Group Information Technology Policies (Executive Summary only)

harel mallac
for the better

Information and information systems are valuable assets and their confidentiality, integrity and availability are critical to our business. These assets can bring competitive advantage, enhance our business strategies and promote efficiency. As the holding entity and an investor in the group entities, the group is committed in instilling a set of consistent and adapted policies focusing on IT governance and information security best practices with the aim of safeguarding these assets.

1. Purpose

The Group IT Policy provides a set of guiding principles relating to IT processes and is aimed at:

- Strengthening the internal control environment
- Promoting consistency across the group, in adhering to desired practices based on management expectations and best practices
- Establishing clear expectations of performance and accountability

2. Applicability

The policy applies to the local and foreign subsidiaries listed in Appendix A of the complete document.

3. Target Audience

This policy is addressed to all employees (full time or part time), contractors and third-parties within the above entities who own, develop, operate or use any information systems. Compliance with this policy is mandatory unless authorised waivers are obtained. The Group IT function reserves the right to monitor the use of IT resources and to perform periodic audits to verify compliance with this policy, at any time and without any prior notice. Failure to follow this policy exposes us to risks that could jeopardise client relationships, make us lose competitive advantage or even breach laws.

4. Ownership

The policy is sponsored by the Group Head of Corporate Services. The Group IT Manager is responsible for maintaining the document and for providing clarifications pertaining to this document.

5. Responsibility Matrix

The Business Unit Leader (or equivalent) of each business unit must designate specific individuals who are responsible for implementing and sustaining the controls defined in this policy. This must be documented in the template provided in Appendix A and must be maintained for compliance monitoring purposes.

6. Compliance Monitoring

Compliance with the policy is required at all times and all control activities within this policy must be documented. To allow for flexibility, two types of compliance activities will be performed to prevent and detect non-adherence. These activities can be either of the following:

- Internal verifications: The Group IT Manager, delegated individuals, contracted service providers or the IT In-Charge (or equivalent) within each entity performs ad-hoc verifications to assess the extent of compliance with the requirements of this policy. Instances of non-compliance are reported to the relevant Business Unit Leader (or equivalent) of the entity concerned for remediation.
- Independent verifications: The Internal Audit function performs audits to detect instances of non-compliance and exceptions, which are reported to the relevant Audit and Risk Management Committees and senior management.

7. Communication

The Group IT Manager is responsible for communicating the policy to relevant stakeholders, including new versions following revisions to the content. For new joiners, the Human Resources function is responsible for training and awareness.

8. Revision and Update

The contents of this policy will be reviewed by the Group IT Manager at least once annually and updated accordingly to reflect any changes in risk exposure, IT environment or organisation structures.

9. Policy Statements Applicability

The following convention has been used:

- Policy statements with a ‘must’ indicate mandatory compliance. Non-compliance requires an approved exception.
- Policy statements with a ‘should’ or ‘may’ indicate recommendations which should be implemented wherever possible. Non-compliance does not require an approved exception.

10. Waivers

Waivers will be accepted only in exceptional circumstances and after a thorough evaluation. Requests for waivers, including the supporting rationales must be documented and submitted to the Business Unit Leader (or equivalent) and the Group IT Manager for review and approval.

END