Information Security Management

Policy Statement

Document	Information Security Policy
Company	eClerx Services Ltd.
Prepared by	Information Security Group
Approved by	Program Manager – ISG

This document is copyright protected in content, presentation, and intellectual origin, except where noted otherwise. You may not modify, remove, augment, add to, publish, transmit, participate in the transfer or sale of, create derivative works from, or in any way exploit any of the elements of this document, in whole or in part without prior written permission from eClerx Services Ltd. © 2025-2026.

Information Security Policy Statement

eClerx is committed to safeguarding all organizational information assets, including the personal and confidential information entrusted to us by our clients, employees, partners, and stakeholders. We recognize that maintaining the highest standards of confidentiality, integrity, and availability of information is essential to deliver secure, reliable, and high-quality services.

To uphold this commitment, eClerx has established a comprehensive Information Security Management framework, which is aligned with ISO/IEC 27001 guidelines and global security practices, endorsed and supported by leadership. This framework ensures that appropriate technical, administrative, and physical security controls are implemented, integrated, and continuously improved to protect against evolving threats, unauthorized access, data breaches, and disruptions.

eClerx ISMS framework has the following objectives defined to maintain the confidentiality, integrity and availability of information:

- **Confidentiality** – Protecting information from unauthorized access or disclosure
- **Integrity** – Safeguarding information from unauthorized modification, ensuring accuracy and completeness
- **Availability** – Ensuring information and critical services remain accessible to authorized users whenever required
- To ensure all eClerx employees feel sense of responsibility and accountability for all eClerx information assets they use or access
- Compliance to all statutory, regulatory, administrative, client and eClerx stakeholder's Information security requirements
- To identify, manage, report and address all risks applicable to eClerx information assets to ensure minimizing/ mitigating the liability of eClerx