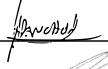
DIGICALL

A12 - PATCH 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	03.02.2020	Ameet Ranchod	Document Creation
0.9	23.03.2021	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 employees and contractors during the performance of company related business and duties.

2 Policy Statement

Regular application of vendor-issued critical security updates and patches are necessary to protect Digicall's data and systems from malicious attacks and erroneous function. All electronic devices connected to the network including servers, workstations, firewalls, network devices, tablets, mobile and cellular devices routinely require patching for functional and secure operations.

3 Purpose

Software is critical to the delivery of services to Digicall customers and users. This policy provides the basis for an ongoing and consistent system and application update policy that stresses regular security updates and patches to operating systems, firmware, productivity applications, and utilities. Regular updates are critical to maintaining a secure operational environment.

4 Policy

4.1 General

All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. System components and devices attached to the Digicall network shall be regularly maintained by applying critical security patches within thirty (30) days after release by the vendor. Digicall's policy on patch versions is N-1 unless the patch addresses a critical vulnerability or security update. Other patches not designated as critical by the vendor shall be applied on a normal maintenance schedule as defined by normal systems maintenance and support operating procedures.

4.2 System, Utility and Application Patching

A regular schedule shall be developed for security patching of all Digicall systems and devices. Patching shall include updates to all operating systems as well as office productivity software, database software, third party applications (e.g., Adobe Reader, Chrome, FortiClient, etc.), and mobile devices under the direct management of Digicall Group IT.

The regular application of critical security patches is reviewed as part of normal change management and audit procedures.

4.3 Patching Exceptions

Patches on production systems (e.g., servers and enterprise applications) may require complex testing and installation procedures and in certain cases, risk mitigation rather than patching may be the preferable option. The risk mitigating alternative, should be determined through an outage risk to exposure comparison. The reason for any departure from the above standard and alternative protection measures taken shall be documented in writing for devices storing non-public data. Deviations from normal patch schedules shall require the authorization of both the CIO and CISO.

4.4 Security Patching Procedures

Policies and procedures shall be established and implemented for vulnerability and patch management.

The process shall ensure that application, system, and network device vulnerabilities are:

a. Evaluated regularly and responded to in a timely manner.
b. Documented and well understood by support staff.
c. Automated and regularly monitored wherever possible.
d. Executed in a manner applicable with vendor-supplied tools on a regularly communicated schedule.
e. Applied in a timely and orderly manner based on criticality and applicability of patches and enhancements.

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's internal systems change management and update procedures. Examples of adequate controls include:

a. Documented change management meetings and conversations between key Digicall stakeholders.
b. System updates and patch logs for all major system.
c. Logs should include system ID, date patched, patch status, exception, and reason for exception.
d. Demonstrated infrastructure supporting enterprise patch management across systems, applications, and devices.

6 Monitoring and Reporting

Those with patching roles, as detailed above, are required to compile, and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to the Digicall Group IT Security and Compliance Team as well as Internal Audit upon request.

7 Responsibilities

7.1 Digicall Group IT Departments

a. Will manage the patching needs for the Windows estate that is connected to the Digicall domain.
b. Responsible for routinely assessing compliance with the patching policy and will provide guidance to all the stakeholder groups in relation to issues of security and patch management.

7.2 Change Advisory Board:

a. Responsible for approving the monthly and emergency patch management deployment requests.

7.3 End Users

a. The end user has a responsibility to ensure that patches are installed, and the machine is rebooted when required. Any problems must be reported to Digicall Group IT via the approved call logging process.

7.4 Third Party Suppliers

a. Will ensure security patches must be up to date for IT systems which are being designed and delivered by third party suppliers prior to going operational.
b. Once the IT systems are operational, third-party suppliers must ensure vulnerability patching is carried out as stipulated. Where this is not possible, this must be escalated to the Head of IT Security and Compliance.

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.

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, 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.