CASH MONEY

INVESTMENTS

Password Policy

Employees must use strong, unique passwords for all systems and accounts related to the organisation. Passwords must be changed every 90 days, and employees must not share their passwords with anyone.

Data Encryption Policy

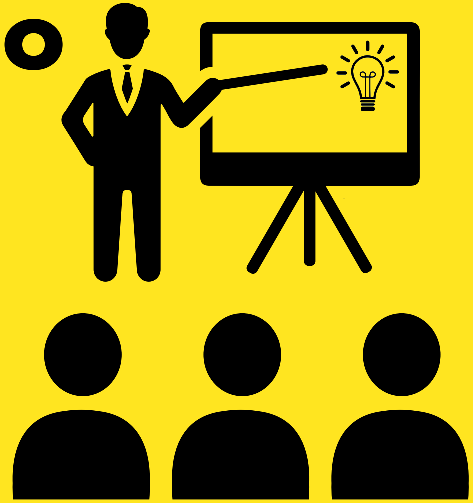
All sensitive data, including financial information and personal data, must be encrypted both in transit and at rest. This includes data stored on servers, laptops, and other devices.

Network Security Policy:

The organisation must implement a firewall to protect against unauthorized access and malware. All incoming and outgoing network traffic must be monitored for suspicious activity.

Training and Awareness Policy:

Employees must receive regular training on cybersecurity best practices, including how to identify and report suspicious activity. All employees must also be made aware of the organization's cybersecurity policies and procedures.



Physical Security Policy

The organisation must implement physical security measures to protect against unauthorized access to its facilities and data centers. This includes measures such as security cameras, security personnel, and access controls.

Constantly save and secure data

To ensure the security of data in case of an emergency. All data should be saved on the company cloud.

Constantly save and secure data

Software and firmware must be constantly updated, to avoid issues and problems with the systems

Constantly save and secure data

All activities on the internet shall be monitored by our organization