INFORMATION SECURITY POLICY

Purpose

This Policy is intended to protect information inside a secure environment that belongs to Synergy Pay Solutions and its stakeholders (third parties, customers or customers and the general public).

This policy apprises Group personnel, in all positions, all divisions within the Company, and all controlled legal entities authorized to utilize Group facilities of the rules governing the retention, use, and disposal of information.

It is the aim of the Group that:

- Information shall be safeguarded against illegal access or exploitation.
- Information confidentiality will be maintained.
- Informational integrity will be protected.
- Information and information systems are made available for service delivery.
- Processes for business continuity planning will be maintained.
- Compliance with regulatory, contractual, and legal standards is ensured.
- Security will be maintained across the physical, logical, environmental, and communications domains.
- A violation of this policy may result in administrative sanctions or criminal prosecution.
- Information that is no longer useful is discarded in an appropriate manner.
- All incidents involving information security will be reported to the Director of Information and Communication Technology (ICT) Systems and examined via the appropriate management channel.

The data pertains to:

- Electronic information systems (software, computers, and peripherals) owned by the Group, regardless of whether they are deployed or accessed off-site.

- Utilization of the Group's computer network directly or indirectly.

- Hardware, software, and data that are Group-owned.

The Policy

The Group imposes a responsibility of care on all users regarding the operation and use of its information systems.

a. Authorized information system users

With the exception of information made available to the public, all users of Group information systems must be legally authorized by appointment as staff members. Each authorized user will have a unique identifier. It is improper to disclose any password connected with a user identity to a third party.

Authorized users will take reasonable precautions to safeguard Group information in their control. The following factors must be considered before copying or transporting confidential, personal, or private information:

• Permission from the data owner

• The dangers connected with loss or unauthorized access

• How the data will be protected during transport and at its final destination.

b. Owners of Information Systems

Heads/Directors responsible for information systems must ensure the following:

1. Systems are sufficiently safeguarded against unwanted access.

2. Systems are safeguarded against theft and damage in a cost-effective manner.

3. Appropriate measures are made to ensure the information system's availability, commensurate with its significance (Business Continuity).

4. The ability to retrieve electronic data in the event of loss of the primary source. I.e. the breakdown or loss of a computer system. All system owners must back up their data and be able to restore it to a level commensurate with its significance (Disaster Recovery).

5. Data is preserved with a high level of precision.

6. Systems are used for their intended purpose, and there are procedures in place to correct any misuse that is identified or reported.

7. To ensure compliance with the data protection, investigatory powers, and freedom of information acts, electronic access logs are only kept for a reasonable period of time.

8. Any third parties entrusted with Group data are aware of their duties for ensuring the data's security.

c. Individual Information

Regarding their usage of Group information systems, authorized users of information systems are not granted with any privacy rights. Group officers with the right authorization can access or monitor any group information system containing personal data (mailboxes, web access logs, file stores, etc.).

d. Individuals who violate this policy are subject to regulatory actions at the direction of the Director with responsibility for the relevant information system, including, if needed, referral to the Police.

The Group will pursue legal action to prevent unauthorized access to its information systems.

Ownership

The Director of ICT Systems is directly responsible for maintaining and advising on the execution of this policy.

Owners of information systems are responsible for implementing and ensuring compliance with this policy in their respective areas.