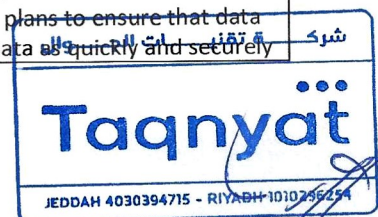


Data Backup and Recovery Policy Template

Title: Data Backup and Recovery Policy														
Department: Cyber Security	Version: Original													
Approved by: CISO	Approval Date: Jan-2023													
Senior Management Approval:														
Effective Date: Jan-2023	Last Updated: Jan-2023													
Author: Yazan Abdelrahman														
Scope This policy applies to all of Taqnyat IT systems and All of Taqnyat Information and Data														
Authority This policy is hereby approved and authorized. Higher Management <table border="0"><tr><td>_____</td><td>_____</td><td>_____</td></tr><tr><td>Name Yazan Abdelrahman</td><td>CISO</td><td>Date: Jan-2023</td></tr><tr><td>_____</td><td>_____</td><td>_____</td></tr><tr><td>Name Saoud Alsalm</td><td>CEO</td><td>Date: Jan-2023</td></tr></table>			_____	_____	_____	Name Yazan Abdelrahman	CISO	Date: Jan-2023	_____	_____	_____	Name Saoud Alsalm	CEO	Date: Jan-2023
_____	_____	_____												
Name Yazan Abdelrahman	CISO	Date: Jan-2023												
_____	_____	_____												
Name Saoud Alsalm	CEO	Date: Jan-2023												
Purpose The purpose of this policy is to define the activities associated with the provision of data backup and recovery plans and programs that protect <company name> information systems, networks, data, databases and other information assets. Additional policies governing specific disaster recovery (DR) activities will be addressed separately.														
Scope The scope of this data backup and recovery policy is all information technology systems, software, databases, applications and network resources needed by the Company to conduct its business.														
Statement of Compliance This policy is designed to be compliant with ISO/IEC 27031:2011 <i>Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity</i> , and NIST SP 800-34 <i>Contingency Planning Guide for Federal Information Systems</i> , and the FFIEC Information Technology Examination Handbook for Business Continuity Management (2022) Data backup and recovery policy compliance is managed by the IT data backup team, with support from other IT departments. To achieve compliance, data backup and recovery processes must include appropriate procedures, and identify staffing and technology resources to meet compliance requirements. Compliance verification is performed monthly by the IT department, internal audit or other appropriate entity.														
Policy The Information Technology (IT) department is responsible for managing all data backup and recovery activities for the Company. Certain departments, such as Finance and Accounting and Human Resources, are also responsible for providing the IT department with their requirements for data backup, protection and recovery. The IT department is also responsible for executing technology disaster recovery (DR) plans to ensure that data are backed up and securely stored, with the ability to quickly access and restore the data as quickly and securely as possible.														



as possible. The IT department is responsible for developing, executing and periodically testing procedures for data backup and recovery. The IT department also acknowledges it will comply with appropriate industry standards for data backup in its activities.

1. The company shall develop comprehensive data backup plans in accordance with good data backup and recovery management practices as defined by the above standards.
2. Data backup and recovery activities shall be performed as part of the company's business continuity management system (BCMS) and technology disaster recovery (DR) plans, which administer and manage the overall technology data backup program, which includes:
 - Planning and design of data backup and recovery activities
 - Identification of data backup teams, defining their roles and responsibilities and ensuring they are properly trained and prepared to respond to an incident
 - Planning, design and documentation of data backup and recovery plans
 - Scheduling of updates to data backup and recovery business impact analyses
 - Scheduling of updates to data backup and recovery risk assessments
 - Planning and delivery of awareness and training activities for employees and data backup team members
 - Planning and design of incident response activities associated with data backup and recovery
 - Planning and execution of data backup and recovery plan exercises
 - Designing and implementing a data backup and recovery program/plan maintenance activity to ensure that plans are up to date and ready for use
 - Preparing for management review and auditing of data backup and recovery plan(s)
 - Planning and implementation of continuous improvement activities for the data backup and recovery program and plan(s).
3. A formal risk assessment (RA) and business impact analysis (BIA) shall be undertaken to determine the requirements for all data backup and recovery plans; RAs and BIAs shall be updated at least annually to ensure they are in alignment with the business and its technology requirements.
4. Strategies for responding to specific technology incidents, as defined in the BIA and RA, shall be identified and used when developing individual data backup and recovery plans
5. Data backup and recovery plans shall address the backup and recovery of critical technology elements, including systems, networks, databases and data, in accordance with key business activities.
6. Data backup and recovery plans shall be periodically tested in a suitable environment to ensure that the systems, networks, databases and other infrastructure elements can be recovered and returned to a business as usual (BAU) status in emergency situations and that <company name> management and employees understand how the plans are to be executed as well as their roles and responsibilities.
7. All employees must be made aware of the data backup and recovery program and plans and their own roles and responsibilities during an incident.
8. Data backup and recovery plans and other documents are to be kept up to date and will reflect existing and changing circumstances.

Data Backup and Recovery Specifications

Following are specific data backup and recovery technical requirements:

General

1. State the frequency and types of backups to be performed
2. State who should be notified if a recurring problem with backup exists

Backup Verification

1. State how data is backed up and stored
2. State where data is stored and how it can be accessed
3. State process for ensuring that backup procedures work properly

Data Access, Security, Recovery and Restoration Procedures

1. State data access and security requirements when recovery is needed
2. State process for data recovery and restoration



Data Integrity

1. State how data integrity is protected during backup

Data Retention

1. State data retention time frames for each type of backup

Restore Requests

1. State process for processing requests for data restoration

Active Directory and System State Backup

1. State the backup process

Server Backup

1. State the backup process

SQL Backup

1. State the backup process

Virtualized System Backups

1. State the imaging and backup processes

Off-Site Backups

1. State the processes for any non-electronic off-site data storage (e.g., tapes)

Policy Leadership

CISO of Taqnyat is designated as the corporate owner responsible for data backup and recovery activities for the Company. Resolution of issues in the support of data backup activities should first be coordinated with IT management, the corporate business continuity and disaster recovery (BC/DR) team, and others as needed.

Policy Responsibilities

- Policy Approval – The <title of executive> is responsible for approving this policy.
- Policy Implementation – The <enter name of department or individual> is responsible for planning, organizing and implementing all activities that fulfil this policy.
- Policy Maintenance and Updating – The <enter name of department or individual> is responsible for all activities associated with maintaining and updating this policy.
- Policy Monitoring and Review – The <enter name of department or individual> is responsible for monitoring and reviewing this policy.
- Policy Improvement – The <enter name of department or individual> is responsible for defining and implementing activities that will improve this policy.

Management Review

IT and Cyber Security Department will review and update this data backup and recovery policy on an annual basis. As changes to this data backup and recovery policy are indicated in the course of business, CISO Yazan Abdelrhman may initiate a change management process to update this policy.

Policy Enforcement

The Data Protection and Cyber Security Departments of Taqnyat will enforce this policy.

Penalties for Non-Compliance



In situations where data backup and recovery activities do not comply with this policy, the IT data backup team will prepare a report stating the reason(s) for non-compliance and present it to IT management for resolution. Failure to comply with this data backup and recovery policy within the allotted time for resolution may result in verbal reprimands, notes in personnel files, termination, and such other remedies as deemed appropriate.

Policy Location

The policy will be signed, scanned into an electronic file and posted in the following location on the network:
4.12.1



©2020 TECHTARGET. ALL RIGHTS RESERVED.

