جامعة فهد بن سلطان
FAHAD BIN SULTAN UNIVERSITY

IT Risk Management and Disaster Recovery Policy

Policy Code:	IT-910-1
Policy Name:	IT Risk Management and Disaster Recovery Policy
Handler:	Computer Center
Date Created:	March 2025
Date of Current Review:	
Approved by:	Board of Trustees
Date of Approval:	May 7, 2025

1. Purpose

This policy establishes a comprehensive framework for identifying, assessing, managing, and mitigating information technology (IT) risks at Fahd Bin Sultan University (FBSU). It ensures the protection of IT assets, operational continuity, compliance with applicable legal, regulatory, and operational requirements, and alignment with FBSU's overarching Institutional Risk Management Policy (Policy Code: AD-040).

2. Scope

This policy applies to all university IT systems, networks, databases, cloud services, third-party services, and users (faculty, staff, students, contractors) interacting with FBSU's IT infrastructure.

3. Definitions

Term	Definition
IT Risk	Potential threat to confidentiality, integrity, or availability of information systems.
Disaster	Any event causing major disruption to IT services.
Disaster Recovery (DR)	Procedures to restore IT services following a disaster.
Risk Management	Identifying, assessing, mitigating, and monitoring IT-related risks.
Residual Risk	Risk remaining after mitigation efforts.
Risk Register	Record of risks, assessments, and mitigation actions.
Crisis	Severe IT event impacting university-wide operations.

4. Policy Statement

FBSU commits to a proactive approach to IT risk and disaster management. The University will identify, evaluate, and mitigate risks while maintaining robust disaster recovery procedures to restore operations swiftly after any disruption.

5. Roles and Responsibilities

- Director of Computer Center: Oversees IT risk management initiatives, maintains IT Risk Register, and ensures reporting to the Institutional Risk Management Committee.
- Information Security Officer (ISO): Manages operational cybersecurity risks and leads incident responses.
- University Legal Counsel: Reviews risk acknowledgment and acceptance decisions.
- Institutional Risk Management Committee: Reviews and oversees the IT risk management process.
- All Users: Follow security protocols and report IT-related risks or incidents.
- Crisis Management and Response Management Team (CMRMT): Coordinates IT crisis response efforts during critical incidents.

6. IT Risk Management Process

FBSU follows a structured IT risk management lifecycle:

6.1 Risk Identification

- Identify threats across Technical, Data, Human, Third-Party, and Natural Disaster categories.

6.2 Risk Assessment

Each risk is assessed based on:

- Likelihood Scale: Low (<20%), Medium (20-60%), High (>60%)
- Impact Scale: Low (minimal impact), Medium (manageable with existing resources), High (severe disruption)

Risks are plotted using a 3x3 matrix to calculate the Overall Risk Score:

	Likelihood		
Impact	Low	Medium	High
Low	1 (Low)	2 (Low)	3 (Low)
Medium	2 (Low)	4 (Medium)	6 (High)
High	3 (Low)	6 (High)	9 (High)

6-9 = High Risk (Immediate action)
3-4 = Medium Risk (Planned mitigation)
1-2 = Low Risk (Acceptable)

6.3 Risk Mitigation

- Develop and implement preventive, detective, and corrective controls.

6.4 Risk Acceptance

- When a risk cannot be fully mitigated, the IT Director, CISO, and University Legal Counsel must complete and approve a Risk Acknowledgment Form.

6.5 Monitoring and Continuous Improvement

- Utilize SIEM tools for monitoring.
- Conduct annual IT risk audits.
- Update mitigation strategies based on lessons learned.

6.6 Integration with Institutional Risk Register

- All IT risks must be reported and updated in the FBSU Risk Register and periodically reviewed.

7. Categories of IT Risks

- Technical Risks: System failures, outages, obsolescence.
- Data Risks: Loss, corruption, unauthorized access.
- Human Risks: Errors, negligence, insider threats.
- Third-Party Risks: Service disruption, vendor failures.
- Natural Disaster Risks: Floods, fires, earthquakes.

8. Crisis Management and Incident Response

In alignment with the FBSU Crisis Management Framework:

- Level 1: Minor IT incidents (handled internally)
- Level 2: Moderate incidents (potential escalation)
- Level 3: Major/Catastrophic events (involving CMRMT activation)

Incident response includes:

- Activation of Data Breach Response Plan (AA-405-F01).
- Notification to affected parties.
- Coordination with external authorities if necessary.

9. Risk Acceptance and Acknowledgment

When a risk is accepted without full mitigation, a Risk Acknowledgment Form (*Appendix 13.2*) must be completed and attached to the IT Risk Register for formal tracking and oversight.

When full mitigation is impractical or infeasible:

- Document risk acceptance formally.
- Secure approvals from the IT Director, CISO, and Legal Counsel.

- Maintain documentation for review by the Institutional Risk Management Committee.

10. Monitoring, Review, and Reporting

- Biennial Review: Comprehensive review of IT risk management practices.
- Incident Reporting: Immediate reporting of significant IT risks or incidents.
- Annual Update: Update risk register and reassess control measures.

Reports will be submitted to the Institutional Risk Management Committee and included in university-wide risk management assessments.

11. Disaster Recovery Procedures

11.1 Preparedness and Inventory

- Maintain updated inventory of all critical systems (e.g., LMS, HR, financial systems).

11.2 Backup Management

- Daily backups for critical data.
- Weekly full-system backups are stored securely.

11.3 Disaster Declaration and Response

- Declared by the Chief IT Officer after assessment.
- Activate the pre-assigned Disaster Recovery Team.
- Prioritize system restoration based on business impact.

11.4 Communication Plan

- Notify University management and stakeholders.
- Provide ongoing updates until full recovery.

11.5 Recovery Time Objective (RTO)

- Set RTO targets for critical services to minimize data loss and downtime.

12. Integration with Other Policies

This policy works in conjunction with:

- Institutional Risk Management Policy (AD-040)
- Data Breach Response Plan (Plan # AA-405-F01)

13. Appendices

13.1 IT Risk Register Template

Risk ID	Category	Description	Impact	Likelihood	Score	Action Plan	Residual Score	Responsible Owner

13.2 Risk Acknowledgment Form (Template)

Risk Acknowledgment Form

Risk ID: _____

Risk Description: _____

Reason for Acceptance: _____

Assessment (Likelihood and Impact): _____

Residual Risk Level: _____

Approved by:

IT Director: _____ Date: _____

Information Security Officer (ISO): _____ Date: _____

University Legal Counsel: _____ Date: _____

Comments (if any): _____

_____

_____

Signature and Date of Final Approval: _____