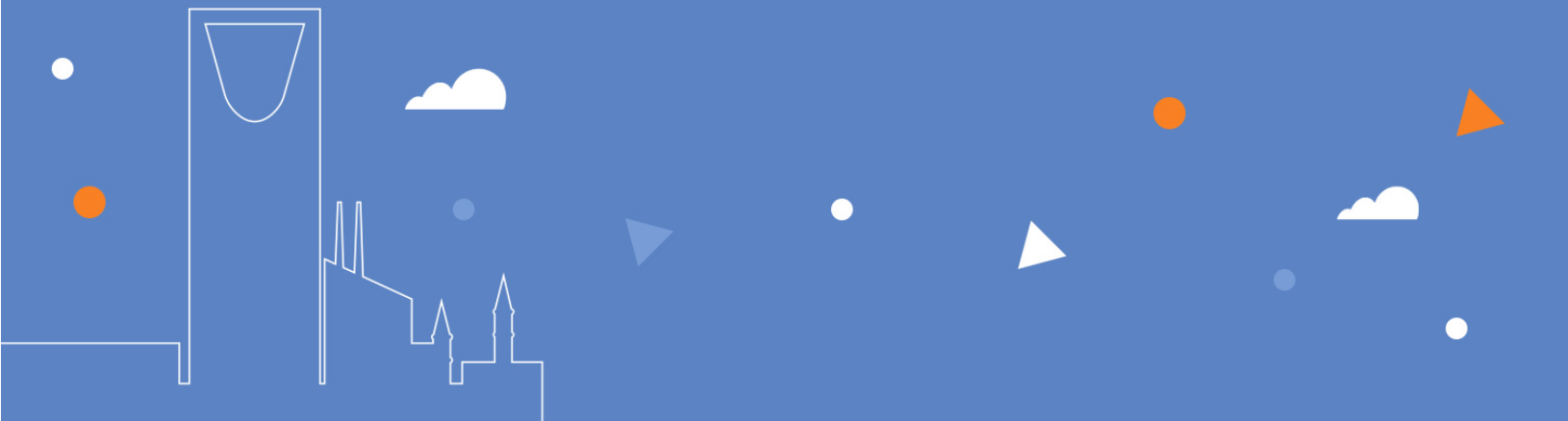


Business Continuity Plan (BCP)



Contents

1. Purpose.....	2
2. Objectives	2
3. Plan activation.....	2
4. Roles and Responsibilities of the Business Continuity Team.....	2
5. Incident Response Procedures.....	3
6. Operational business continuity procedures	3
7. Communications	3
8. Testing and training.....	4
9. Review	4

Version	Adjustment Date	Approved By	Approval Date and signature
1.0	13-4-2024	Saud Alsulami	15-4-2024
2.0	5-3-2025	Saud Alsulami	6-3-2025

1. Purpose

The goal of this plan is to establish a comprehensive framework that ensures business continuity for Taqnyat Al-Jawal Company and its critical services to customers, enabling rapid recovery and protecting information and technical assets that support key services

2. Objectives

- 2.1. Ensure the availability of critical services used by customers and all supporting services.
- 2.2. Work to minimize downtime and data loss.
- 2.3. Protect information assets
- 2.4. Effective response to any incident that could impact business continuity

3. Plan activation

3.1. Plan activation metrics

The business continuity plan is activated in the event of the following incidents:

- Failure in a system or group of systems that affects the services provided to customers
- Uncontrollable cyber-attacks that can lead to service outages or disruptions, or data leaks
- Inability to access the data center

3.2. Activation authority

- CEO
- Technical Consultant
- Security Incident Response Committee

4. Roles and Responsibilities of the Business Continuity Team

Responsibility for disaster management and ensuring business continuity lies with the Cybersecurity Committee, which handles any security incident and its potential impact on the company's services. The committee consists of:

- Technical Consultant
- Cybersecurity officer
- NOC officer

This committee is responsible for crisis management, identifying necessary requirements to address them, and ensuring full cooperation with the committee's decisions and their immediate implementation. These requirements include human and financial resources, as well as communication with external parties to ensure optimal crisis management

5. Incident Response Procedures

- Incidents are managed through the approved security incident response policy, which includes detection, reporting, classification, information gathering, containment, and initiating the recovery process
- Crises should be managed through policies and procedures for emergency changes. Approval is not obtained for changes, and all required documentation is prepared, and events are recorded. After the recovery phase, the following steps are taken
- Service recovery procedures may require data restoration from backups, which should be done through the approved recovery policy
- The Asset Recovery Plan is activated when replacing any physical assets

6. Operational business continuity procedures

The top priority in operational continuity procedures is to restore customer services, followed by technical support services, and then other internal services

The following procedures are included:

- Operating the backup site and ensuring all data is available within it
- Directly modifying network architecture and data flow to ensure business continuity, then making the required changes to network plans
- Finding alternative communication methods, including email and Teams
- Forming a communication team as needed to liaise with customers or external parties
- Finding alternative workplaces if required
- Setting up secure and encrypted connections via VPN for remote access

7. Communications

All communication methods and their alternatives in case of any issues:

- Ticketing System: Customers can submit tickets and receive answers through the same portal
- Email communication is possible through support@taqnyat.sa
- Chat systems available on the website
- Hotline 920015404
- Direct contact with the account manager

8. Testing and training

- An annual plan test is conducted to ensure its readiness or after significant changes to the service infrastructure
- Employees are trained annually in the plan and how to handle crises, roles, and the responsibilities required of all individuals

9. Review

- The plan is reviewed annually after training to make necessary amendments based on the lessons learned from the training

Internal Use Only