Information Security Steering Group: Terms of Reference

Classification: **Internal**

This document may only be shared internally without prior confirmation from the owner.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Version | Approved By | Owner | Date Last Updated | Review Frequency | Next Review | Comments |
|  |  |  |  |  |  |  |

# Introduction

This document outlines the scope, objectives, membership, and governance of the Information Security Steering Group (ISSG) for [Company Name].

# Purpose

The ISSG is responsible for overseeing and advising on the organisation's information security strategy and practices in alignment with its business objectives.

# Objectives

* Provide strategic direction for information security initiatives.
* Prioritise information security projects and resource allocation.
* Ensure compliance with legal and regulatory requirements.
* Facilitate communication between stakeholders.
* Periodically review and assess the effectiveness of security measures.

# Membership

* Chief Operational Officer (Chair)
* IT Director
* Legal Counsel
* Product Director
* Data Director
* Representative from HR
* Representative from Finance

# Meetings

* Monthly general meetings
* Quarterly strategic reviews
* Annual evaluation and planning

# Responsibilities

* Develop an annual Information Security Strategy.
* Review and approve information security policies and procedures.
* Monitor security incidents and responses.
* Approve budgets for security projects.

# Standing Agenda

## Monthly Activities:

* **Opening Remarks**: Brief recap of security status.
* **Monitoring & KPIs review**
  + **Incident Report Review**: Discuss any security incidents and responses.
  + **Risk Review**: Summarise any new or updated risks the group monitors.
  + **KPI & Metrics Review**: Review report on KPIs and ISMS Metrics
* **Project Updates**: Update on ongoing and upcoming security projects.
* **Compliance Review**: Updates on legal and regulatory compliance.
* **Resource Allocation**: Discuss needs and priorities.
* **Any Other Business**: Open floor for other concerns.

## Quarterly Activities:

* **Strategic Review**: Assess the status of key initiatives from the Information Security Strategy.
* **Risk Assessment**: High-level overview of emerging risks and vulnerabilities.
* **Budget Review**: Assess budget utilisation and future allocation.
* **External Audit Summary**: Presentation of external audit findings, if any.

## Annual Activities:

* **Annual Evaluation**: Evaluate the year's accomplishments, failures, and areas for improvement.
* **Strategic Planning**: Update the Information Security Strategy for the following year.
* **Annual Compliance Review**: Detailed compliance assessment.
* **Membership Review**: Consideration for adding or removing members.