DIGICALL

A9 - ACCOUNT AND IDENTITY MANAGEMENT POLICY V1.3

DOCUMENT CLASSIFICATION	Internal Use Only
VERSION	1.3
DATED	01 September 2024
DOCUMENT AUTHOR	Ameet Ranchod
DOCUMENT OWNER	Johan Kriel

Approval

NAME	POSISTION	SIGNATURE	DATE
Donald Fraser	IT Security & Compliance Manager		03/10/2024
Ameet Ranchod	IT Infrastructure Manager		04/10/2024
Johan Kriel	Group CIO		09/10/2024

This policy supersedes and replaces all previous versions of this policy.

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0.1	17.02.2021	Ameet Ranchod	Document Creation
0.9	17.02.2021	Ameet Ranchod	Final Draft
1.0	02.03.2021	Ameet Ranchod	Version 1.0
1.1	31.05.2022	Celeste Ramnarayan	Version 1.1
1.2	01.07.2023	Donald Fraser	Updated personnel & roles
1.3	01.09.2024	Donald Fraser	2024 Revision, template change

Table of Contents

1 Policy Scope

This policy applies to all Digicall Group users and management responsible for application identity and role definition within their departments.

2 Policy Statement

Information security requires the participation and support of all users with access to Digicall Group systems and information. It is the responsibility of every employee, consultant, temporary employee, and contractor of Digicall Group (collectively known as “users”) to help ensure that all information and data are kept secure and available. Likewise, well-defined management practices and supports are necessary. Account identification and authentication procedures are one of the key components in this policy.

3 Purpose

Computerized user accounts are the means used to grant access to systems and applications. These accounts provide a means of providing standards, security, and accountability across the application pool and system environment for organizational roles. Creating, controlling, and monitoring computer accounts are actions that are critically important to the overall security policy and strategy. The purpose of this policy is to provide mechanisms that define and manage accounts for user communities accessing Digicall Group resources.

4 General

4.1 Applications and Systems

Applications and systems in the scope of this policy include, but are not limited to operating systems, application software, tablets, telecommunications equipment, and/or devices or network software that accesses Digicall Group resources.

4.2 Roles and Responsibilities

a. The relevant regional IT Infrastructure Manager or their designee shall ensure that Digicall Group systems and applications are protected from unauthorized access by establishing requirements for the authorization and management of user accounts, providing user authentication, and implementing access controls for all departments in their region.
b. The data owner for each information system shall be responsible for ensuring that user access requests, authorization, and account management, are followed for their specific application, user roles are defined, and that the appropriate people are assigned the responsibility of overseeing application usage. The design and

development of the authorization and account management processes shall be defined through the Digicall IT Infrastructure Manager and managed through the relevant regional IT Infrastructure Manager and his helpdesk team.

4.3 Access Credential Management

a. Account requests shall be processed through a standard procedure and process across Digicall Group. The relevant regional IT Department shall define and manage this process on behalf of the Digicall Group through the Digicall Group helpdesk and support/ticketing system. The following requirements shall be enforced:
    i. Access requests shall be limited to the systems and applications described in the work order.
    ii. Applications shall only be used for the purposes stated on the request.
    iii. A new request is required if there are changes in role or access privilege to the stated application.
    iv. The authorization request must be approved by the data/application owner.
    v. System administrators managing computer systems must have at least two user IDs, one that provides privileged access and is logged, and another that provides the privileges of a normal user for day-to-day work.
b. Access to systems and applications are generally established or reviewed under the following conditions:
    i. A new user requires access for the purpose of fulfilling job responsibilities.
    ii. An existing user has a change in job function requiring a change in role and privileges.
    iii. A user is terminated or no longer needs access to the system or application.
c. System owners must perform quarterly access reviews to ensure appropriate access and maintain system security.
d. Users engaged by a third party will only have access to Digicall systems and applications for a three-month period, after which access will be disabled. Users will have to reapply for renewed access after the three-month period has expired.
e. Requests for a change in access rights (e.g., to allow or disallow access) shall be accomplished by submitting a new help desk request following account management procedures and processes defined by the Digicall Group.
f. Privileged account passwords provide administrative or elevated levels of access to enterprise systems and sensitive data, based on higher levels of permissions. A privileged account can be associated with a human being or non-human IT system, such as:
    i. Service accounts, which run application services such as Windows Services, scheduled tasks, batch jobs, and Application Pools within IIS.

ii. Application accounts, which include database logins, certificates for software signing, embedded build script passwords, configuration files, and application services used during software development.
iii. System administrator accounts used to manage databases.
iv. Domain administrator accounts used to manage servers and control Active Directory users, as well as local domain accounts at the workstation level.
v. Root accounts used to manage Unix/Linux platforms

g. Privileged User Account Approval
    i. The creation or modification of privileged user accounts must be approved by at least two individuals:
        - The IT Infrastructure Manager and
        - The Back Office Manager and or IT Security & Compliance Manager.
    ii. System administrators must not be allowed to create other privileged accounts without authorization.

h. User Account Password Complexity
    i. Please refer to section 4. *Security* in the *Acceptable Use Policy* for User Account complexity.

i. Privileged Account Password Complexity
    i. Password length should be at least 20 characters.
    ii. Should have a complete mix of upper case, lower case, numbers, and symbols.
    iii. Where available Multifactor Authentication (MFA) must be enabled.

j. Password History and Change Interval
    i. User passwords must be changed once every 90 days.
    ii. Password history should not be less than 20 passwords.
    iii. All privileged accounts should have their passwords changed based on the internal risk assessment for potential disruption, e.g. Domain Admin account would have zero disruption, but the risk is very high, therefore the account should be disabled and only enabled when needed. Domain Admin access should rather be delegated to named admin accounts.
    iv. All privileged system accounts (Service, Domain, etc) should have their credentials changed upon departure of senior IT Staff.

k. Ensure passwords are communicated through a secure channel.

l. Maximum login attempts should be set to 5 attempts to enter an incorrect password, after which the account should be locked out.

m. All accounts that have been locked out due to incorrect login attempts should remain inactive until unlocked by an administrator.

n. Domain administrators should be notified of all account lockouts for incorrect login attempts so that investigations can be conducted, and necessary remediation conducted.

o. If a privileged user credential has been compromised, all passwords relating to that, and related systems must be changed immediately.

4.4 Acceptable Use of Accounts

a. User account passwords must never be shared or revealed to anyone other than the authorized user.
b. Privileged account passwords should not be shared, and each privileged account must have a unique password.
c. The display and printing of account passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.

4.5 Transfers, Terminations, Maintenance and Data Retention/Transfer

a. When a user is transferred or terminated, access to systems and applications shall be immediately terminated unless justified and approved in writing by the data owner and relevant regional IT Manager.
b. User work records and data stored locally or on Digicall Group servers shall be preserved.
c. The process for system and account revocation is managed through the relevant regional IT Manager and helpdesk in concert with application data owners and Digicall Group management.
d. It is the responsibility of the direct supervisor or manager to notify all appropriate personnel when a user transferred or terminated.
e. The data owner for each information system shall ensure that all user accounts are reviewed, and access rights evaluated at least once per year.
f. Account databases shall be regularly scavenged for inactive records and disabled as appropriate based on a schedule for account maintenance determined by the relevant regional IT Manager.

4.6 Remote Access

a. Digicall's chosen method of remote access is via VPN, using the Digicall provided VPN client.
b. Staff shall contact the IT help desk for approval to remotely connect to Digicall Group systems.
c. Staff accessing systems remotely are responsible for ensuring their mobile device is compliant with applicable Digicall Group policy.
d. All devices shall be inspected by the Digicall Group IT help desk prior to use to ensure the device is up to date with all applicable security patches and virus/malware protection software.

e. Users with remote access privileges shall ensure that their remote access connection is used explicitly for business and used in a manner consistent with their on-site connection to the Digicall Group network.
f. Secure remote access shall be strictly controlled.
g. Information security shall determine the appropriate access methodology and hardening technologies up to and including multi-factor password authentication, smart card, VPN, or PKI technology with strong passphrases.
h. All user passwords shall follow guidelines and procedures in the Digicall Group Acceptable Use Policy.
i. Staff shall ensure that devices used for work purposes are not shared in a multi-user capacity, violate the Acceptable Use Policy conditions, or used in any inappropriate activity.
j. Users shall bear full responsibility for any access misuse.
k. Digicall Group users with remote access privileges shall ensure their remotely connected workstation does not bridge or share another private or public internet connection.
l. A home routed and firewalled, internal private network using network address translation (NAT) technology is exempted from this clause (l) provided said network is under the complete control of the user.
m. Personal equipment shall not be used to connect to the Digicall Group network using remote connection software and exceptions require relevant regional Digicall IT Manager's written approval.

4.7 Administration and Management

a. The relevant regional IT Manager or their designee shall ensure that:
    i. All default user passwords are changed at the first login.
    ii. Default application, database, and system passwords shall be changed by systems personnel before moving into production.
    iii. Default user accounts provided with purchased software must be disabled or the account names changed upon installation.
    iv. Default accounts must be used only for designated maintenance tasks and must not be employed for daily use.
    v. Security mechanisms shall restrict access to credentials for the least privilege necessary to perform job responsibilities and such access is based on job classification role and function.
    vi. Approvals are secured by authorized parties specifying necessary access control lists.
    vii. Access control lists for systems components shall be set to deny all unless privilege to a particular function is explicitly allowed.

viii. Termination procedures exist for handling data, and they are well known by support staff and Digicall Group data owners.
ix. Procedures exist that assign responsibility for removing IT and/or physical access to facilities and collection or removal of biometric access, premise keys, cards, and other mechanisms for secure facility access.
x. Regular reviews of users with access to sensitive information shall be performed to ensure they are appropriate, necessary, and valid.
xi. Inactive accounts shall be immediately disabled or removed from account databases.
xii. The organization assigns a unique name and/or number for identifying and tracking user and administration identity. Procedures require that:
    - User identifiers be in a specific format and singularly unique.
    - Identifiers be used to track activity within information systems that contain sensitive information.
    - Authentication procedures verify identity.
    - Policies defined by the relevant regional IT Manager shall specify the types of approved authentication mechanisms that are reasonable and appropriate and control the addition, deletion, and modification of user credentials and other identifier objects.
xiii. Shared or guest accounts shall not exist for system administration or generic roles/usage or other functions, excepting identified service account credentials managed, defined, and documented by the Digicall Group IT Department.

xiv. Configuration standards are developed for all system components. Such standards shall:
    - Address known security vulnerabilities.
    - Be consistent with industry-accepted system hardening standards recommended by industry best practice.
    - Ensure that security policies and operational procedures for managing application default accounts, system accounts, and other security parameters are documented, in use, and known to all affected parties.
    - Ensure two-factor authentication is implemented for remote network access originating from outside the network by all staff and all third-party providers, (including vendor access for support or maintenance).

b. End-user support and helpdesk staff shall ensure:
    i. Vendor supplied default credentials are modified, removed, or disabled.

ii. Unnecessary default or generic accounts are changed before system is allowed on the network, including firewalls, routers, servers, storage devices, wireless devices, etc. that are connected to sensitive data or used to transmit sensitive data.
iii. Ensure all default passwords are changed including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, Point-of-Sale ("POS") terminals, Simple Network Management Protocol ("SNMP") community strings, etc.).
iv. Change wireless vendor defaults for environments containing or transmitting sensitive data, including, but not limited to, default wireless encryption keys, passwords, and SNMP community strings.
v. Account creation and control shall be governed by this policy, the Digicall Group Acceptable Use Policy, all the defined Digicall Group Access Policies and the Data Encryption Policy.
vi. Accounts of individuals on extended leave (more than 30 days) shall be disabled.
vii. All new user accounts not been accessed within 60 days of creation will be disabled.
viii. Existing accounts not accessed for a period of 90 days will be disabled and deleted from the account database if not accessed after 180 days.

4.8 Network Administration and Support - System administrators or other designated staff shall ensure:

a. A documented process exists to modify accounts that accommodate situations such as name changes, accounting changes, and/or permission changes.
b. All actions and systems are available, and staff cooperate with independent audit reviews for compliance.
c. Account listings and other controls are reported as requested by authorized management.
d. Staff cooperate with authorized Digicall Group management during security incident investigations.
e. Server roles and functions are organized and partitioned to appropriate functions and services that limit access risk (for example, web servers, database servers, and Domain Name Servers ("DNS") should be implemented on separate systems).
f. Where virtualization technologies are in use, the administrator shall implement only one primary function per virtual system component.
g. Only necessary services, protocols, daemons, etc., required for the function of the system are enabled and all unnecessary features or unsecure features are disabled (NetBIOS, Telnet, FTP, etc.).

h. Any additional security features required for services, protocols, or daemons that are insecure are implemented (for example, use of secured technologies such as SSH, SFTP, SSL, etc. to protect unsecure services).
i. System security parameters and group policies are appropriately configured to prevent misuse and limit access to local consoles.
j. All non-console administrative access using strong cryptography is encrypted.
k. Inventory of infrastructure assets and related functions are maintained.
l. Identity is verified before modifying authentication credentials or security access.

4.9 User Notification

a. Users of information systems shall be notified either in writing or through electronic means whenever:
    i. Gaining access to a system where usage is monitored, recorded, and subject to audit.
    ii. Logging into Digicall Group systems via active directory security notification/splash screen and that the user has granted consent to such monitoring and recording.
    iii. Unauthorized use is prohibited and subject to criminal and civil penalties.

4.10 Other Considerations

a. Security personnel shall ensure effective administration of computer access to maintain system security. The following are important administrative considerations:
    i. Audit and Management Reviews – On an annual basis, the relevant regional IT Manager and management personnel shall review system user account documentation for compliance. These reviews shall be conducted on a system-wide basis. Reviews should examine:
        - Levels of access.
        - Conformity with the concept of least privilege.
        - Accounts scavenging practices.
        - Appropriate documentation and authorizations are secured.
b. Detecting unauthorized/illegal activities – Alternative mechanisms shall be used to detect unauthorized and illegal acts. The IT Infrastructure Manager and Group CIO shall determine the mechanisms and tools used to assist in managing premise, network, and system security.
c. Staff Terminations - Termination of staff shall be classified as either friendly or unfriendly.
    i. Friendly terminations – These events shall be accomplished by implementing a standard set of procedures and protocols for individuals. All termination

work shall be coordinated through the Digicall Group Human Resources Department. This normally includes:

- Removal of access privileges, computer accounts, authentication tokens.
- The control of keys to the office and/or office furniture and equipment.
- The briefing on the continuing responsibilities for confidentiality and privacy.
- Return of any Digicall Group property.
- Interim or replacement staff's ability to access data.

ii. Unfriendly terminations – These events have the potential for adverse consequences. All termination work shall be coordinated through the Digicall Group Human Resources Department. As such the following protocols shall be observed:

- System access shall be terminated to all systems as quickly as possible.
- If staff are immediately terminated, system access shall be removed at the same time (or just before) the individual is notified and dismissed. Coordination of the event shall occur through the Digicall Group Human Resources Department.
- Staff shall return all items or assets that belong to the Digicall Group.
- All actions should be performed in accordance with the Digicall Group Human Resources Department's leadership and direction.
- Assets shall be held as instructed in the case of legal review, chain of custody, or other investigative events. Legal holds shall be communicated by the Digicall Group Human Resources Department through the Group CIO and IT Infrastructure Manager.

5 Audit Controls and Management

1. On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the Digicall Group. Satisfactory examples of evidence and compliance include:
    a. Unit procedural and process documentation with roles and responsibilities.
    b. Security logs detailing system and application access events.
    c. Documented account creation, scavenging, deletion, and other procedures outlined in this policy in use by Digicall Group IT Department support staff.
    d. Historical and archival correspondence around policies and procedure outlined in this document.

6 Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

7 Responsibilities

The IT Security and Compliance Manager is responsible for maintaining this policy and providing support and advice during its implementation in line with the IT Risk Management Policy

All Managers are directly responsible for implementing the policy and ensuring staff compliance.

Compliance with this Information Security and all subsequent policies is mandatory.

8 Policy Compliance Monitoring

8.1 Compliance

Group IT will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

If any user is found to have breached this policy, they may be subject to the Digicall Group's disciplinary procedures. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

8.2 Exceptions

Any exception to this policy must be approved by the Group Chief Information Officer in advance.

8.3 Non-compliance

All users (employees, contractors, vendors) are required to adhere to this Policy. Failure to comply may result in disciplinary action up to and including termination from employment, termination of contract, and civil penalties and/or criminal sanctions, depending on the circumstances.

8.4 Remediation of Non-compliance

Where non-compliance has been identified, dependent on the severity and criticality and impact, opportunities may be provided to correct identified non-compliance. This corrective

action will be evaluated on a case-by-case basis and timelines will be imposed and strictly enforced to ensure timeous remediation.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Human Resources Department or the IT Security and Compliance Manager.

9 Policy Governance

The following table identifies who within the Digicall Group is **Accountable, Responsible, Informed** or **Consulted** with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	IT Security and Compliance Manager
Accountable	Group Chief Information Officer
Consulted	IT Infrastructure Manager, Regional IT Infrastructure Managers
Informed	All Employees, All Temporary Staff, All Contractors, All Vendors and All Suppliers

10 Audit and Review Process

This policy and compliance there to, will be audited and reviewed internally at least once every 12 months depending on the changes or requirements within the group which will be reviewed by Management, or as required by significant changes in business operations or regulatory requirements.

For Group companies' pursuing certification, policies are required to be audited externally at least once in a 36-month cycle or sooner depending on changes or requirements within the group. Any employees or contractors with suggestions should refer these to their line manager in the first instance so they can be considered for implementation. Whenever changes are made to this policy the final draft will be shared with the Group CIO, IT Infrastructure Manager and the IT Security & Compliance Manager for review and approval before publication.

The IT Security and Compliance Manager will undertake annual policy reviews.

11 Appendices

None included with this policy.