DIGICALL

A12 - SERVER HARDENING POLICY V1.4

DOCUMENT CLASSIFICATION	Internal Use Only
VERSION	1.4
DATED	01 September 2024
DOCUMENT AUTHOR	Ameet Ranchod
DOCUMENT OWNER	Johan Kriel

DIGICALL

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	01.02.2019	Justus Boyens	Document Creation
0.9	04.02.2019	Justus Boyens	Final Draft
1.0	05.02.2019	Justus Boyens	Version 1.0
1.1	31.01.2020	Ameet Ranchod	Annual Review
1.2	31.05.2022	Ameet Ranchod	Annual Review
1.3	01.07.2023	Donald Fraser	Updated personnel & roles
1.4	01.09.2024	Donald Fraser	2024 Revision, template change

DIGICALL

Table of Contents

1 Policy Scope

This policy applies to all Digicall Group staff that use, deploy, or support Digicall Group server hardware/virtual resources.

2 Policy Statement

Servers in their many forms (file, print, application, web, and database) are used by the organization to supply critical information for staff. These assets must be protected from both security and performance related risks. One of the required steps to attain this goal is to ensure that hardware (whether on premise or in the cloud) is installed and maintained in a manner that prevents unauthorized access, unauthorized use, consistent configuration, and minimal service disruptions.

3 Purpose

Appropriate measures must be taken when configuring and managing server-based resources to ensure the confidentiality, integrity and availability of information. This policy provides general procedures and requirements for installing server-based resources in a secure manner as well as maintaining the security integrity of the hardware and application software.

4 General

4.1 Overall

A server hardening procedure shall be created and maintained that provides detailed information required to configure and harden Digicall Group servers whether on premise or in the cloud. The procedure shall include:

1. Installing the operating system from an IT approved source.
2. Applying all appropriate vendor supplied security patches and firmware updates.
3. Removing unnecessary software, system services, protocols, ports, and drivers.
4. Setting security and operational parameters including configuring system services, firewall, anti-virus, anti-malware, and local system passwords/accounts.
5. Enabling appropriate local file system/sharing permissions, audit logging, local/physical security, reporting, and intrusion detection software as applicable.
6. Applying Digicall Group Domain-based Active Directory server-based group policy, configured to industry best practice most restrictive settings.

4.2 Operations and Maintenance

Digicall Group server support shall perform the following procedures and processes to ensure hardening compliance after the initial system is delivered:

1. Post-install operating system, utility/system service patches (e.g., COM and .NET), database, web, and application security patches shall be pre-tested and deployed on a regular basis against similar systems before rolling out to the production environment.
2. In the case of custom applications or enterprise software, Digicall Group server support shall take appropriate precautions to ensure patch compatibility prior to install. Should a patch be incompatible with a specialized software package, exceptions must be approved in writing by the relevant regional Digicall Group IT Manager or their designee.
3. All sensitive information shall be encrypted at-rest and in-transit as well as complying with the Digicall Group Data Encryption Policy. Where appropriate, PKI certificates/key strategies shall be used to additionally secure web-based access.
4. Periodic audits of server compliance shall be conducted at least annually. Results shall be documented, and any deficiencies corrected.

5 Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the Digicall Group internal processes and procedures. Examples of appropriate controls and documentation are:

1. Documented servers build processes and images.
2. Internal configuration and asset management protocols and procedures.
3. Patch logs containing server name, patch installed, service installed and date.
4. GPO documentation showing hardening and security measures employed across the enterprise.
5. Archival audit documentation with results and remedies taken to address security concerns.

6 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 personally 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.