.2	Add responsible office section 4
16/08/2019	Louis Van Dyk	1.4	Add statement that ADM not allowed to have internet access
21/08/2019	Louis Van Dyk	2.0	Change version for sign off
15/02/2021	Michael Stadler	2.1	Update policy details
10/09/2021	Louis van Dyk	2.2	Update and change name of the password management section to authentication management and added subsections
16/02/2022	Louis van Dyk	3.0	Added intended audience section & Change version for sign off

Reviews:

DATE	Name	VERSION NUMBER	REVIEW DETAILS
30/08/2019	Michael Stadler	2.0	Reviewed

28/03/2022	Deidre Marais	3.0	Reviewed
------------	---------------	-----	----------

Sign offs:

DATE	Name	DESIGNATION	SIGNATURE
	Andrew Coleman	Director: DSCS	
	Augi de Freitas	CD: GMS	
	Hilton Arendse	DDG: Be-I	

2 Policy Overview

The purpose of this policy is to define logical access control measures for all the WCG IT systems and applications in order to ensure that the right access is granted to users based on their job function, business requirements and security objectives. The policy covers the digital identity lifecycle across the joiner, mover and leaver stages, along with ensuring the appropriateness of access to IT resources.

3 Applicability

This policy applies to all individuals that provide and manage IT resources and services under the custodianship of the WCG or sourced from 3rd party services. This includes all WCG employees, third parties, temporary staff, contractors, external service providers and consultants.

3.1 Intended Audience

This policy is intended for review by all **IT operational Teams**.

The following are the key expectations of users:

- To familiarise themselves with this policy and all other related policies, standards and guidelines (where applicable).
- Take responsibility for all activity related to IT accounts they have been allocated and any information they access.
- Report any accidental breach of policy or suspected misuse of WCG IT resources or fraudulent activity to their line manager.

4 Responsible Office

The WCG Be-I information Security sub-directorate owns and maintains this policy, they can be contacted with the following email address ictpolicy@westerncape.gov.za

5 Policy Statement

The policy addresses the lifecycle of IT users from enrolment of user accounts to the allocation of access and ongoing access management. It governs access to information, technology infrastructure and applications whether hosted on-premises or in cloud-based services. The policy does not address access to facilities and physical environments. While this policy addresses the specific requirements of this security area, there are other related information security policies, IT policies and standards that need to be considered.

The coverage and mandate of this policy will be limited to the scope of the Be-I managed IT environment within the WCG. These IT and information security services are focused on the Corporate Virtual Private Network (VPN) used by multiple provincial departments in the Western Cape. Other IT areas may make use of this policy, but enforcement is limited by the scope of IT governance and security controls.

6 Related Policy Detail

Policy Section	6.1 User Enrolment, Provisioning and De-provisioning
Rationale	Due to the common challenges of careless allocation of IT access and fraud, it is necessary to validate a person's identity before granting access to the trusted network and resources. It is also necessary to ensure that the right access is granted to the right user, with the right authorisation, in the right way and for the right time. This section covers the process of coordinating the creation of user accounts, granting

	access with authorisations supported by rules and roles and the timely de-provisioning of access when no longer required.
Policy Statements	<p>6.1.1 A formalised user registration process must be implemented and followed in order to validate the identity of an IT user and ensure that they have been assigned the correct HR organisational role and job function.</p> <p>6.1.2 In the case of third-party contractors and vendors, the process (6.1.1) must be validated by the supervisor with a level 13 or higher.</p> <p>6.1.3 Every IT account must be assigned to an individual who is responsible for the login credentials. No account shall be assigned to more than one individual.</p> <p>6.1.4 All user and privilege accounts must be created using a defined naming standard.</p> <p>6.1.5 All-access must be authorised and approved by senior management through a governed and auditable process.</p> <p>6.1.6 A workflow-driven process must be in place to ensure the level of access granted is appropriate and consistent with other requirements such as segregation of duties.</p> <p>6.1.7 A process must be in place for modifying access rights of users who have changed roles/jobs and to immediately revoke access rights of users who have left or have changed roles.</p> <p>6.1.8 A central record must be maintained for granting and revoking access for all systems and should provide an adequate audit trail to identify when the user's access was authorised or revoked.</p> <p>6.1.9 The use of Guest accounts or other unsecured accounts is prohibited on the WCG Trusted Network. Default Guest accounts on operating systems and applications must be disabled.</p> <p>6.1.10 Admin Accounts for support staff must be deleted when they do not require access anymore.</p> <p>6.1.11 Admin accounts must not have a mailbox linked to the administrator account.</p> <p>6.1.12 Should a user account be compromised the account must be deleted and recreated.</p>
Related Policies and Procedures	Network Security Policy

Policy Section	6.2 Management of Privileged Access Rights
Rationale	Privileged accounts have elevated access rights to applications and infrastructure and are therefore the most critical and powerful accounts on IT systems. These accounts are typically targeted by cyber-attacks to gain possession of resources and to access confidential data. The inadvertent misuse of these accounts could also cause significant damage to systems and business process availability.

Policy Statements	6.2.1	An authorisation process must be followed before granting privileged access to a user.
	6.2.2	The assignment of privileges must be limited to a minimum /as-needed basis and linked to a specific job function or service provider role.
	6.2.3	Once privileges assigned to a user or system are no longer required, privileged rights must be revoked, and records must reflect such change.
	6.2.4	Accounts with privileged rights must not be used for daily activities and must not have access to the internet. The user must use their regular accounts for these activities and only use privilege accounts for authorised operational or change management tasks.
	6.2.5	Wherever possible multi-factor authentication must be used for all privilege access.
	6.2.6	Privileged access to systems (such as administrative or supervisor accounts) must be reviewed on a monthly basis by the designated Line Manager.
	6.2.7	Privilege groups must be quarterly reviewed for the appropriateness of permissions and membership.
	6.2.8	Audit logging must be enabled to monitor all privileged account usage and protection mechanisms must be implemented to prevent audit log tampering.
	6.2.9	The activity of privileged users must be reviewed by a respective system owner on a quarterly basis.
Related Policies and Procedures	Third-Party Security Policy	

Policy Section

6.3 Role-Based Access

Rationale	WCG is a large corporate IT environment with several applications and systems. This results in a significant number of users and permissions that need to be managed, giving rise to increased security risk. Role-based access control (RBAC) restricts access based on a person's role or function within WCG and has become one of the main methods for advanced access control. The RBAC roles provide an aggregated set of permissions related to the various applications, systems and physical locations that a person requires to perform their job.	
Policy Statements	6.3.1	Functional access roles must be defined based on the user's organisational role as defined by Human Resources (HR).
	6.3.2	In the case of contractors, access roles must be defined by the respective Line Manager.
	6.3.3	Access rights must be granted to only provide users with the minimum access needed to perform their authorised job functions. The principle of least privilege must be applied.
	6.3.4	The allocation of users to roles must follow the standard provisioning process and be authorised by the respective Line Manager and System Owner (See section 6.1.1)

Related Policies and Procedures

- 6.3.5 User access across roles must be reviewed by the respective system owner for compliance with Segregation of Duty (SoD) requirements and prevent toxic access combinations.
- 6.3.6 Functional and system roles must be reviewed on a quarterly basis and attested by the respective System Owners, Line Management and HR.
- 6.3.7 Changes to role permissions must be logged for auditing purposes.

Policy Section

6.4 System Accounts

Rationale

A system account is created for the purposes of authenticating transactions at an operating system or application level. These accounts are a common target of cyber-attacks because they typically carry a higher level of account privileges and are often not monitored sufficiently. Specific protection is therefore required for these account types.

Policy Statements

- 6.4.1 Access rights must be granted to only provide the minimum access needed based on the functional requirement. The principle of least privilege must be applied.
- 6.4.2 All system accounts must be created using a defined naming standard.
- 6.4.3 The password management and complexity requirements for privileged accounts must be applied to system accounts.
- 6.4.4 The use of system accounts must be monitored for security incident use cases with events triggering the respective alerting and response processes.
- 6.4.5 All system accounts must be assigned to a specific individual.

Related Policies and Procedures

Policy Section

6.5 Remote Access

Rationale

Remote access provides employees and service providers with the flexibility to perform a wide range of IT tasks from anywhere. In some cases, employees will need to work remotely, and this could lead to high-security risks such as if one of the devices goes missing, lost or stolen or falls into the wrong hands. The WCG needs to ensure that adequate access control measures are in place to protect information and IT resources from loss, unauthorised use or viewing when systems are used to connect from remote access points.

Policy Statements

- 6.5.1 An authorisation process needs to be followed before granting a user or vendor remote access to the network.
- 6.5.2 In the case of third-party contractors and vendors, the process (4.1.1) must be validated by the supervisor with a level 13 or higher.

6.5.3	Remote access must be strictly controlled with an authenticated and encrypted technology such as Virtual Private Network (VPN) software.
6.5.4	Multi-factor authentication must be used for all remote access connectivity.
6.5.5	All Users must use generated one-time pins from approved fobs or smartphone authenticator apps as second factor in addition to their WCG credentials to authenticate to the WCG systems and applications that require multi-factor authentication.
6.5.6	While remotely connecting to the corporate network, authorised users must ensure the remote host is not connected to any other network at the same time i.e., the bridging of networks is not permitted.
6.5.7	All hosts, personal devices, that are connected to internal network via remote access technologies must use the most up to date antivirus software.
6.5.8	Personal equipment used to connect to WCG's networks must meet WCG's minimum security requirements for remote access (refer to WCG ICT Standards).
6.5.9	The use of unsecured remote access tools must be blocked by the WCG network perimeter controls such as firewalls or intrusion prevention system (IPS).
Related Policies and Procedures	Network Security Policy
	Mobile Device Management Policy
	Third Party Security Policy

Policy Section **6.6 Authentication Management**

Rationale	Authentication mechanisms such as passwords are the primary means of protecting access to computer systems and data. It is essential that the methods and configurations used for authentication are well defined and used to ensure maximum protection of the underlying systems to which it provides access.
Policy Statements	<p>General</p> <p>6.6.1 All users are responsible for any activity that occurs as a result of the use of authentication methods issued by them.</p> <p>6.6.2 All users are responsible for reporting any suspicious use of assigned authentication mechanisms. Anyone that reasonably believes his or her password to be known by anyone else must change it immediately.</p> <p>6.6.3 Lost or stolen WCG owned authentication devices must be reported immediately using the Incident template form.</p> <p>Password Management</p> <p>6.6.4 A procedure for self-service or service desk assisted issuing of new or changing passwords must be in place. This procedure must ensure that users are appropriately identified before these changes are made.</p> <p>6.6.5 In order to prevent the unauthorised access of WCG computer systems, a formalised Password Management Standard must be in</p>

Related Policies and Procedures

	place regarding password complexity (i.e. length and composition, frequency of change and re-use of passwords).
6.6.6	Users must keep their password secret and must not make their password known to anyone else, including management, supervisors, personal assistants, human resources and system administrators.
6.6.7	WCG must implement system password policies that automatically force the user to change their password at least every 72 days.
6.6.8	Passwords must not be written down or stored in an unsecured manner.
Password-less Authentication	
6.6.9	The WCG users may only use authorised devices/methods for password-less login.
6.6.10	If a user's mobile device is used as part of their password-less access to their computer or other WCG systems, a unique PIN must be set on their mobile device and changed periodically.
6.6.11	The use of approved mechanisms such as accompanying mobile device, fingerprint or facial recognition may be used to log onto the WCG computers or systems.
Multi-factor Authentication	
6.6.12	The WCG users must use their respective individually assigned password or password-less authentication credentials (e.g., username and password) and wherever possible the WCG MFA (multi-factor authentication) mechanism to validate their identity.
6.6.13	Users will be required to enrol a device/method to serve as the second authentication mechanism as part of multi-factor authentication. This second method can be an automated phone call from Microsoft, a SMS sent with a one-time pin or an approve/deny message sent to an MS Authenticator App on your mobile phone.
Password Standard	
Incident template form in the Management of physical security incidents documents SOP 151117.	
Security and OHS SOP	

Policy Section 6.7 Operational Technology Systems

Rationale

Operational Technology (OT) systems bring performance, operational and management challenges to the network infrastructure along with increased security risks from all endpoints. To address these issues, the WCG needs to adapt traditional network designs to provide new levels of network intelligence, automation and security. If security is not properly addressed in the early stages of implementing OT systems, hackers can target weak points and exploit the data of your entire infrastructure. OT systems are not traditionally built with good security functionality (such as authentication). In

	some cases, compensating controls may need to be added to protect these systems.
Policy Statements	<p>6.7.1 The OT system must be analysed for its capability to meet the access management requirements (e.g., authentication, authorisation, auditing, etc.). Where systems do not cater to the required functionality, compensating access controls such as network isolation, must be implemented.</p> <p>6.7.2 To prevent physical unauthorised access to the OT devices, devices must be safely stored/placed where they cannot be tampered with.</p> <p>6.7.3 Access to OT systems (such as administrative or supervisor accounts) must be reviewed monthly by the designated Line Manager.</p> <p>6.7.4 Monitoring and alerting tools must be used to continuously monitor the security health of the OT infrastructure.</p> <p>6.7.5 OT device access to the Internet must be limited and restricted.</p>
Related Policies and Procedures	

Policy Section 6.8 Access Review	
Rationale	The WCG must have the right permissions and settings so that users can access the files they need. The WCG wants to be sure a user who does not need access to an “administrator group” is not a member accidentally of that group. Access reviews will help to identify accounts that have been assigned excessive privileges, accounts with access that have not been updated to reflect job position changes, failing to perform user access rights will put the WCG in a higher risk as some users will have access to resources which they do not have permission to.
Policy Statements	<p>6.8.1 A quarterly review process must validate that all IT users and related accounts are valid based on current employment or third-party contracts.</p> <p>6.8.2 A quarterly review process must be in place to review all privileged access and critical system user access to applications and infrastructure. This will be done in cooperation with the application/system owner and line managers and must be designed to positively re-confirm all users and their access.</p> <p>6.8.3 Access attestation reports must be submitted to the line manager/ system owner on a quarterly basis for review and approval.</p> <p>6.8.4 In systems that provide the ability to monitor inactivity, the following must be applied:</p> <ul style="list-style-type: none"> ○ workstation accounts which remain unused for 31 days should be deleted ○ user accounts which remain unused for 60 days should be disabled.

Related Policies and Procedures	<ul style="list-style-type: none"> Any account that has not been used for this set period of time should be considered inactive.
	6.8.5 Procedures must be in place to quarterly review system accounts, including privileges assigned and the periodic update of passwords.

Policy Section 6.9 Audit Logging

Rationale	While access restrictions are preventative controls, it is necessary to constantly monitor user activity for both malicious and inadvertent access issues. Effective event logging of all systems and security monitoring work together to ensure users are only performing the activities they are authorised to perform. They also play a key role in identifying and responding to cyber-attacks.
Policy Statements	<p>6.9.1 User log-on and log-off access to infrastructure, applications and file systems, as well as significant system events must be logged.</p> <p>6.9.2 Use cases must be defined to identify relevant security events on applications, operating systems, databases and infrastructure. Logs must be enabled to record activity based on these use cases.</p> <p>6.9.3 System administrators must not have “write” or “delete” access to audit trails.</p> <p>6.9.4 To protect the integrity of logs they must be recorded both locally and to a remote logging server such as a SIEM.</p> <p>6.9.5 Audit logs must be retained for a minimum of 30 days so that investigations can be pursued.</p> <p>6.9.6 Full audit logging must be enabled for system accounts.</p>
Related Policies and Procedures	

Policy Section 6.10 Cloud and Federated Access

Rationale	Although there are many benefits to adopting Cloud Computing, there are also some significant barriers. Cloud access management and federated access are particular challenges that must be taken into account as part of the strategy. Multiple services are most likely to be subscribed by the WCG, resulting in multiple login requirements from users.
Policy Statements	<p>6.10.1 The WCG network logon credential must not be exposed to the public Internet without the requirement for a second-factor credential.</p> <p>6.10.2 All administrative access to cloud services must only be permitted to a trusted WCG device or else via a jump-host server.</p>

Related Policies and Procedures

6.10.3	Passing and storing of all credentials on cloud-based services must be encrypted and highly secured.
6.10.4	The architecture of all cloud federation services entailing user identities and access credentials must be risk assessed and securely designed.
6.10.5	The WCG must have robust identity management and authentication processes, which include multi-factor authentication, single sign-on and/or other technologies such as cloud access brokers (CASB).
6.10.6	User credentials must conform to the WCG password standard.

7 Enforcement

The BE-I Security sub-directorate will verify compliance with this policy through various methods, including but not limited to, security reporting tools, internal and external audits, and management feedback to the policy owner.

Violation of this policy (e.g., wilful or negligent exposure of confidential information) may result in disciplinary action which may include termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with the WCG. Additionally, employees, contractors and agents who violate this policy may be subject to civil and criminal prosecution.

8 Exception Handling

Exceptions to the guiding principles in this policy must be documented and formally approved by the relevant Accounting Officer of the department. Policy exceptions must describe:

- The nature of the exception
- Why the policy exception is required
- Risks created by the policy exception
- Evidence of approval by the Accounting Officer and Be-I Security Officer.

The IT and Enterprise Risk Management team must be notified of any exceptions having a risk impact.

9 Glossary

Term	Definition
CASB	Cloud access security broker work by ensuring that network traffic between on-premises devices and the cloud provider complies with the WCG security policies.
Administrative Access	Level of access above that of a normal user
SIEM	Security information and event management
Access attestation	Attestation is the process performed by one or more designated attestors to confirm a user entitlement as it exists
OT devices	Operational Technology Devices

Two-factor authentication	Multi-factor authentication is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism
Privilege account	A privileged account is a user account that has more privileges than ordinary users.
Remote access	Remote access is the ability to access a computer or a network remotely through a network connection
System Accounts	A system account is a user account that is created by an operating system during installation and that is used for operating system defined purposes

10 References

- National Institute of Standards and Technology (NIST) Cybersecurity Framework, Version 1.1 (2018)
- National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4
- NIST Special Publication 800-63-3 Digital Identity Guidelines.
- Center for Internet Security, CIS Controls
- COBIT 5
- ISO/IEC 27002:2013 Information technology, Security techniques – Code of practice for information security management
- CIS Critical Security Controls Version 7