Redundancy and Disaster Recovery

Hex Secure Framework

VERSION: 1.2 REVISION DATE: Apr 17, 2025

Contents

Section 1 Purpose 3

Section 2 Redundancy Strategy 3

2.1 Redundant Servers 3

2.2 Redundant Power 3

2.3 Redundant Data 3

2.4 Redundant Networking 3

Section 3 Data Backup Planning 4

3.1 Daily Level Backup and Restore 4

3.2 Data Backup Planning 4

3.2 Snapshot Backup Planning 4

Section 4 Disaster Recovery Planning 4

4.1 Contact Information 4

4.2 Impact Determination 5

4.3 Recovery Plan 5

4.4 Business Continuity Plan 5

4.5 Disaster Recovery Drills and Exercises 5

Section 10 References 6

Section 1 Purpose

The purpose of this document is to establish a comprehensive IT security policy for Hexagon Group. This policy aims to ensure continuous business operations, minimize data loss, and enhance resilience against potential threats, cyberattacks, and system failures. By implementing redundancy strategies, robust data backup planning, and an effective disaster recovery framework, Hexagon Group will strengthen its IT infrastructure and mitigate risks associated with data breaches and hardware failures.

Section 2 Redundancy Strategy

2.1 Redundant Servers

Hexagon Group ensures server redundancy by implementing multiple strategies to prevent downtime and service disruptions. This includes deploying load-balancing mechanisms that distribute workloads across multiple servers, preventing overloading of any single system. Additionally, failover mechanisms are configured to automatically switch operations to backup servers in case of primary server failures. Geographic redundancy is also employed by maintaining data centers in multiple locations, ensuring continuity of services even in the event of a localized disaster.

2.2 Redundant Power

A reliable power supply is crucial for maintaining IT infrastructure. To mitigate power failures, Hexagon Group utilizes an Uninterruptible Power Supply (UPS) system for all critical infrastructure, ensuring that power fluctuations or outages do not impact operations. Backup generators are in place, equipped with automatic switching capabilities to activate immediately upon power loss. Furthermore, critical servers and networking equipment are designed with dual power supplies, allowing continued functionality even if one power source fails.

2.3 Redundant Data

Data redundancy is implemented through multiple layers to prevent data loss and ensure accessibility. Data mirroring and replication techniques are used across multiple storage locations to provide real-time data availability. Redundant Array of Independent Disks (RAID) configurations are employed to enhance fault tolerance within storage systems. Additionally, offsite backups are maintained to safeguard against data corruption or physical damage to primary storage systems, ensuring business continuity in any scenario

2.4 Redundant Networking

To maintain uninterrupted network connectivity, Hexagon Group deploys multiple internet service providers (ISPs) to establish failover connections, ensuring alternative routes for data transmission in case of primary network failures. Redundant firewalls, routers, and switches are configured to provide seamless connectivity and prevent single points of failure. Network segmentation using Virtual LANs (VLANs) further enhances security and traffic management, isolating critical systems from general access networks.

Section 3 Data Backup Planning

3.1 Daily Level Backup and Restore

Hexagon Group enforces a daily backup policy to protect business-critical data. Automated backup schedules are configured to run outside peak hours to avoid performance degradation. Integrity checks are performed regularly to ensure that backup files remain error-free and usable. A streamlined data restoration process is in place, enabling quick retrieval of lost or corrupted data to minimize downtime and operational impact.

3.2 Data Backup Planning

Hexagon Group implements a comprehensive data backup strategy to ensure data integrity and availability. This strategy encompasses:

Backup Frequency: Critical data is backed up daily, while less critical data follows a weekly backup schedule. Backup Types: A combination of full, incremental, and differential backups is utilized to optimize storage and recovery times. Storage Locations: Backups are stored in multiple locations, including on-premises servers and secure cloud storage solutions, to safeguard against data loss due to physical damage or cyber threats. Retention Policy: Backup data is retained for a period of 90 days, after which it is securely deleted, unless longer retention is required for compliance purposes. Access Controls: Access to backup data is restricted to authorized personnel only, with regular audits conducted to ensure compliance.

3.2 Snapshot Backup Planning

To complement traditional backups, Hexagon Group employs snapshot backups for rapid recovery and minimal downtime:

- Backup Frequency: Critical data is backed up daily, while less critical data follows a weekly backup schedule.
- Backup Types: A combination of full, incremental, and differential backups is utilized to optimize storage and recovery times.
- Storage Locations: Backups are stored in multiple locations, including on-premises servers and secure cloud storage solutions, to safeguard against data loss due to physical damage or cyber threats.
- Retention Policy: Backup data is retained for a period of 90 days, after which it is securely deleted, unless longer retention is required for compliance purposes.
- Access Controls: Access to backup data is restricted to authorized personnel only, with regular audits conducted to ensure compliance.

Section 4 Disaster Recovery Planning

4.1 Contact Information

In the event of a disaster, the following individuals are designated as primary contacts:

- IT Director
- Systems Administrator

- DR Specialist

4.2 Impact Determination

Hexagon Group conducts regular Business Impact Analyses (BIAs) to assess the potential effects of various disaster scenarios on operations. This includes evaluating:

- Critical Systems: Identifying systems essential to business continuity.
- Downtime Tolerance: Determining acceptable downtime for each critical system.
- Data Loss Tolerance: Establishing Recovery Point Objectives (RPOs) to define acceptable data loss periods.
- Recovery Time Objectives (RTOs): Setting target times for system restoration.

4.3 Recovery Plan

The recovery plan outlines the procedures for restoring operations following a disaster: Activation: The Disaster Recovery Team (DRT) assesses the situation and activates the recovery plan if necessary. Notification: Stakeholders, including employees, clients, and vendors, are informed of the incident and provided with regular updates. System Restoration: Critical systems are restored in order of priority, utilizing backups and redundant infrastructure. Verification: Restored systems are tested to ensure functionality and data integrity. Post-Incident Review: A thorough review is conducted to evaluate the response and identify areas for improvement.

4.4 Business Continuity Plan

To maintain operations during and after a disaster, Hexagon Group has established a Business Continuity Plan (BCP) that includes: Alternate Worksites: Pre-arranged locations equipped to support essential functions. Remote Work Capabilities: Infrastructure to enable employees to work remotely if necessary. Supply Chain Management: Strategies to ensure the continuity of critical supply chains. Communication Plans: Protocols for internal and external communications during a crisis.

4.5 Disaster Recovery Drills and Exercises

Regular drills and exercises are conducted to test the effectiveness of the disaster recovery plan: Tabletop Exercises: Simulated scenarios to evaluate response strategies and decision-making processes. Functional Drills: Hands-on tests of specific components, such as data restoration or failover systems. Full-Scale Exercises: Comprehensive simulations involving all aspects of the disaster recovery plan. Findings from these exercises are documented, and necessary adjustments are made to improve the plan's efficacy.

Section 10 References

Document No.	Document Title	Date	Author