Public Document

Information security policy

Company name:	Cives Ltd
Effective date:	14/09/2024

Version history

Version	Date	Description	Author	Approved by
1.0	14/09/2024	First version	Brian McGlynn	Alfeo Pareschi

Purpose

This information security policy is intended to protect employees, partners, and the Cives Ltd company from illegal or harmful actions by individuals, knowingly or unknowingly.

Systems related to the Internet/ Intranet/ Extranet, including but not limited to computer equipment, software, operating systems, storage media, network accounts that provide e-mail, Web browsing, and file transfers, are the property of the company. These systems are to be used for business purposes to serve the interests of the company and our clients and customers in the normal course of operations.

Effective security is a team effort that involves the participation and support of all employees or contractors in the company who deal with information and/or information systems. It is the responsibility of each team member to read and understand this procedure and conduct their activities accordingly.

Index

Reporting of security incidents

All employees are required to report known or suspected security events or incidents, including policy violations and any observed security vulnerabilities. Incidents should be reported immediately or as soon as possible to incident@cives.ai in which please describe the incident or observation along with all relevant details.

Fraud reporting

Information security policies are intended to encourage and enable employees and others, to raise any concerns internally so that inappropriate behavior/actions can be addressed and corrected. It is the responsibility of all parties involved in this policy to raise concerns about violations of the company's code of ethics or suspected violations of laws/regulations to which the company must adhere.

It is contrary to our values for anyone to retaliate against an employee or anyone who, in good faith, reports an ethics violation or suspected violation of law, 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 disciplinary action, up to and including possible dismissal.

Mobile devices

All employee devices (e.g., cell phones, tablets, laptops) must comply with this policy. Employees should exercise caution when opening e-mail 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 an unknown outsider, either deliberately or through failure to secure a device, is prohibited.

All end-user, personal (BYOD) or company-owned devices used to access the company's information systems (e.g., e-mail) must comply with the following rules and requirements:

- Devices must be locked with a password-protected screen saver (or equivalent control such as biometric) or a subsequent screen lock after 5 (five) minutes of non-use as evidenced
- Devices must be locked whenever they are left unattended
- Users should immediately report any suspected misuse or theft of a mobile device to Top Management

- Confidential information should not be stored on mobile devices or USB drives (this does not apply to corporate contact information, e.g., names, phone numbers, and e-mail addresses)
- Any mobile device, used to access corporate resources (such as file shares and e-mail), 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

Screen Lock

Employees should not leave unprotected confidential materials on their desks or workspace and will ensure that screens are locked when not in use.

Work and remote access

Remote work refers to any situation in which organizational staff operate from locations outside the office. This includes telecommuting, flexible workplace, virtual work environments and remote maintenance. Laptops and other computing resources used to access the corporate network must comply with the security requirements defined in the Information Security Policy and adhere to the following standards:

- Business rules must be followed while working remotely, including clean desk protocols, printing, resource disposal, and information security event reporting to prevent improper handling or accidental exposure of sensitive information.
- To ensure that mobile devices do not contain viruses that could compromise the corporate network, employee-side antivirus software is required to be installed.
- Antivirus software should be configured to detect and prevent or quarantine malicious software, perform periodic system scans, and enable automatic updates.
- When the employee connects from a home network, it should be ensured that the default Wi-Fi settings are changed, such as name, password and administrator access.
- Employees should not connect to any external network without a secure and up-to-date software firewall configured on the laptop.
- Employees are prohibited from modifying or disabling any organizational security controls such as personal firewalls, antivirus software on systems used to access company resources.
- The use of remote access software and/or services (e.g., VPN client) is allowed as long as it is provided by the company and configured for multi-factor authentication (MFA).

- Unauthorized remote access technologies may not be used or installed on any enterprise system.
- Forces the use of VPN when transmitting confidential information over public Wi-Fi to prevent potential eavesdropping or man-in-the-middle attacks.
- For the system administrator, it is recommended to configure a specific working network with advanced WPA3 encryption or at least WPA2 with Robust password, along with, if supported, configuration of a dedicated VLAN. In addition, WPS (Wi-Fi Protected Setup) and UPnP (Universal Plug and Play) should be disabled unless specifically requested.
- Employees should use a VPN when transmitting confidential information over public Wi-Fi.

Acceptable use

Proprietary and customer information stored on electronic and computing devices, whether owned or leased by the organization, the employee, or a third party, remains the exclusive property of the company. Employees and external contractors must ensure, through legal or technical means, that proprietary information is protected in accordance with the Data Management Policy procedure. The use of Share point for storing company files is required for employees who have laptops or devices provided by the company.

Employees are responsible for promptly reporting the theft, loss or unauthorized disclosure of company proprietary information or equipment. Company proprietary information may be accessed, used, or shared only to the extent authorized and necessary to perform assigned job duties. Employees are expected to exercise common sense regarding the reasonableness of personal use of company-provided devices.

For network security and maintenance purposes, authorized persons within the company may monitor equipment, systems, and network traffic at any time. The company reserves the right to periodically audit networks and systems to ensure compliance with this procedure.

Unacceptable use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions while performing their legitimate job responsibilities, subject to properly documented top management approval. Under no circumstances is an employee of the organization permitted to engage in any activity illegal under local, state, or international law while using company-owned resources or while representing the company in any capacity. The following list is not exhaustive, but attempts to provide a framework for activities that fall into the category of unacceptable use.

The following activities are strictly prohibited without exception:

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 properly licensed for use by the organization.
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 installation of any copyrighted software for which the organization or employee does not have an active license.
3. Accessing data, a server, or an account for purposes other than conducting the organization's business, even if you have authorized access.
4. Exporting software, technical information, encryption software or technology in violation of international or regional export control laws is illegal. Appropriate management should be consulted before exporting any such materials.
5. Introduction of malicious programs into the network or systems (e.g., viruses, worms, Trojans, email bombs, etc.).
6. Revealing your account password to others or allowing others to use it. This includes family and other family members when work is done at home.
7. Using an organization's IT resource to actively engage in the provision or transmission of material that violates sexual harassment or hostile workplace laws.
8. Making fraudulent offers of products, items or services from any of the organization's accounts.
9. Make warranty statements, express or implied, unless they are part of normal job duties.

10. Performing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data that the employee is not the intended recipient of or accessing a server or account that the employee is not expressly authorized to access. For the purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping flooding, packet spoofing, denial of service, and forged routing information for malicious purposes
11. Door scanning or security scanning is expressly prohibited without prior notification to the company.
12. Performing any form of network monitoring that intercepts data not intended for the employee's host, unless this activity is part of the employee's normal work/duty.
13. Circumvent user authentication or security of any host, network or account.
14. Introduction of honeypot, honeynet or similar technologies on the network.
15. Interfering or denying service to any user other than the employee's host (e.g., denial of service attack).
16. Using programs/ scripts/ commands or sending messages of any kind with the intent to interfere with or disable a user's session by any means.
17. Providing information or lists of: employees, contractors, partners, or customers to parties outside the organization without authorization.

E-mail and communication activities

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

The following activities are strictly prohibited without exception:

1. Sending unsolicited e-mail messages, including sending "junk mail" or other advertising material to individuals who have not specifically requested such material (e-mail spam).
2. Any form of harassment via email, phone or text message
3. Unauthorized use or falsification of e-mail header information
4. Email solicitation for any email address other than the author's account with the intent to harass or collect responses.
5. Creation or forwarding of "chain letters," "ponzi schemes," or other "pyramid" schemes of any kind.
6. Use of unsolicited e-mail from within networks or other service providers on behalf of, or to advertise, any of the organization's hosted services connected through the company's network.

Additional policies and procedures incorporated by reference

Personnel are responsible for reading and following all policies related to their roles and responsibilities listed on the corporate document.

Policy	Purpose
Information security roles and responsibilities policy	This policy establishes and communicates roles and responsibilities within the company. Roles are necessary within the organization to provide clearly defined responsibilities and an understanding of how information is protected. Their purpose is to clarify, coordinate the activities and actions necessary to disseminate information security policy, standards and implementation.
Information security risk management policy	The following policy is intended to define actions to address information security risks and establish a plan for achieving the Information security and privacy objectives.
Asset management policy	Identify organizational resources and define appropriate protection responsibilities.
Human resources policy on information security	The purpose of this policy is to ensure that employees and contractors meet safety requirements, understand their responsibilities, and are suited to their roles.
Information security policy for former employees	This policy is written to ensure the security of information and protection of company assets after an employee's termination of employment. Former employees are required to follow the directions in this document.

Data management policy	The purpose of this policy is to ensure that information is classified, protected, stored, and disposed of securely according to its importance.
Operational security policy	Ensure the proper and safe operation of information processing systems and facilities.
Access control policy	Restrict access to information and information processing systems, networks and facilities to authorized parties in accordance with business objectives.
Encryption policy	Ensure proper and effective use of encryption to protect the confidentiality, authenticity and/or integrity of information.
Safe design and development policy	Ensure that information security is designed and implemented within the application and information system development life cycle.
Third-party management policy	To ensure the protection of the organization's data and resources shared with, accessed, or managed by vendors, 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 vendor agreements.

Compliance with policies

The organization will measure and verify compliance with this procedure through various methods, including but not limited to continuous monitoring and internal and external audits.

Exceptions

Requests for exceptions to this procedure must be submitted to the CTO for approval.

Violations and enforcement

Any known violations of this procedure should be reported to the Top Management. Violations of this procedure may result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including dismissal.