Procedure PTPKM

Document Title: Disaster Recovery, Backups, and Business Continuity Plan (DRBCP)
Document Owner: Pusat Teknologi dan Pengurusan Kriptologi Malaysia (PTPKM)
Version: 1.0
Effective Date:
Next Review Date:

Introduction

The IT Department at Pusat Teknologi dan Pengurusan Kriptologi Malaysia (PTPKM) is responsible for managing and securing the organization's digital infrastructure. This includes ensuring system availability, safeguarding data, and responding to technical disruptions. As part of its role, the department oversees the Disaster Recovery, Backups, and Business Continuity Plan (DRBCP), which outlines step-by-step procedures to recover disrupted IT systems and networks. The plan aims to minimize operational impact by identifying critical assets, setting recovery priorities, and detailing actions for system restoration. It also includes key contacts, external support resources, and a clear sequence of recovery steps to ensure smooth and efficient resumption of services.

Purpose

This policy outlines the framework for disaster recovery, data backups, and business continuity to ensure the resilience and continued operation of essential services in the event of disruptions, natural disasters, cyberattacks, or other emergencies.

Scope

This policy applies to all employees who interact with or manage the organization's IT infrastructure, data, and critical business operations.

Definitions

- Disaster Recovery Plan (DRP): A plan to restore IT systems and data following a catastrophic event.

- Business Continuity Plan (BCP): Strategies to maintain critical operations during and after a disruption.
- Backup: A copy of data stored separately from the primary data to enable recovery.
- RTO (Recovery Time Objective): Maximum acceptable downtime.
- RPO (Recovery Point Objective): Maximum acceptable data loss.

Risks

- Inability to resume operations in a timely manner
- Loss of critical data and information
- Operational disruption and loss of stakeholder trust
- Financial losses and damage to organizational reputation

Roles and Responsibilities

- **IT Department:** Manage backups, implement DR solutions, maintain infrastructure.
- **DRP Supervisor:** Ensures that team members perform their assigned tasks during an incident.
- **Asset Manager:** Secure and protect critical assets when a disaster strikes.

Policy Statements

The following policies define how PTPKM will manage disaster recovery, backups, and business continuity:

Disaster Recovery

- PTPKM shall maintain a documented Disaster Recovery (DR) plan for all mission-critical IT systems.
- The DR plan shall include procedures for restoring systems, applications, and data following an incident.
- Disaster recovery capabilities must be tested at least once a year to ensure effectiveness.
- Alternate facilities, cloud recovery, or system redundancy shall be used where necessary.

Backups

- All critical data must be backed up regularly, according to data classification and sensitivity.
- Backup copies must be encrypted and stored off-site or in a secure cloud environment.
- Backup processes shall be monitored and verified regularly to ensure integrity and completeness.
- Restoration tests must be performed quarterly to confirm that backup data can be successfully recovered.

Business Continuity

- Each department shall maintain a business continuity plan identifying key functions, personnel, and dependencies.
- Continuity plans must be reviewed and updated annually or upon significant organizational or technological changes.
- Business continuity procedures shall be activated during prolonged outages or major incidents.
- PTPKM shall maintain a communication plan to notify stakeholders during disruptive events.

Compliance and Audit

Non-compliance with this policy may result in disciplinary action and jeopardize data integrity and organizational trust. Internal audits shall be conducted to assess compliance.

Approval

Name:
Title:
Signature:
Date: