Taqnyat

Change Management Policy, version 1.0.0
Status: ☐ Working Draft ☒ Approved ☐ Adopted
Document Owner: Information Security Committee
Last Review Date: July 2023

Change Management Policy

Purpose

The purpose of the Taqnyat Change Management Policy is to establish the rules for the creation, evaluation, implementation, and tracking of changes made to Taqnyat Information Resources.

Audience

The Taqnyat Change Management Policy applies to any individual, entity, or process that create, evaluate, and/or implement changes to Taqnyat Information Resource.

Policy

- Changes to production Taqnyat Information Resources must be documented and classified according to their:
  - Importance,
  - Urgency,
  - Impact, and
  - Complexity.
- Change documentation must include, at a minimum:
  - Date of submission and date of change,
  - Owner and custodian contact information,
  - Nature of the change,
  - Change requestor,
  - Change classification(s),
  - Roll-back plan,
  - Change approver,
  - Change implementer, and
  - An indication of success or failure.
- Changes with a significant potential impact to Taqnyat Information Resources must be scheduled.
- Taqnyat Information Resource owners must be notified of changes that affect the systems they are responsible for.
- Authorized change windows must be established for changes with a high potential impact.
- Changes with a significant potential impact and/or significant complexity must have usability, security, and impact testing and back out plans included in the change documentation.
- Change control documentation must be maintained in accordance with the Taqnyat Data Retention Schedule.

Taqnyat Change Management Policy

- Changes made to Taqnyat customer environments and/or applications must be communicated to customers, in accordance with governing agreements and/or contracts.
- All changes must be approved by the Information Resource Owner, Director of Information Technology, or Change Control Board (if one is established).
- Emergency changes (i.e. break/fix, incident response, etc.) may be implemented immediately and complete the change control process retroactively.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 12.1.2
- NIST CSF: PR.IP-3
- Network Management Policy
- Data Retention Schedule

Waivers

Waivers from certain policy provisions may be sought following the Taqnyat Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	Nov 2022		FRSecure	Document Origination

شركة تقنيات الجوال
Taqnyat
JEDDAH 4030394715 - RIYADH 1010296254