Data Protection of CRM System Policy Enforcement Framework - School of Business and Management

1. Technical Controls:

1.1 Access Controls:

Role-based access controls are implemented to ensure that only authorized personnel have access to the CRM system. Access permissions are regularly reviewed and updated in accordance with staff roles and responsibilities.

1.2 Encryption:

All data within the CRM system, both in transit and at rest, is encrypted to safeguard against unauthorized access and protect sensitive information.

1.3 Audit Trails:

Robust audit trails are maintained to log and monitor user activities within the CRM system. This ensures accountability, traceability, and early detection of any suspicious or unauthorized activities.

1.4 Multi-Factor Authentication (MFA):

MFA is enforced to add an additional layer of security, requiring users to authenticate their identity through multiple verification methods before gaining access to the CRM system.

2. Policy Controls:

2.1 Data Classification and Handling:

Clear data classification policies are in place to categorize data based on its sensitivity. This classification determines the level of access, storage, and protection measures applied to each type of data within the CRM system.

2.2 User Training and Awareness:

Regular staff training sessions are conducted to ensure that all users are aware of data protection policies and best practices. This includes training on the appropriate use of CRM data and the consequences of non-compliance.

2.3 Incident Response Plan:

An incident response plan is established, outlining the procedures to be followed in the event of a security incident or data breach within the CRM system. This plan includes steps for containment, eradication, and recovery.

SBM DATA PROTECTION OF CRM SYSTEM POLICY

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

3. Process Controls:

3.1 Change Management:

A formalized change management process is in place to assess and implement any changes or updates to the CRM system. This includes testing procedures to ensure that changes do not compromise data security.

3.2 Regular Audits and Assessments:

Periodic internal and external audits are conducted to assess the effectiveness of data protection controls within the CRM system. Vulnerability assessments and penetration testing are also performed to identify and address potential security risks.

3.3 Policy Review and Update:

The data protection policy for the CRM system is subject to regular reviews to align with evolving technology, compliance requirements, and organizational changes. Updates are made to the policy as needed.

4. Continuous Improvement:

4.1 Feedback Mechanism:

A feedback mechanism is established to encourage users to report any concerns or potential policy violations. This helps in continuous improvement and the refinement of controls.

4.2 Training Program Evaluation:

The effectiveness of the staff training program is regularly evaluated, and adjustments are made to address emerging data protection challenges and enhance user awareness.

By implementing a comprehensive framework of technical, policy, and process controls, the School of Business and Management ensures the consistent enforcement of the Data Protection of CRM System Policy.