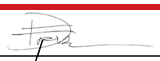
DIGICALL

A12 - CHANGE MANAGEMENT POLICY V1.7

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	01.02.2019	Justus Boyens	Document Creation
0.9	05.02.2019	Justus Boyens	Final Draft
1.0	06.02.2019	Justus Boyens	Version 1.0
1.1	15.08.2019	Justus Boyens	Addition of point 6 Implementation and Operational Considerations
1.2	10.02.2020	Ameet Ranchod	Annual review, addition, and inclusion of the Change Management Log Form
1.3	16.03.2020	Ameet Ranchod	Further enhancements and clarifications
1.4	19.03.2020	Ameet Ranchod	Amendments to Review, Added Policy Compliance Monitoring and Policy Governance, updated template.
1.5	31.05.2022	Celeste Ramnarayan	Annual Review
1.6	01.07.2023	Donald Fraser	Updated personnel & roles
1.7	01.09.2024	Donald Fraser	2024 Revision, template change

Table of Contents

1 Policy Scope

This policy applies to all Digicall Group staff and Contractors, involved in application or systems changes, updates, or patches.

2 Policy Statement

Applications and systems are increasingly more complex in their function, interaction, and form. There is an increasing dependency between resources and applications that can negatively impact operations if not managed and orchestrated in an organized fashion. Effective management and communication of updates, maintenance, and regular releases help to minimize customer impacts. From time-to-time systems require outages for planned upgrades, maintenance, or fine-tuning. Managing these changes is a critical part of providing a stable infrastructure.

3 Purpose

The purpose of this policy is to manage changes in a well-communicated, planned, and predictable manner that minimizes unplanned outages and unforeseen system issues. Effective change management requires planning, communication, monitoring, rollback, and follow-up procedures to reduce negative impact to the user community.

4 General

4.1 General

1. All system and application changes in the relevant regional Digicall Group IT Department or managed by Contracting parties (e.g., operating system, computing hardware, networks, applications, data centres) are subject to this policy and shall follow unit change management procedures.
2. The following general requirements shall be met in the change management process:
    a. Scheduled change calendars and departmental communications operational procedures shall be developed to inform stakeholders of upcoming application and system changes that impact system availability or operations.
    b. Regular planned changes shall minimally be communicated to all stakeholders on a weekly basis through a communication mechanism of the relevant regional Digicall Group IT Manager's choosing.
    c. Unplanned outages shall be communicated immediately to stakeholders with regular updates on progress towards resolution and resumption of service.
    d. Regular system and application patching schedules shall be communicated to users and performed in such a way as to minimize system downtime and user productivity, as indicated in the Patch Management Policy.

e. Changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) shall be reported to or coordinated with facilities and stakeholders shall be notified through the relevant regional Digicall Group change management communications.
f. Processes shall ensure that production data is not unnecessarily replicated or used in non-production environments.
g. Device configurations shall be backed up and rollback procedures must exist prior to implementing a change.

4.2 Change Management Committee

1. A Digicall Group Change Management Committee shall convene to discuss system changes, interactions, and any perceived issues. This committee shall be made up of network and systems staff, application development owners, developers, and chaired by the relevant regional Digicall Group IT Manager or their designee. The following procedures shall be implemented by the committee:
    a. The committee shall meet on a schedule determined by the Digicall Group IT Infrastructure Manager but shall meet when needed to discuss plans for future updates and patching.

4.3 Change Request Management

1. The following procedure shall be implemented surrounding the change management process:
    a. Change requests shall be submitted for all changes, both scheduled and unscheduled.
    b. All scheduled change requests shall be submitted in accordance with departmental change management procedures so that the Change Management Committee has time to review the request, determine and review potential failures, and make the decision to allow or delay the system update.
    c. Change requests shall receive Change Management Committee approval before proceeding with the change.
    d. A change review must be completed for each change, whether scheduled or unscheduled, and whether successful or unsuccessful.

4.4 Change Management Denials

1. The relevant regional Digicall Group IT Manager or their designee, system owners or stakeholders may deny a scheduled or unscheduled change for reasons including, but not limited to:
    a. Inadequate change planning or unit testing.

b. Lack of stakeholder acceptance (where applicable).
c. System integration or interoperability concerns.
d. Missing or deficient roll-back plans.
e. Security implications and risks.
f. Timing of the change negatively impacting key business processes.
g. Timeframes do not align with resource scheduling (e.g., late-night, weekends, holidays, or during unique events).

4.5 Administration

1. A Change Management Log Form shall be maintained for all changes. This log must contain, but is not limited to:
    a. Date of submission and date of change.
    b. Owner and custodian contact information.
    c. Nature of the change
    d. Implementation and rollback plans.
    e. Systems affected.
    f. Priority and impact of the change on the environment.
    g. Risk statement.
    h. Supporting documents, if any.
    i. Release statement indicating success or failure with a report and a remedial plan in the case of an unsuccessful, aborted or rolled back change.
    j. User acceptance testing.
    k. Signatures of the required approvers.

4.6 Implementation and Operational Considerations

1. No new server implementations are to be commissioned in the Digicall Group environment without approval in writing, received from both the CIO and the IT Infrastructure Manager.
    a. All newly approved implementations must be updated and documented in the Group IT's infrastructure documentation repository upon completion.
2. No production virtual machine migrations between host servers are to be performed without approval in writing, received from both the CIO and the IT Infrastructure Manager.
    a. All approved migrations must be updated and documented in the Group IT's infrastructure documentation repository upon completion.
3. All new implementation and migration processes should follow the standard change control management process as described in this document.

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. Historical logs of change events.
    b. Archival Change Management Committee meeting minutes.
    c. Anecdotal documentation and communications showing regular compliance with the policy.

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, 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.

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.