MRC Mycetoma Research Center
WHO Collaborating Center on Mycetoma
Excellence and Leadership

www.mycetoma.edu.sd
info@mycetoma.edu.sd

Managing Access and Security of Research Data Policy Document

Background

This document outlines the policy for managing access to and ensuring the security of research data at the Mycetoma Research Center, University of Khartoum. This includes protocols for handling personal and confidential data, as well as measures in place to prevent cyber attacks. The Mycetoma Research Center is committed to protecting the integrity and confidentiality of research data. This policy serves as a framework for managing access, ensuring security, and preventing cyber attacks.

Scope

This policy applies to all staff, researchers, students, and collaborators who handle research data within the organisation.

1. Data Classification

Research data will be classified into the following categories:

1. **Public Data:** Data and information that can be freely shared without restrictions.
2. **Confidential Data:** Sensitive data and information that requires protection (e.g., personal data, proprietary research).
3. **Restricted Data:** Highly sensitive data and information that is subject to legal or ethical restrictions.

2. Access Management

User Authentication

Access Control

All users must authenticate their identity using university-issued credentials. Multi-factor authentication (MFA) is required to access sensitive data.

Role-Based Access

Access to data will be granted based on the user's role and necessity. Only authorised personnel will have access to confidential and restricted data.

3. Data Access Logs

Monitoring

Access to research data will be logged and monitored. Regular audits will be conducted to ensure compliance with access policies.

Incident Reporting

Any unauthorised access attempts must be reported immediately to the IT department.

4. Data Security Measures

A. Encryption

Data Encryption

All confidential and restricted data must be encrypted both in transit and at rest.

B. Secure Storage

Data will be stored on secure servers with access restrictions.

5. Backup Procedures

Regular Backups

Daily backups of all critical research data will be performed and stored securely.

Disaster Recovery

A disaster recovery plan will be maintained to restore data in case of loss or corruption.

6. Cybersecurity Training

Staff Training

All staff and researchers will undergo mandatory cybersecurity training annually. This training will cover data protection best practices and how to recognise potential cyber threats.

7. Cyber Attack Prevention

A. Firewalls and Intrusion Detection

Network Security

- Firewalls will be implemented to protect the organisation’s network. Intrusion detection systems will be in place to monitor for suspicious activities.

B. Regular Security Assessments

Vulnerability Assessments

- Regular security assessments will be conducted to identify potential vulnerabilities in systems and processes.

C. Penetration Testing

- Annual penetration testing will be performed to assess the effectiveness of security measures.

8. Incident Response Plan

Response Protocols

An incident response plan is in place for addressing data breaches or cyber incidents. This plan will outline roles, responsibilities, and communication strategies during a security incident.

9. Compliance and Review

Regulatory Compliance

The Mycetoma Research Center will comply with all applicable laws and regulations regarding data protection and privacy.

Policy Review

This policy will be reviewed annually and updated as necessary to adapt to changing security landscapes and regulatory requirements.

Approved by

Fahal

Prof Ahmed Hassan Fahal
MBBS, FRCS, FRCSI, FRCS(Gal), MD, MS, FRCPath, FRCP(London)

Director

Mycetoma Research Center, University of Khartoum
15th April 2015
Updated on 15th March 2024