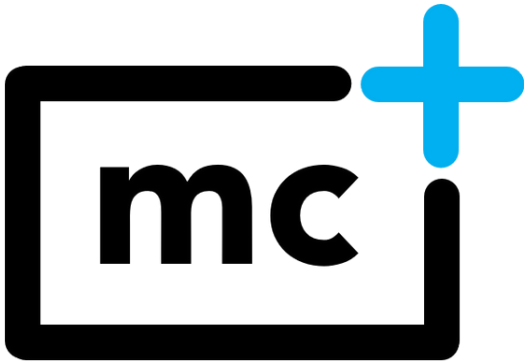

End-User Computing (EUC) Policy

Purpose

The purpose of this policy is to establish guidelines for the use of end-user computing devices and applications within Economic Capital Solutions Ltd. This policy aims to ensure the security, integrity, and confidentiality of data and systems.

Scope

This policy applies to all employees, contractors, and other personnel who use company-owned or personal devices to access company data and systems.

Policy

Employees are responsible for using end-user computing devices and applications in a manner that protects company data and systems. This includes adhering to security protocols, maintaining data integrity, and ensuring compliance with relevant laws and regulations.

Device Management and Security

All devices used for work purposes must have up-to-date security software, including antivirus and firewall protection. Devices must be encrypted to protect sensitive data. Remote monitoring and tracking of devices should be enabled to ensure security and compliance.

Password and Authentication Policies:

Employees must use strong passwords that include a combination of letters, numbers, and special characters. Passwords must be changed regularly. Multi-factor authentication (MFA) should be implemented to add an extra layer of security.

Data Access and Sharing:

Access to company data should be based on job roles and responsibilities. Employees should only access data necessary for their job functions. Data sharing should be limited to authorized channels and secure methods.

Data Backup and Recovery

A reliable data backup strategy should be in place to ensure critical information is regularly backed up to secure servers or the cloud. Regular testing of the recovery process should be conducted to ensure smooth functioning in case of data loss.

Employee Training and Awareness

Employees should receive regular training on the EUC policy and the importance of data security. Training should cover recognizing potential threats and avoiding phishing scams or other social engineering attacks.

Compliance and Enforcement

Employees must comply with this policy at all times. Violations of this policy may result in disciplinary action, up to and including termination.

Policy Review and Update

This policy should be reviewed and updated regularly to ensure it remains relevant and effective.