Security Trainings and Awareness Policy

1. Document Owner and Approval:

This policy is owned by the Security Department, and approval for its implementation was granted by the Chief Information Security Officer (CISO).

2. Scope:

This policy applies to all employees, contractors, consultants, temporary and other workers, who have access to the company's private or personal data, the company's network, or devices owned or controlled by the company.

3. Responsibilities:

• The CISO is responsible for overseeing the implementation of the training and awareness policy. This includes:

> Ensuring that training programs align with industry best practices and regulatory requirements.
>
> Allocating resources for the development and delivery of training materials.
>
> Collaborating with department heads and stakeholders to address any security concerns or training needs.

• The GPC team is primarily responsible for the development of the Security Training and Awareness Policy. Their responsibilities include:

> Collaborating with stakeholders to assess training needs and requirements.
>
> Designing comprehensive training programs that cover security policies, procedures, and best practices.
>
> Developing training materials, including presentations, e-learning modules, and quizzes.
>
> Ensuring that training content aligns with industry standards, regulatory requirements, and organizational goals.
>
> Incorporating feedback from employees, managers, and security experts to continuously improve training effectiveness.
>
> Working closely with all departments to coordinate training schedules and logistics.

Regularly reviewing and updating the Security Training and Awareness Policy to address emerging threats and changes in technology.

• Managers are responsible for ensuring that their staff and other workers within their remit participate in the information security awareness, training and educational activities where appropriate.

• Workers are personally accountable for compliance with applicable legal, regulatory and contractual obligations, and conformity with policies at all times.

4. Policy:

All employees of the company must be aware of their responsibilities in protecting the data, devices and network of the company.

To help with this, the company give training to all staff members before and during their time using company devices and networks. When new staff join, they'll get a quiz to find out what they already know about security. Then, they'll have training that's personalized to focus on the areas they need help with the most.Training will be in the form of online training courses. These courses will be sent out by email and accessed from the company email inbox.

All employees are required to undergo an annual quiz to assess their understanding of security concepts and practices. If an employee fails to pass the quiz, they will be required to retake the corresponding training course to reinforce their knowledge. Staff need to finish each training course within 20 working days.

The training will cover important security topics like:

- using email and the internet safely
- spotting phishing emails
- understanding social engineering tricks
- dealing with malware, adware, spyware, and ransomware
- staying secure while working from different locations
- keeping physical areas secure
- managing passwords safely
- using social media securely
- recognizing voice and text phishing attempts.

If a staff member doesn't get a training email or if they have any problems with their training, they should contact the IT support team right away.

5.Enforcement:

If employees don't follow the training rules, it can result in disciplinary action, up to and including termination of employment. Regular audits will be conducted to monitor compliance, and non-compliance will be addressed promptly.