Information Security Policy (AUP)

Policy Owner: Dotan Simha

Effective Date: Aug 14, 2024

Overview

This Information Security Policy is intended to protect Software Products Guilda Ltd.'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file transfers, are the property of Software Products Guilda Ltd.. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Software Products Guilda Ltd. employee or contractor who deals with information and/or information systems. It is the responsibility of every team member to read and understand this policy, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to communicate our information security policies and outline the acceptable use and protection of Software Products Guilda Ltd.'s information and assets. These rules are in place to protect customers, employees, and Software Products Guilda Ltd.. Inappropriate use exposes Software Products Guilda Ltd. to risks including virus attacks, compromise of network systems and services, and legal and compliance issues.

The Software Products Guilda Ltd. "Information Security Policy" is comprised of this policy and all Software Products Guilda Ltd. policies referenced and/or linked within this document.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Software Products Guilda Ltd. business or interact with internal networks and business systems, whether owned or leased by Software Products Guilda Ltd., the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Software Products Guilda Ltd. and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Software Products Guilda Ltd. policies and standards, and local laws and regulations.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Software Products Guilda Ltd., including all personnel affiliated with third parties. This policy applies to all Software Products Guilda Ltd.-controlled company and customer data as well as all equipment, systems, networks and software owned or leased by Software Products Guilda Ltd..

Security incident reporting

All users are required to report known or suspected security events or incidents, including policy violations and observed security weaknesses. Incidents shall be reported immediately or as soon as possible by sending email to security@the-guild.dev.

In your report, please describe the incident or observation along with any relevant details.

Whistleblower anonymous fraud reporting

Our Whistleblower Policy is intended to encourage and enable employees and others to raise serious concerns internally so that we can address and correct inappropriate conduct and actions. It is the responsibility of all employees to report concerns about violations of our code of ethics or suspected violations of law or regulations that govern our operations.

It is contrary to our values for anyone to retaliate against any employee or who in good faith reports an ethics violation, or a suspected violation of law, such as a complaint of discrimination, or suspected fraud, or suspected violation of any regulation. An employee who retaliates against someone who has reported a violation in good faith is subject to discipline up to and including termination of employment.

Anonymous reports may be submitted via anonymous Google form: https://forms.gle/nVrQiR8qEjK99kUq7.

Mobile device policy

All end-user devices (e.g., mobile phones, tablets, laptops, desktops) must comply with this policy. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

System level and user level passwords must comply with the Access Control Policy. Providing access to another individual, either deliberately or through failure to secure a device is prohibited.

All end-user, personal (BYOD) or company owned devices used to access Software Products Guilda Ltd. information systems (i.e. email) must adhere to the following rules and requirements:

- Devices must be locked whenever left unattended
- Users must report any suspected misuse or theft of a mobile device immediately to the company's CTO
- Confidential information must not be stored on mobile devices or USB drives (this does not apply to business contact information, e.g., names, phone numbers, and email addresses)
- Any mobile device used to access company resources (such as file shares and email) must not be shared with any other person
- Upon termination users agree to return all company owned devices and delete all company information and accounts from any personal devices

Clear screen clear desk policy

Users shall not leave confidential materials unsecured on their desk or workspace, and will ensure that screens are locked when not in use.

Remote working and access policy

Remote working refers to any situation where organizational personnel operate from locations outside the office. This includes teleworking, telecommuting, flexible workplace, virtual work environments, and remote maintenance. Laptops and other computer resources that are used to access the Software Products Guilda Ltd. network must conform to the security requirements outlined in Software Products Guilda Ltd.'s Information Security Policies and adhere to the following standards:

- Company rules shall be followed while working remote including clear desk protocols, printing, disposal of assets, and information security event reporting to prevent mishandling or accidental exposure of sensitive information.
- To ensure mobile devices do not connect a compromised device to the company network, Antivirus policies require the use and enforcement of client-side antivirus software
- Antivirus software must be configured to detect and prevent or quarantine malicious software, perform periodic system scans, and have automatic updates enabled
- When working from a home network, ensure that the default wifi settings are changed, such as name, password and admin access
- Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer
- Users are prohibited from changing or disabling any organizational security controls such as personal firewalls, antivirus software on systems used to access Software Products Guilda Ltd. resources
- Use of remote access software and/or services (e.g., VPN client) is allowable as long as it is provided by the company and configured for multifactor authentication (MFA)
- Unauthorized remote access technologies may not be used or installed on any Software Products Guilda Ltd. system
- Users shall use a VPN when transmitting confidential information on public Wi-Fi
- If you access from a public computer (e.g., from a business center, hotel, etc.), log out of the session and don't save anything. Don't check "remember me", collect all printed materials and do not download files to a non-Software Products Guilda Ltd. controlled system

Acceptable use policy

Software Products Guilda Ltd. proprietary and customer information stored on electronic and computing devices, whether owned or leased by Software Products Guilda Ltd., the employee or a third party, remains the sole property of Software Products Guilda Ltd. for the purposes of this policy. Employees and contractors must ensure through legal or technical means that proprietary information is protected in accordance with the Data Management Policy. The use of Google Drive/Notion for business file storage is required for users of laptops or company issued devices. Storing important documents on the file share is how you "backup" your laptop.

You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Software Products Guilda Ltd. proprietary information or equipment. You may access, use or share Software Products Guilda Ltd. proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties. Employees are responsible for exercising good judgment regarding the reasonableness of personal use of company-provided devices.

For security and network maintenance purposes, authorized individuals within Software Products Guilda Ltd. may monitor equipment, systems and network traffic at any time.

Software Products Guilda Ltd. reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Unacceptable use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities with properly documented Management approval. Under no circumstances is an employee of Software Products Guilda Ltd. authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Software Products Guilda Ltd.-owned resources or while representing Software Products Guilda Ltd. in any capacity. The list below is not exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Software Products Guilda Ltd.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Software Products Guilda Ltd. or the end user does not have an active license
3. Accessing data, a server, or an account for any purpose other than conducting Software Products Guilda Ltd. business, even if you have authorized access, is prohibited
4. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate management shall be consulted prior to export of any material that is in question
5. Introduction of malicious programs into the network or systems (e.g., viruses, worms, Trojan horses, email bombs, etc.)
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home
7. Using a Software Products Guilda Ltd. computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws
8. Making fraudulent offers of products, items, or services originating from any Software Products Guilda Ltd. account
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient, or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes
11. Port scanning or security scanning is expressly prohibited unless prior notification to the Software Products Guilda Ltd. engineering team is made
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty
13. Circumventing user authentication or security of any host, network, or account
14. Introducing honeypots, honeynets, or similar technology on the Software Products Guilda Ltd. network
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack)
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means
17. Providing information about, or lists of: Software Products Guilda Ltd. employees, contractors, partners, or customers to parties outside Software Products Guilda Ltd. without authorization

Email and communication activities

When using company resources to access and use the Internet, users must realize they represent the company and act accordingly.

The following activities are strictly prohibited, with no exceptions:

1. Sending unsolicited email messages, including the sending of "junk mail", or other advertising material to individuals who did not specifically request such material (email spam)
2. Any form of harassment via email, telephone, or texting, whether through language, frequency, or size of messages
3. Unauthorized use, or forging, of email header information
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies
5. Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type
6. Use of unsolicited email originating from within Software Products Guilda Ltd. networks or other service providers on behalf of, or to advertise, any service hosted by Software Products Guilda Ltd. or connected via Software Products Guilda Ltd.'s network

Additional policies and procedures incorporated by reference

Policy	Purpose
Access Control Policy	To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.
Asset Management Policy	To identify organizational assets and define appropriate protection responsibilities.
Business Continuity & Disaster Recovery Plan	To prepare Software Products Guilda Ltd. in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.
Cryptography Policy	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
Data Management Policy	To ensure that information is classified and protected in accordance with its importance to the organization.
Human Resources Policy	To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.
Incident Response Plan	Policy and procedures for suspected or confirmed information security incidents.
Operations Security Policy	To ensure the correct and secure operation of information processing systems and facilities.
Physical Security Policy	To prevent unauthorized physical access or damage to the organization’s information and information processing facilities.
Risk Management Policy	To define the process for assessing and managing Software Products Guilda Ltd.'s information security risks in order to achieve the company’s business and information security objectives.
Secure Development Policy	To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.

Policy compliance

The organization will measure and verify compliance to this policy through various methods, including but not limited to ongoing monitoring, and both internal and external audits.

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 CEO. 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 14, 2024	Version 1.0	Dotan Simha	Dotan Simha