School of Business and Management Data Protection and IT Security Policy

1. Introduction

The School of Business and Management is committed to maintaining the confidentiality, integrity, and availability of all data, while ensuring compliance with relevant data protection laws and best practices. This policy outlines the procedures for the creation, management, and deletion of staff accounts, enforces restrictions on remote work, and establishes protocols for handling data breaches.

2. Staff Accounts Creation, Management, and Deletion

2.1 Creation of Staff Accounts

New staff accounts will be created by the IT department upon request from the HR department. The request should include the necessary information for account setup, such as the employee's name, position, and department. Access permissions will be granted based on the principle of least privilege.

2.2 Management of Staff Accounts

Ongoing management of staff accounts will be the responsibility of the IT department. This includes updates to access permissions based on changes in job roles, promotions, or other relevant factors. Requests for modifications should be submitted through the appropriate channels and will be processed in a timely manner.

2.3 Deletion of Staff Accounts

Staff accounts will be promptly deactivated upon termination of employment or any other circumstance that requires account removal. The HR department is responsible for notifying the IT department of employee departures or changes in job roles that necessitate account deletion.

3. Remote Work Policy and Technical Controls

3.1 Remote Work Restrictions

For security reasons, staff members are not permitted to work from home unless explicit authorization is granted by the IT department and is in compliance with the organization's remote work policy. Remote work requests must be submitted in advance and are subject to review and approval.

SBM Data Protection and IT Security Policy

- Version:2.24
- Issue date: 13th February 2024
- Review date: 13th February 2027

3.2 Technical Controls

To enforce the remote work policy, technical controls will be implemented. This includes secure VPN connections, multi-factor authentication, and monitoring tools to ensure compliance. Any unauthorized attempts to access the network remotely will be flagged and addressed immediately.

4. Data Breach Handling Policy

4.1 Definition of Data Breach

A data breach is defined as the unauthorized access, acquisition, disclosure, or destruction of sensitive information that compromises the confidentiality, integrity, or availability of such data.

4.2 Reporting Procedure

In the event of a suspected or confirmed data breach, staff members are required to report the incident immediately to the IT department. The IT department will then conduct an investigation and take necessary actions to mitigate the impact.

4.3 Notification Protocol

If the breach involves personal data and is likely to result in a high risk to the rights and freedoms of individuals, affected parties will be promptly notified as required by applicable data protection laws.

5. Review and Update

This policy will be regularly reviewed and updated by the IT department to ensure its effectiveness and compliance with evolving data protection and IT security standards.

By adhering to this policy, the School of Business and Management aims to create a secure and compliant digital environment for its staff and stakeholders.

SBM Data Protection and IT Security Policy

- Version:2.24
- Issue date: 13th February 2024
- Review date: 13th February 2027