Almarys

Information Technology & Security

Governance Policy

TABLE OF CONTENTS

Introduction

At Almarys, we uphold the highest standards in managing our information and technology environment. We adopt and comply with the ER Group's Information Technology (IT) and Information Security (IS) policies that govern how we use technology, protect data, mitigate risks, and ensure business continuity. These policies are consistent with local and international standards, regulatory requirements, and corporate governance best practices.

The policies are developed and maintained under the oversight of the Group's Information Technology and Security functions, approved by the Board of Directors, and reviewed annually to ensure alignment with strategic objectives and stakeholder expectations. Almarys applies these policies fully within its operations, tailoring implementation to its specific business needs while maintaining compliance with Group requirements.

Summary of Almarys' Information Technology and Security Related Policies

Almarys follows a comprehensive suite of Information Technology (IT) and Information Security (IS) policies designed to ensure the secure, reliable, and efficient use of technology. These policies form a critical part of our corporate governance framework, ensuring that technology supports our business objectives while safeguarding the confidentiality, integrity, and availability of information.

In line with the Data Protection Act, applicable sectoral regulations, and internationally recognised standards such as ISO 27001 and the NIST Cybersecurity Framework, Almarys takes a proactive approach to managing IT and security risks. All employees share the responsibility for protecting the company's information assets, and compliance with these policies is embedded in their contractual obligations.

The IT and Security policies address key areas including:

- Governance and management of IT systems and infrastructure
- Logical and physical access control
- Data classification, storage, transmission, and disposal
- Secure management of IT assets and resources
- Incident detection, reporting, and response
- Business continuity and disaster recovery preparedness
- Vendor and third-party security management
- Responsible use of artificial intelligence and emerging technologies
- Protection against cyber threats through layered security controls

To ensure these policies remain effective and relevant, Almarys reviews and updates them regularly to reflect evolving threats, regulatory changes, and technological advancements. They are accessible to all employees via the company intranet and supported by regular training programmes, awareness campaigns, and e-learning modules to strengthen understanding and promote compliance.

Independent assurance is provided by the Group’s Compliance and Internal Audit functions, which conduct regular reviews to assess the effectiveness of controls. Findings are reported to Almarys’ Senior Management and the Group’s oversight committees, with remedial actions tracked through established governance channels.

Through these policies and governance arrangements, Almarys demonstrates its commitment to protecting information assets, ensuring technology resilience, and maintaining the trust of its customers, partners, and stakeholders.

Governance Disclaimer

This summary provides a high-level overview of Almarys’ Information Technology and Security policies, which are based on the Group’s governance framework. It does not replace the full policies, which contain detailed requirements and procedures. Employees are expected to refer to the official documents on the company intranet and comply with all applicable provisions. Non-compliance may result in disciplinary action in line with the Group’s governance requirements.