DIGICALL

A13 - FIREWALL 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		04/10/2024
Ameet Ranchod	IT Infrastructure Manager		07/10/2024
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	28.02.2019	Justus Boyens	Document Creation
0.9	24.02.2021	Ameet Ranchod	Final Draft
1.0	23.03.2021	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 staff responsible for managing premise, physical, and logical networks as well as internet and application security.

2 Policy Statement

Firewalls are hardware devices or software programs that control the flow of traffic between networks, servers, and computer systems. They protect internal resources from intrusion and are an important part of information security. This policy defines the policies and procedures around firewall implementation within the Digicall Group.

3 Purpose

This policy helps protect Digicall Group information asset availability, confidentiality, and integrity from outside intrusion and hacking activities. Firewalls and the technology/procedures that support them help protect internal networks and manage traffic in and out of the network.

4 General

Digicall Group uses a multi-layered approach to protect computer resources and assets. Network security design shall include firewall functionality at all places in the network where outside exploitation exposures exist. This may include areas other than the network perimeter to provide an additional layer of security and protect devices that are placed directly onto external networks (demilitarized zone).

4.1 General Configuration

a. The relevant regional Digicall IT Manager or their designee shall define how an organization's firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization's information security policies.
b. Digicall Group IT staff shall:
    i. Restrict inbound and outbound traffic to that which is necessary for sensitive data and specifically deny all other traffic.
    ii. Install perimeter firewalls between all wireless networks and sensitive data and configure these firewalls to deny or, control (if such traffic is necessary for business purposes), to permit only authorized traffic between the wireless environment and environments containing sensitive data.
    iii. Regularly review and develop a list of the types of traffic needed by the organization and how they must be secured including an analysis of which

types of traffic can traverse a firewall under what circumstances. This should be performed at least once every 18 months.

iv. All inbound and outbound traffic not expressly required shall be blocked which reduces the risk of attack and decreases traffic volume carried on the Digicall Group's internal network.

v. Identify configuration requirements when determining firewalls.

vi. Consider network-related assets as well as the firewall technologies most effective at blocking network-related threats.

vii. Identify performance considerations and concerns surrounding firewall integration into existing network and security infrastructure.

viii. Design firewall solutions to include Digicall Group physical network requirements as well as consideration of possible future needs.

ix. Create network traffic rules that are as specific as possible while allowing user functionality.

x. Document traffic and protocol exceptions a firewall may need, for use in management and administrative functions.

xi. Implement a demilitarized zone (DMZ) that limits inbound traffic to system components that provide authorized publicly accessible services, protocols, and ports/services.

xii. Disallow direct connections (inbound and outbound) for traffic between the internet and environments containing sensitive, confidential, or personally identifiable information.

xiii. Implement anti-spoofing measures to detect and block forged source IP addresses from entering the internal network.

xiv. Use stateful packet inspection technologies (e.g. dynamic packet filtering) so that only established connections are allowed into the network.

xv. Ensure all system components that store sensitive information (e.g. production databases) in an internal network zone are segregated/segmented from the DMZ and other untrusted or public networks.

xvi. Disallow private IP addresses and routing information to unauthorized parties.

xvii. Authorized methods to obscure IP addressing shall include Network Address Translation (NAT) configurations, removal or filtering of route advertisements for private networks, and internal use of RFC1918 address space instead of registered addresses.

xviii. Formal hardening and testing procedures are in place. As part of the hardening procedure, default passwords and configurations shall be changed to further enhance device security. Further to this annual

penetration tests should be performed, the results of which should be used to further strengthen security policies in place.

xix. All device passwords shall be long and complex meeting all requirements in the Digicall Group Acceptable Use Policy.

xx. Enterprise firewalls shall be under maintenance and support contract with appropriate response time guarantees.

4.2 Administration and Management

a. The relevant regional Digicall IT Manager and network support staff are responsible for managing firewall architectures, policies, software, and other solution components. Policy rules shall be updated as Digicall Group network and access requirements change, when new applications or servers are implemented within the network or should other business drivers indicate. The following firewall management procedures shall be implemented:

   i. Performance shall be monitored daily to ensure availability and operation of all premise and architectural firewall components.

   ii. Monitoring and alerting tools shall be used to proactively monitor and address issues before the environment has an outage or a threat is detected.

   iii. Configuration rules and policies shall be managed by a formal change management control process.

   iv. Rules, reviews, and periodic tests shall be performed to ensure continued compliance with organizational policy, this should take place at least once every 18 months.

   v. Software and hardware firmware shall be patched as vendors provide updates to address vulnerabilities. Refer to the A12 - Patch Management Policy for more detail.

   vi. All configurations shall prohibit direct internal access to public networks (e.g. internet).

   vii. Port or Internet Protocol (IP) address filtering technology shall be used to limit network access.

   viii. Configurations shall restrict all traffic, inbound and outbound, from untrusted wired/wireless networks and hosts and specifically deny all other traffic except for necessary protocols.

   ix. Physical access to hardware firewall devices shall be tightly restricted to authorized security and network personnel.

   x. All desktops, laptops, and similar devices should have software firewalls installed as an additional means of protection.

xi. Firewall security log files shall be configured, maintained, and periodically reviewed for anomalies as indicated in the Group Information Security Policy.
xii. Logs shall be of sufficient size to provide useful information in case of a security event.
xiii. Appropriate security staff shall receive periodic training regarding new and developing threats, current data security practices, and changes in compliance regulations as and when they become available.

4.3 Audit Controls and Management

a. On-demand documented procedures and evidence of practice should be in place for this operational policy as part of Digicall Group internal operational processes and procedures. Examples of appropriate controls and management practice include:
    i. Formalized change procedures surrounding network configuration and management.
    ii. Archival logs of configuration changes and premise intrusion monitoring.
    iii. Network system documentation and regular review processes.
    iv. System and device patching logs.
    v. Historical incident and response logs.

5 Enforcement

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

6 Responsibilities

a. The relevant regional Digicall IT Manager or their designee shall ensure the following controls are in place:
    i. A formal process for approving and testing all network connections and changes to the firewall and configurations.
    ii. Current network infrastructure diagrams identifying connections between environments containing sensitive data and other networks, including any wireless networks.
    iii. Network diagrams and documents detailing sensitive data flows across systems and networks.
    iv. Firewalls are positioned at each internet connection and between any demilitarized zone (DMZ) and the internal Digicall Group network.

v. Documentation is in place that describes groups, roles, and responsibilities for management of network components.
vi. Documentation exists for use of all services, protocols, and ports/services allowed.
vii. Procedural review of firewall configurations at least annually.
viii. A standard configuration exists for fast and consistent firewall deployment.
ix. All critical firewalls are identified and are under maintenance/replacement contracts.
x. Subscriptions/licenses satisfy business and legal requirements.

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.

7 Policy Compliance Monitoring

7.1 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).

7.2 Exceptions

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

7.3 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.

7.4 Remediation of Non-compliance

Where non-compliance has been identified, dependent on the severity and criticality and possible 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.

8 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

9 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.

10 Appendices

None included with this policy.