Human Resource Security Policy

Policy Owner: Dotan Simha

Effective Date: Aug 28, 2024

Purpose

To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.

Scope

This policy applies to all employees of Software Products Guilda Ltd., consultants, contractors and other third-party entities with access to Software Products Guilda Ltd. production networks and system resources.

Screening

Background verification checks on Software Products Guilda Ltd. personnel shall be carried out in accordance with relevant laws, regulations, and shall be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. Background screening shall include criminal history checks unless prohibited by local statute. All third-parties with technical privileged or administrative access to Software Products Guilda Ltd. production systems or networks are subject to a background check or requirement to provide evidence of an acceptable background, based on their level of access and the perceived risk to Software Products Guilda Ltd..

Competence & performance assessment

The skills and competence of employees and contractors shall be assessed by human resources staff and the hiring manager or his or her designees as part of the hiring process. Required skills and competencies shall be listed in job descriptions and requisitions, and/or aligned with the responsibilities outlined in the Information Security Roles and Responsibilities Policy. Competency evaluations may include reference checks, education and certification verifications, technical testing, and interviews.

All Software Products Guilda Ltd. employees will undergo an annual performance review which will include an assessment of job performance, competence in the role, adherence to company policies and code of conduct, and achievement of role-specific objectives.

Terms & conditions of employment

Company policies and information security roles and responsibilities shall be communicated to employees and third-parties at the time of hire or engagement, and employees and contractors are required to formally acknowledge their understanding and acceptance of their security responsibilities. Employees and third-parties with access to company or customer information shall sign an appropriate non-disclosure, confidentiality, and appropriate code-of-conduct agreements. Contractual agreements shall state responsibilities for information security as needed. Employees and relevant third-parties shall follow all Software Products Guilda Ltd. information security policies.

Management responsibilities

Management shall be responsible for ensuring that information security policies and procedures are reviewed annually, distributed and available, and that employees and contractors abide by those policies and procedures for the duration of their employment or engagement. Annual policy review shall include a review of any linked or referenced procedures, standards or guidelines.

Management shall ensure that information security responsibilities are communicated to individuals, through written job descriptions, policies or some other documented method which is accurately updated and maintained. Compliance with information security policies and procedures and fulfillment of information security responsibilities shall be evaluated as part of the performance review process wherever applicable.

Management shall consider excessive pressures, and opportunities for fraud when establishing incentives and segregating roles, responsibilities, and authorities.

Information Security awareness, education & training

All Software Products Guilda Ltd. employees and third-parties with administrative or privileged technical access to Software Products Guilda Ltd. production systems and networks shall complete security awareness training at the time of hire and annually thereafter. Management shall monitor training completion and shall take appropriate steps to ensure compliance with this policy. Employees and contractors shall be aware of relevant information security and data privacy policies and procedures. The company shall ensure that personnel receive security and data privacy training appropriate to their role and data handling responsibilities.

In order to maintain a robust level of security awareness, the company will provide security-related updates and communications to company personnel on an on-going basis through multiple communication channels as needed.

Information security leaders and managers shall ensure appropriate professional development occurs to provide an understanding of current threats and trends in the security landscape. Security leaders and key stakeholders shall attend trainings, obtain and maintain relevant certifications, and maintain memberships in industry groups as appropriate.

Termination process

Employee and contractor termination and offboarding processes shall ensure that physical and logical access is promptly revoked in accordance with company SLAs and policies, and that all company issued equipment is returned.

Any security or confidentiality agreements which remain valid after termination shall be communicated to the employee or contractor at time of termination.

Disciplinary process

Employees and third-parties who violate Software Products Guilda Ltd. information security policies shall be subject to the Software Products Guilda Ltd. progressive disciplinary process, up to and including termination of employment or contract.

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 policies 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