Password and Access Control Security Measures - School of Business and Management

1. Authentication into Microsoft 365:

1.1 User Identification:

Students and staff authenticate into Microsoft 365 using unique usernames that are assigned based on their roles and affiliations with the School of Business and Management (SBM).

1.2 Password Complexity:

Strong password policies are enforced, requiring users to create complex passwords that include a combination of uppercase and lowercase letters, numbers, and special characters.

1.3 Password Expiry and Renewal:

Passwords have a predefined expiration period, and users are prompted to change their passwords regularly to enhance security.

1.4 Account Lockout Policies:

Account lockout policies are in place to mitigate the risk of unauthorized access due to multiple unsuccessful login attempts. After a specified number of failed attempts, the account is temporarily locked.

2. Azure Active Directory (Azure AD) and Multi-Factor Authentication (MFA):

2.1 Azure AD Integration:

SBM utilizes Azure Active Directory (Azure AD) as the identity and access management service for Microsoft 365 accounts. This ensures centralized user identity management and enhances security.

2.2 Multi-Factor Authentication (MFA):

Multi-Factor Authentication (MFA) is implemented to add an extra layer of security during the login process. Users are required to authenticate their identity through a secondary method, such as a mobile app, phone call, or text message.

2.3 Conditional Access Policies:

Conditional Access policies are configured in Azure AD to define specific conditions under which access is granted. This includes factors such as user location, device compliance, and the strength of authentication methods used.

3. Desktop PC Authentication:

SBM Password and Access Control Security Measures

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

3.1 Windows Authentication:

Desktop PCs within SBM are integrated with Azure AD for Windows authentication. Users log in using their Microsoft 365 credentials, providing a seamless and secure login experience.

3.2 Single Sign-On (SSO):

Single Sign-On is implemented to allow users to access multiple applications, including desktop PCs, after signing in once with their Microsoft 365 credentials.

3.3 Group Policy Controls:

Group Policy controls are configured to enforce security settings on desktop PCs, including password complexity requirements, screen lock policies, and other access controls.

4. Security Awareness Training:

4.1 User Education:

Students and staff receive regular security awareness training to educate them on the importance of strong passwords, secure authentication practices, and the significance of MFA.

4.2 Phishing Awareness:

Specialized training on recognizing and avoiding phishing attempts is provided to prevent unauthorized access due to social engineering attacks.

5. Continuous Monitoring and Improvement:

5.1 Security Audits:

Regular security audits and monitoring activities are conducted to identify and address any potential vulnerabilities or unauthorized access attempts.

5.2 Policy Review and Update:

Access control policies are subject to periodic reviews to align with industry best practices, technological advancements, and evolving security threats.

By implementing these comprehensive security measures, SBM aims to ensure robust protection for both student and staff accounts, enhancing the overall security posture of its information systems.