
Third Party Security Policy

Scope

This policy applies to all third parties, including but not limited to business partners, contractors, vendors, suppliers, and outsourced service providers who access, process, store, or handle the PCE Hi-Tech Solutions' networks, information systems, or organizational data.

This is a high-level, public version of the company's information security requirements.

Purpose

The purpose of this policy is to outline PCE Hi-Tech Solutions LTD's expectations for third parties, who particularly access company's systems or manage information on behalf of the company.

Third Parties Obligations

Third parties are required to protect the company's information that is shared with or managed by them and safeguard it from unauthorized access, disclosure, modification, or loss, whether stored, processed, or transmitted, and securely return or promptly delete when no longer required.

Third parties are expected to operate in accordance with the terms defined in their contractual agreements, including Non-Disclosure Agreements (NDAs), Service Level Agreements (SLAs), and Data Processing Agreements (DPAs), where such agreements are signed or required.

Third Parties Evaluation

To assess Third Parties' operational performance, security and quality, the Company shall, where deemed necessary, conduct a formal evaluation using an Evaluation Questionnaire, which must be completed and returned to the Company.

Document Validity

This policy shall be reviewed periodically and upon significant ISMS or organizational changes to ensure its ongoing suitability, adequacy, and effectiveness in alignment with ISO/IEC 27001:2022.

Vaggelis Karasoulas
CEO

Charalambos Charalambous
CTO