Third-Party Management Policy

Policy Owner: Dotan Simha

Effective Date: Aug 28, 2024

Purpose

To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

This document outlines a baseline of security controls that Software Products Guilda Ltd. expects partners and other third-party companies to meet when interacting with Software Products Guilda Ltd. Confidential data.

Scope

All data and information systems owned or used by Software Products Guilda Ltd. that are business critical and/or process, store, or transmit Confidential data. This policy applies to all employees of Software Products Guilda Ltd. and to all external parties, including but not limited to Software Products Guilda Ltd. consultants, contractors, business partners, vendors, suppliers, partners, outsourced service providers, and other third-party entities with access to Software Products Guilda Ltd. data, systems, networks, or system resources.</p

General requirements

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

For all service providers who may access Software Products Guilda Ltd. Confidential data, systems, or networks, proper due diligence shall be performed prior to provisioning access or engaging in processing activities. Information shall be maintained regarding which regulatory or certification requirements are managed by or impacted by each service provider, and which are managed by Software Products Guilda Ltd. as required. Applicable regulatory or certification requirements may include ISO 27001, SOC 2, PCI DSS, CCPA, GDPR or other frameworks, compliance standards, or regulations.

Addressing security in agreements

Relevant information security requirements shall be established and agreed upon with each supplier that may access, process, store, transmit, or impact the security of Confidential data and systems, or provide physical or virtual IT infrastructure components for Software Products Guilda Ltd..

For all service providers who may access Software Products Guilda Ltd. production systems, or who may impact the security of the Software Products Guilda Ltd. production environment, written agreements shall be maintained that include the service provider's acknowledgment of their responsibilities for the confidentiality of company and customer data, and any commitments regarding the integrity, availability, and/or privacy controls that they manage in order to meet the standards and requirements that Software Products Guilda Ltd. has established in accordance with Software Products Guilda Ltd.'s information security program or any relevant framework.

Technology supply chain

Software Products Guilda Ltd. will consider and assess risk associated with suppliers and the technology supply chain. Where warranted, agreements with suppliers shall include requirements to address the relevant information security risks associated with information and communications technology services and the product supply chain.

Monitoring & review of third-party services

Software Products Guilda Ltd. shall regularly monitor, review, and audit supplier service delivery. Supplier security and service delivery performance shall be reviewed at least annually.

Management of changes to third-party services

Changes to the provision of services by suppliers, including changes to agreements, services, technology, policies, procedures, or controls, shall be managed, taking account of the criticality of the business information, systems, and processes involved. Software Products Guilda Ltd. shall assess the risk of any material changes made by suppliers and make appropriate modifications to agreements and services accordingly.

Third-party risk management

Software Products Guilda Ltd. will ensure that potential risks posed by sharing Confidential data or providing access to company systems are identified, documented and addressed according to this policy. Risk management plays an integral part in the governance and management of the organization at a strategic and operational level. The purpose of a partner and third-party security policy is to ensure that partnerships and services achieve their business plan aims and objectives, and are consistent with Software Products Guilda Ltd.'s requirements for information security.

Software Products Guilda Ltd. shall not share or transmit Confidential data to a third-party without first performing a third-party risk assessment and fully executing a written contract, statement of work or service agreement which describes expected service levels and any specific information security requirements.

Information security for use of cloud services

This section outlines the fundamental parameters for managing and mitigating risks related to cloud service usage.

Responsibilities and Risk Management:

- Roles and responsibilities related to the use and management of cloud services can be found in the Roles and Responsibilities Policy.
- Information security risks associated with cloud services use shall be managed in accordance with this policy and the Risk Management Policy.

Security Requirements and Control:

- The company shall be responsible for all customer controls as defined in cloud service providers' responsibility matrices.

Service Selection and Usage Scope:

- Reviews of cloud service agreements for inherently high risk providers shall be performed annually to ensure they align with company requirements.

Incident Management:

- Information security incidents related to cloud services managed in accordance with the Incident Response Plan.

Service Review and Exit Strategy:

- Risks related to exit and vendor lock-in should be evaluated prior to the acquisition as part of the vendor security assessment.

Provider and Customer Agreement:

- Agreements with cloud service providers will specify protections for Software Products Guilda Ltd.'s data and service availability, even though they might be predefined and non-negotiable.
- Where possible, Software Products Guilda Ltd. will seek advance notification from providers concerning substantive changes in service delivery, including changes in technical infrastructure, data storage location, or usage of sub-contractors.

Ongoing Management and Assurance:

- Information regarding how to obtain and utilize information security capabilities provided by the cloud service provider should be assessed as part of the vendor review at time of acquisition.

Third-party security standards

All third-parties must maintain reasonable organizational and technical controls as assessed by Software Products Guilda Ltd..

Assessment of third-parties which receive, process, or store Confidential data or access Software Products Guilda Ltd.'s resources shall consider the following controls as applicable based on the service provided and the sensitivity of data stored, processed or exchanged.

Information Security Policy
Third-parties maintain information security policies supported by their executive management, which are regularly reviewed.

Risk Assessment & Treatment
Third-parties maintain programs that assess, evaluate, and manage information and technology risks.

Operations Security
Third-parties implement commercially reasonable practices and procedures designed, as appropriate, to maintain operations security. Protections may include:

- Technical testing
- Protection against malicious software
- Network protection and management
- Technical vulnerability management
- Logging and monitoring
- Incident response
- Business continuity planning

Access Control
Third-parties maintain a technical access control program.

Secure System Development
Third-parties maintain a secure development program consistent with industry software and systems development best practices including risk assessment, formal change management, code standards, code review and testing.

Physical & Environmental Security
If third-parties are storing or processing confidential data, their physical and environmental security controls should meet the requirements of the Software Products Guilda Ltd. Physical Security Policy.

Human Resources
Third-parties maintain human resource policies and processes which include criminal background checks for any employees or contractors who access Software Products Guilda Ltd. confidential information.

Compliance & Legal
Software Products Guilda Ltd. shall consider all applicable regulations and laws when evaluating suppliers and third parties who will access, store, process or transmit Software Products Guilda Ltd. confidential data. Third-party assessments should consider the following criteria:

- Protection of customer data, organizational records, and records retention and disposition
- Privacy of Personally Identifiable Information (PII)

Exceptions

Requests for an exception to this Policy must be submitted to the CTO for approval.

Violations & enforcement

Any known violations of this policy should be reported to the CTO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version history

Version	Date	Description	Author	Approver
1.0	Aug 28, 2024	Version 1.0	Dotan Simha	Dotan Simha