Information Technology Disaster Recovery Policy

1. Purpose and Scope

This policy establishes the procedures and controls necessary to ensure the continuity of King's Own Institute's IT operations and services in the event of technical failures, cyber incidents, or disasters. The scope of this policy encompasses all IT staff, system administrators, and personnel involved in maintaining and recovering KOI's information technology infrastructure. As an integral component of KOI's overall Business Continuity Plan, this policy specifically focuses on IT systems and services critical to the institution's operations.

2. Related Documents

This Policy is to be read in conjunction with KOI's:

- Information Technology Disaster Recovery Plan
- Business Continuity Plan

3. Definitions

IT Disaster: Any event that causes disruption to IT services, including but not limited to cybersecurity incidents (such as ransomware, data breaches, and DDoS attacks), hardware failures, network outages, data corruption, system compromises, and power failures affecting IT infrastructure.

Recovery Time Objective (RTO): The targeted duration of time within which a business process or IT service must be restored after a disaster.

Recovery Point Objective (RPO): The maximum targeted period in which data might be lost due to a disaster.

Critical IT Systems: Core technology systems essential for KOI's operations, including the Student Management System, Learning Management System, email and communication systems, network infrastructure, and data storage systems.

GenAI-Related Incidents: Security events involving generative artificial intelligence tools, including but not limited to data exfiltration through AI platforms, AI-generated malicious code, deepfake attacks, or compromise of systems through AI-assisted social engineering.

4. Roles and Responsibilities

IT Disaster Recovery Manager

The IT Disaster Recovery Manager coordinates all IT disaster recovery efforts and maintains oversight of the recovery process. This role is responsible for maintaining and updating the IT disaster recovery plan, overseeing recovery testing and documentation, and reporting recovery status to senior management.

System Administrator

The System Administrator is responsible for monitoring system health and security, implementing backup and recovery procedures, executing recovery procedures for assigned systems, and documenting technical recovery processes.

Network Engineer

The Network Engineer maintain network redundancy and failover systems, implement network security measures, execute network recovery procedures, and monitor network performance and availability.

Database Administrator

The Database Administrator is tasked with maintaining database backup and recovery procedures, implementing data replication and redundancy, executing database recovery procedures, and monitoring database performance and integrity.

5. IT Disaster Recovery Team Structure

The IT Disaster Recovery Team consists of a Core Team and Extended Support network. The Core Team includes the IT Disaster Recovery Manager, System Administrator, Network Engineer, and Database Administrator. Extended Support encompasses relationships with Cloud Service Providers, Hardware Vendors, Software Vendors, and Cybersecurity Specialists.

6. Technical Recovery Procedures

6.1 System Classification and Recovery Priorities

Systems are classified into three priority levels based on their criticality to operations:

Priority 1 (Critical) systems require an RTO of 4 hours and RPO of 15 minutes. These systems include the Student Management System, Learning Management System, Authentication Services, and Core Network Infrastructure.

Priority 2 (High) systems operate with an RTO of 8 hours and RPO of 1 hour. This category encompasses Email Systems, File Storage, Intranet Services, and Database Services.

Priority 3 (Medium) systems maintain an RTO of 24 hours and RPO of 4 hours. These include Administrative Systems, Reporting Systems, and Development Environments.

GenAI platforms and AI-related services used by KOI should be classified based on their integration with critical systems and data access levels.

6.2 Technical Infrastructure Requirements

The institute maintains redundant systems including failover servers, redundant network paths, mirror storage systems, and backup power systems. The backup infrastructure consists of automated backup systems, off-site backup storage, cloud backup solutions, and backup verification procedures.

6.3 Recovery Procedures

The recovery process follows a structured approach beginning with Initial Response, during which teams assess system status, identify affected components, activate relevant recovery teams, and implement emergency response procedures.

System Recovery involves activating failover systems, restoring from backups, verifying system integrity, and testing system functionality.

Network Recovery encompasses implementing failover connections, restoring network services, verifying network security, and testing connectivity.

Data Recovery requires restoring from backup systems, verifying data integrity, implementing data synchronization, and validating data consistency.

7. Technical Testing and Maintenance

7.1 Testing Schedule

The institute implements a comprehensive testing schedule that includes weekly backup system tests, monthly failover system tests, quarterly full disaster recovery simulations, and annual comprehensive recovery plan tests.

7.2 Testing Types

Testing encompasses multiple areas of the IT infrastructure, including system failover tests, backup restoration tests, network redundancy tests, data recovery tests, and application recovery tests.

8. Technical Documentation Requirements

The institute maintains comprehensive technical documentation including system architecture diagrams, network topology maps, recovery procedure flowcharts, configuration documentation, vendor contact information, and system dependencies documentation.

9. Cybersecurity Considerations

Cybersecurity measures form an integral part of the disaster recovery strategy. These include the implementation of incident response procedures, regular security assessments, vulnerability management, access control protocols, security monitoring and logging, and encryption requirements.

9.1 GenAI Security Threats

The disaster recovery plan must account for emerging GenAI-related threats including: data exfiltration through unauthorised GenAI platform usage; AI-generated phishing and social engineering attacks; deepfake attacks targeting authentication systems; malicious code generation and deployment; and AI-assisted reconnaissance and system exploitation.

10. Technology Infrastructure Recovery

10.1 Infrastructure Components

The technology infrastructure recovery plan addresses servers and storage systems, network equipment, security systems, end-user computing resources, and cloud services.

10.2 Recovery Strategies

Recovery strategies encompass hardware replacement procedures, cloud failover implementation, virtual machine recovery, data restoration protocols, network reconfiguration procedures, procedures for identifying and containing AI-generated threats, protocols for validating authentic communications versus AI-generated content, and recovery procedures for systems compromised through GenAI-assisted attacks..

11. Compliance and Standards

The institute adheres to multiple compliance frameworks and standards including ISO 27001 Information Security Management, Australian Privacy Principles (APPs), Higher Education Standards Framework, and industry best practices for IT disaster recovery.

12. Review and Maintenance

This policy undergoes annual review, with quarterly procedure updates, monthly contact list updates, and continuous improvement processes to ensure its effectiveness and relevance.

Document Control

Policy title	Information Technology Disaster Recovery Policy
Policy owner	Director of IT
Policy approver	AIBM Council on the recommendation of the Academic Board
Policy version date	29 August 2025 Version 1.1
Date of approval	29 August 2025
Date of implementation	29 August 2025
Date of next review	29 August 2026
Changes in this version	Changes in this version include adding a new definition for "GenAI-Related Incidents" covering data exfiltration through AI platforms and AI-assisted attacks, incorporating GenAI security threats into cybersecurity considerations (such as AI-generated phishing, deepfake attacks, and malicious code), and establishing recovery procedures for systems compromised through GenAI-assisted attacks and protocols for validating authentic communications versus AI-generated content.