INFORMATION SECURITY BACKUP POLICY

Information Technology Department

Document ID	**ITSS-BKP-02**
Version Number:	**2.0**
Dated:	**10th JAN2025**

1. Purpose

It is essential for organizations to draft topic-specific policies that specifically address how they protect their network's relevant areas.

All business-critical data, software, and systems should have backup facilities in place to ensure they can be recovered following the below events:

- Business interruption.
- Failure of systems, applications or storage media.
- Data loss.
- Intrusion.

This policy ensures the integrity, availability, and confidentiality of the Iqra ERP application and its associated databases by implementing systematic and regular backup procedures for both the primary and secondary data centres, aligned with the requirements of ISO 27001.

2. Scope

This policy applies to all Iqra ERP systems and their corresponding databases deployed within the university.

3. Roles and Responsibilities

3.1. Data Center Team:

- Oversee the overall backup strategy and policy compliance.
- Implement and monitor backup processes for application and database servers at the VM level and database level for both primary and secondary data centers.
- Conduct periodic penetration testing of backup infrastructure for both sites.
- Maintain detailed audit logs of all backup and restore activities for both primary and secondary data centers.

3.2. Iqra Development Team:

- Manage and maintain code backups following a separate version control system.
- Assist with application-level backup procedures upon request from the Data Center Team.
- Perform restoration procedures from replicated backups at the DR site.

3.3. Management:

- Review and approve this policy periodically.
- Allocate necessary resources for backup infrastructure for both sites.

4. Backup Schedule

4.1. Primary DataCenter

4.1.1. VM Level Backups

- **Full Backups:** Weekly (Sundays at 0200 hrs)
- **Incremental Backups:** Daily (1500 hrs and 2300 hrs)

4.1.2. Database Level

- **Full Backups:** Weekly (Saturdays at 1000 hrs)
- **Incremental Backups:** Three times a day (0800 hrs, 1300 hrs, and 1800 hrs)
- **Transaction Log Backups:** Hourly

4.2. Secondary Data Center (DR Site)

- Database backups are replicated from the primary data center in real-time or with minimal lag.

4.2.1. DR Site Server and Services Backups:

- **Full Backups:** Saturdays at 1100 hrs
- **Incremental Backups:** One time a Day at 1100 hrs

5. Backup Types and Retention Period

Backup Type	Retention Period	Location
Primary Data Center		
Full Backups (Weekly)	6 Months	Onsite Storage
Full Backups (Monthly)	1 Year	Onsite Storage
Annual Backups	Indefinitely (or as per compliance regulations)	Onsite Storage
Incremental Backups	1 Month	Onsite Storage
Transaction Log Backups	1 Week	Onsite Storage
Secondary Data Center (DR)		
Database Backups (Replicated)	Align with Primary Data Center Retention	Onsite Storage (DR)
DR Site Server and Services Backups	Daily for Critical Systems	Primary Data Center Storage

6. Backup Locations

6.1. Primary Data Center:

- Primary backup for all university data (applications, databases, etc.)
- Backup storage for DR Site server and services.

6.2. Secondary Data Center (Gulshan DC):

- Replicated database backups from the primary data center.

6.3. Third Storage (Offline External Backup):

- A separate detachable drive is used for additional redundancy for critical data.

- This external drive will be in custody of System Administrator who will be responsible for the secure handling of the data.

7. Safe Custody Measures

7.1. Physical Security:

- External backup drives are kept in a locked, access-controlled cabinet when not in use.
- Storage area is monitored by security systems (e.g., cameras, alarms).

7.2. Environmental Controls:

- External backup drives are kept in a climate-controlled environment to prevent damage from humidity or extreme temperatures.
- Use fireproof and waterproof safes for additional protection of critical backups.

7.3. Access Control:

- Access to external drives is limited to authorize personnel only.
- Access log documenting who accesses the backup drives and for what purpose.

8. Backup Verification

- The Data Center Team will conduct regular verification procedures for both primary and DR sites to ensure:
    - Integrity of backup software and hardware.
    - Sufficient storage space availability.
    - Backup data integrity through test restores.
- Quarterly restore tests will be conducted at both, primary and DR sites to validate backup functionality.

9. Security Measures

- Limited access to backup data and infrastructure to authorized personnel only (applicable to both, primary and DR sites).
- Maintained comprehensive audit logs of all backup and restore activities for both sites for tracking and accountability.
- Consider encrypting backups at rest and in transit for additional security.
- Regularly reviewal and update security measures based on industry best practices, identified vulnerabilities, and evolving ISO 27001 requirements.