INSERT LOGO

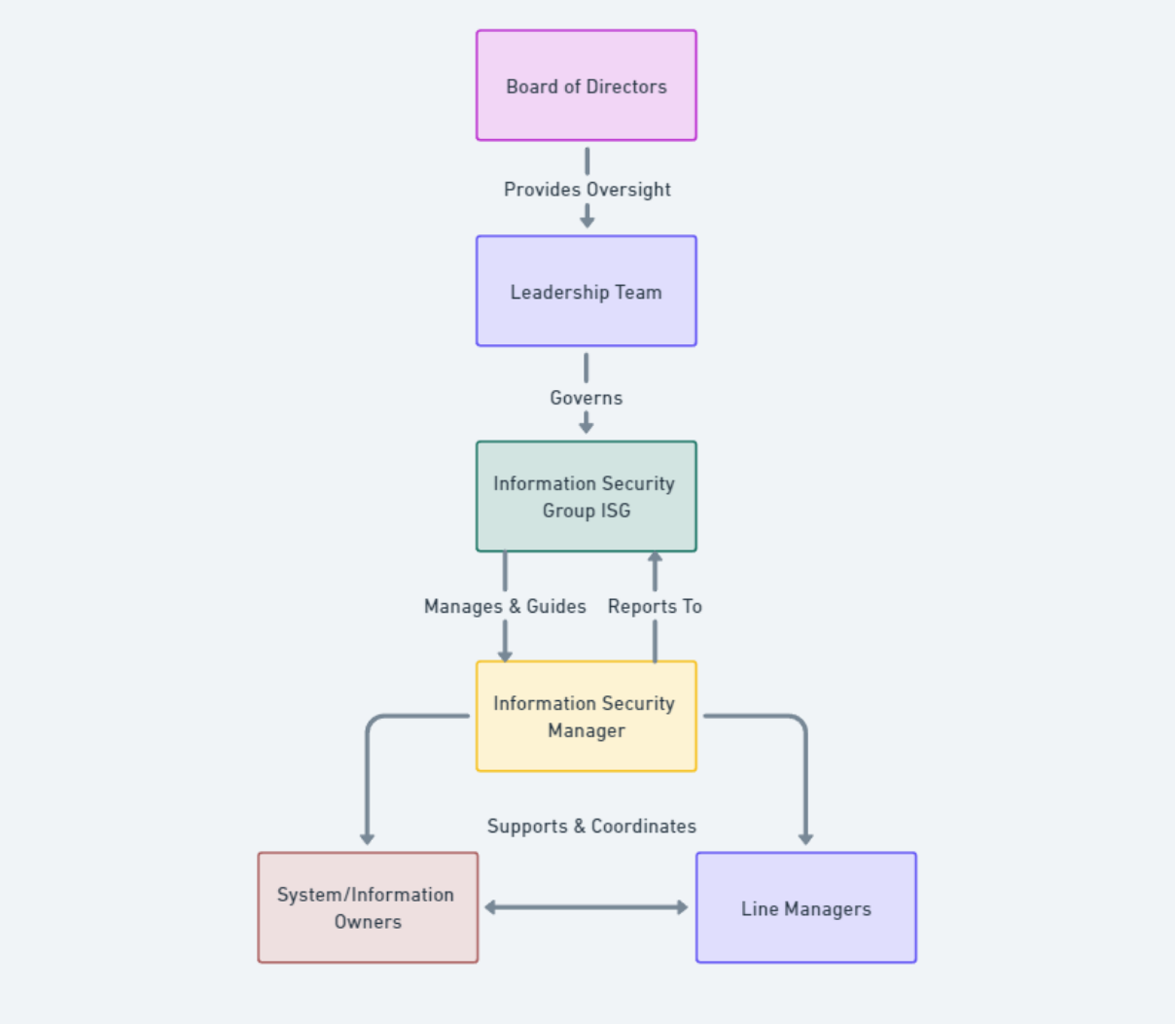
ISMS ROLES & RESPONSIBILITIES

Classification: **Public**

This document may be shared with interested parties outside of [Company Name]

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

Contents



Introduction

Purpose

This document defines and details the Information Security Management System (ISMS) roles and responsibilities within [Company Name]. It ensures all employees understand their duties and are accountable for maintaining and enhancing the organisation's security posture.

Scope

This document applies to all employees, contractors, and third-party vendors involved in managing, implementing, and maintaining the ISMS at [Company Name].

Key Roles and Responsibilities

Information Security Group (ISG)

- **Approve and Oversee Security Policy:**

  - Approve the organisation's security policies and ensure they align with business objectives.

- **Manage the ISMS Framework:**
  - Develop, implement, and maintain the ISMS framework per ISO 27001 standards.
- **Guide and Support Security Efforts:**
  - Provide strategic direction and support for security initiatives and projects within [Company Name].

Information Security Manager

- **Manage the ISMS:**
  - Oversee the day-to-day operations of the ISMS, ensuring it is effectively implemented and maintained.
- **Handle Security Risk Assessments:**
  - Conduct regular security risk assessments to identify and mitigate potential organisational threats.
- **Ensure Adherence to the ISMS:**
  - Monitor compliance with the ISMS policies and procedures and enforce corrective actions as necessary.

System / Information Owners

- **Manage Security Risks:**
  - Identify, evaluate, and manage security risks within their specific areas of responsibility.
- **Support the Information Security Manager:**
  - Collaborate with the Information Security Manager to implement and maintain security measures.
- **Ensure Compliance:**
  - Ensure compliance with data protection procedures and policies within their respective domains.

Line Managers

- **Grant Access Based on Role Needs:**
  - Authorise access to systems and information based on the principle of least privilege.
- **Ensure Policy Compliance:**
  - Ensure that team members adhere to the organisation's security policies and procedures.
- **Manage Access and Return of Devices:**

- Oversee the issuance, use, and return of [Company Name] devices and systems.

All Staff

- **Comply with Policies and Procedures:**
  - Follow all security policies and procedures as outlined by the ISMS.
- **Report Policy Breaches:**
  - Promptly report any security incidents or breaches to the appropriate authority.
- **Seek Exceptions via IT Helpdesk:**
  - Request any necessary exceptions to security policies through the IT Helpdesk.

Responsibility Assignment Matrix (RACI)

Activity	Information Security Group	Information Security Manager	System/Information Owners	Line Managers	All Staff
Approve Security Policies	A	R	C	I	I
Oversee ISMS Framework	A	R	C	I	I
Conduct Risk Assessments	C	R	A	I	I
Ensure ISMS Compliance	C	A	R	I	I
Manage Security Risks	C	A	R	I	I
Grant Access	I	I	R	R	I
Report Policy Breaches	I	I	I	I	R
Seek Policy Exceptions	I	I	I	I	R
Develop and Maintain Security Policies	A	R	C	I	I
Security Awareness Training	A	R	C	C	I

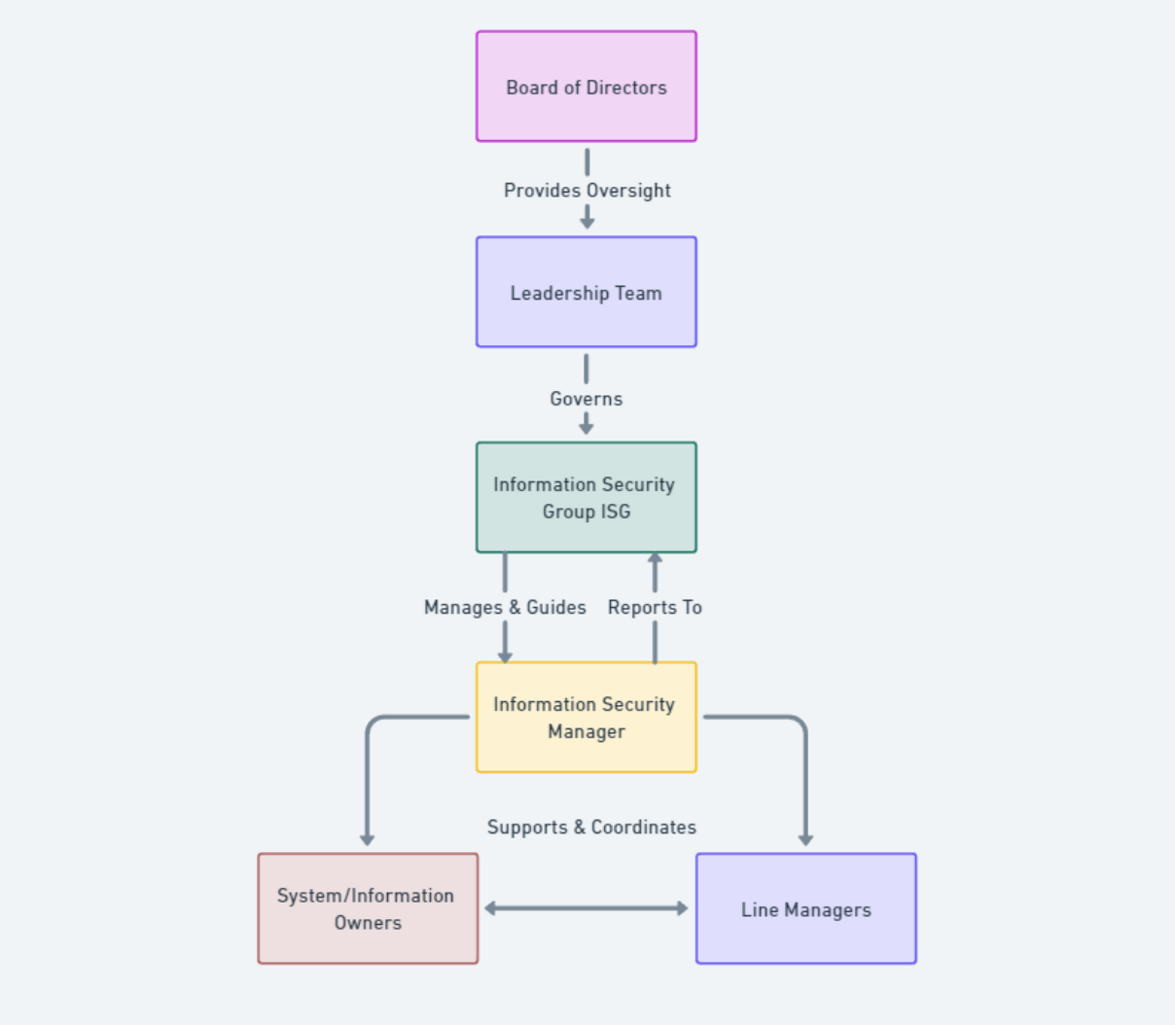
Incident Response and Management	A	R	C	I	I
Access Review and Audit	C	A	R	C	I
Third-Party Risk Management	A	R	C	I	I
Security Metrics and Reporting	A	R	C	I	I
Data Protection and Privacy Compliance	A	R	C	I	I
Oversee ISMS Framework	A	R	C	I	I
Conduct Risk Assessments	C	R	A	I	I
Ensure ISMS Compliance	C	A	R	I	I
Manage Security Risks	C	A	R	I	I
Grant Access	I	I	R	R	I
Report Policy Breaches	I	I	I	I	R
Seek Policy Exceptions	I	I	I	I	R
Develop and Maintain Security Policies	A	R	C	I	I
Security Awareness Training	A	R	C	C	I
Incident Response and Management	A	R	C	I	I
Access Review and Audit	C	A	R	C	I

Third-Party Risk Management	A	R	C	I	I
Security Metrics and Reporting	A	R	C	I	I
Data Protection and Privacy Compliance	A	R	C	I	I

Legend:

- **R** = Responsible
- **A** = Accountable
- **C** = Consulted
- **I** = Informed

Organisational Chart



Integration with Policies and Procedures

This document should be read in conjunction with the relevant policies and procedures within the ISMS. Each policy and procedure will provide more detailed responsibilities for the activities covered.