Information Technology & Security

Governance Policy

TABLE OF CONTENTS

1. Introduction

At ER Group, we uphold the highest standards in managing our information and technology environment. Our Group wide IT and Information Security policies govern how we use technology, protect data, mitigate risks, and ensure business continuity while aligning with local and international standards, regulatory requirements, and corporate governance best practices.

These policies are developed and maintained under the oversight of ER Group's Information Technology and Security functions, approved by the Board of Directors, and reviewed annually to ensure alignment with our strategic objectives and stakeholder expectations.

2. Summary of ER Group's Information Technology and Security Related Policies

ER Group has established a comprehensive suite of Information Technology (IT) and Information Security (IS) policies to ensure the secure, reliable, and efficient use of technology across all subsidiaries. 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, the NIST Cybersecurity Framework and industry-specific best practices, ER Group takes a proactive approach to managing IT and security risks. All employees share the responsibility for protecting the Group'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, ER Group regularly reviews and updates them in line with evolving threats, regulatory changes and technological advancements. They are made accessible to all employees via the Group's intranet and are supported by regular training programmes, awareness campaigns and e-learning modules designed to strengthen understanding and promote compliance.

Independent assurance is provided by Compliance and Internal Audit, who conduct regular reviews to assess the effectiveness of controls. Findings are reported to Senior Management and the Board's oversight committees, with the implementation of remedial actions closely tracked through established governance channels.

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

3. Governance Disclaimer

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