Disaster Recovery Policy summary

v1 | 22-Apr-2025 | RAG

Excerpts from Pisys Disaster Recovery Policy for Data Centres 2.0

SECTION A. POLICY STATEMENT

Pisys is committed to maintaining a robust Disaster Recovery (DR) Plan for all our data centres to ensure the continuity of critical IT services and minimize the impact of disruptions on business operations. This policy outlines the framework for developing, implementing, maintaining, and testing a comprehensive disaster recovery strategy that aligns with the requirements of the ISO 27001 Information Security Management System (ISMS).

SECTION B. PURPOSE

The purpose of this policy is to provide a structured approach to:

- Protect the confidentiality, integrity, and availability of data and information assets.
- Minimize downtime and disruption to critical IT services in the event of a disaster or disaster scenario.
- Ensure that the data centre can recover to its pre-disaster state in a timely and controlled manner.
- Provide a foundation for compliance with legal, regulatory, and contractual requirements related to disaster recovery.

SECTION C. SCOPE

This policy applies to all data centres operated by Pisys and all associated information systems, data, and infrastructure. It also applies to third-party service providers that support Pisys' data centre operations.

Section D.3. DISASTER RECOVERY PLAN (DRP) DOCUMENTATION

The Pisys DRP is described in:

- Business Continuity Plan
- Data Breach Procedure
- Dealing with Security Incidents Procedure

SECTION F. NON-COMPLIANCE

Failure to adhere to this policy may result in disciplinary action, up to and including termination of employment or contract, as well as potential legal and financial repercussions for the organization.