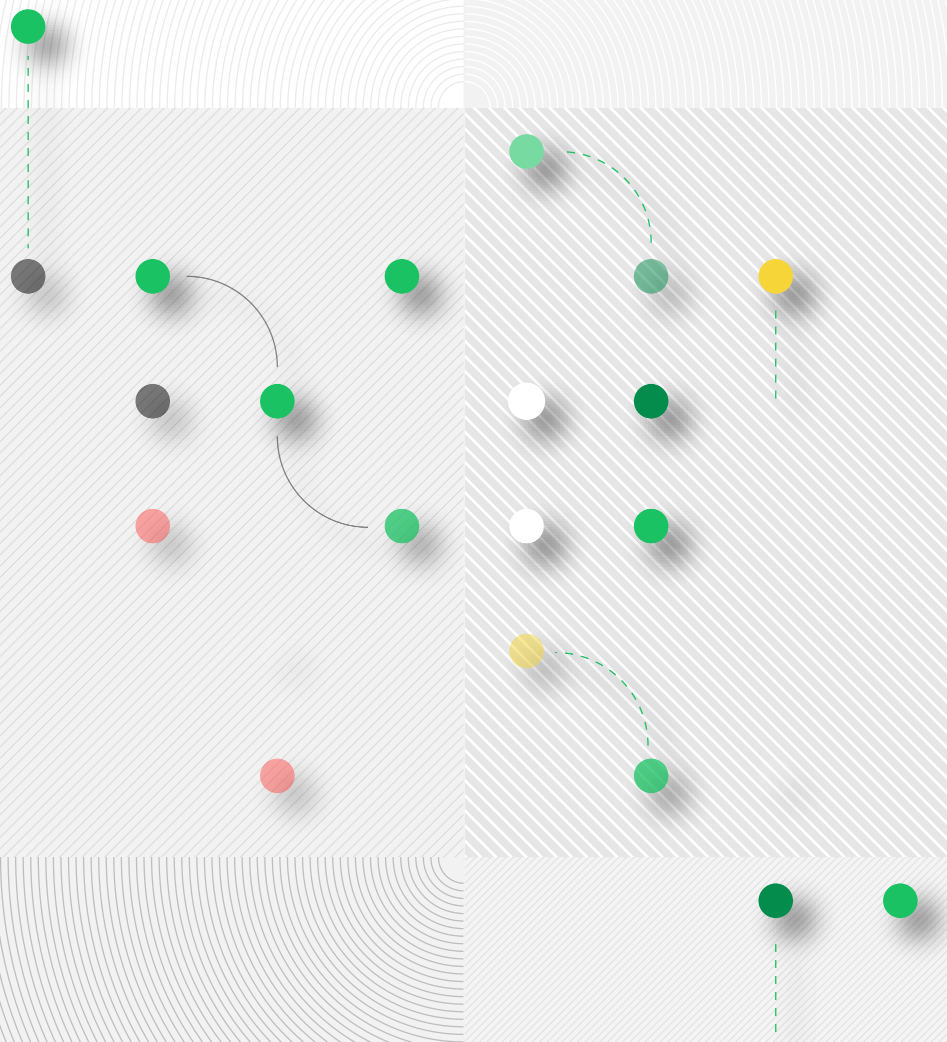
Authomize

# Information Security Policy & Procedures



| | |
|---|---|
| Version | 1.0 |
| Reference | ISM-002 |
| Date | May 1, 2021 |

## 1. General and Company Profile

1.1 Authomize provides a fully automated cloud-based authorization management solution for all the organization's SaaS & IaaS. Authomize's solution is a "system of intelligence" for identity and cloud services permissions/entitlements.

1.2 Integrated to the company's cloud services and SSO, Authomize generates visibility to the organization's identity entitlements: effective user privileges, user actions audit, and actual utilized user privileges. The solution also provides a unified and straightforward permission managementtool reducing the proficiency needed for managing the permission of multiple applications.

1.3 The platform uses the company's proprietary SmartGroups technology, which aggregates data in real-time from multiple enterprise IT systems and dynamically infers "right-sized" permissions. The recommendations based on the organization's operational needs and actual permission usage and continuously maintaining good security hygiene.

## 2. Purpose, Overview, and Applicability

2.1 The responsibility for information security on a day-to-day basis is every employee's duty. In complying with the following policy, the company reduces the ever-growing threat to information systems. This policy does not conflict with any official duties of users but protects them and assets from unauthorized and damaging use. The purposes of this policy are as follows:

2.1.1 Ensure that the company's information resources are appropriately protected from destruction, alteration, or unauthorized access.

2.1.2 Ensure that this protection is accomplished in a manner consistent with the business and workflow requirements of the company.

2.1.3 Ensure that the industry's best security practices are implemented in order to reduce vulnerabilities, increase safety, and provide guidance to the company on the expected threats.

2.1.4 Provide a concise set of standards in order to attain consistency across the entire information infrastructure about securing systems and networks.

2.2 Overview and applicability:

2.2.1 This policy covers the best security practices to protect all the company's information system resources and information.

2.2.2 This policy applies to all the company's personnel including, but not limited to, employees, contractors, consultants, and temporary personnel.

2.2.3 All the company's personnel are expected to become familiar and comply with this policy. Personnel, who are not in compliance, may be subject to disciplinary actions, including, but not limited to, termination.

2.2.4 This policy also applies to all outsourcing firms that perform services for the company.

## 3. Definitions

3.1 **Information Security** All technological and organizational means used to mitigate risk pertaining to the confidentiality, integrity, and availability of information stored in IT systems.

3.2 **IS Manager** The person responsible for the overall information security program to ensure the adequate protection of the company's information assets and technology.

3.3 **Identification** Means to identify a person or system while attempting access and authorizing processes in an IT system.

3.4 **Username** A unique identification string provided to each network or system user in order to verify identity.

3.5 **Information** Data whether stored in writing, print, magnetic device, optical device, or any other means.

3.6 **Sensitive Information** Data defined as sensitive by the company's management.

3.7 **Restricted Information** Data defined by local data protection legislation in each of the countries where the company or a subsidiary of the company carries on business, or as may be defined or determined by the company.

3.8 **Storage Media** Media used for information storage.

3.9 **User** An employee of the company or an employee of an outsourcing firm supplying goods or services or both to the company that uses the company's information systems for that person's work. Each user has a personal username.

3.10 **Information Asset** File or information system containing company information.

3.11 **Password** A string of characters known only to the user, used for identification confirmation of the user and typed as part of the user identification process while logging on.

3.12 **ISO27001:2013** A leading information security standard, detailing how an organization should manage its Information Security Management System (ISMS).

3.13 **Information Security Management System (ISMS)** A long term framework that aims to enhance information security throughout the organization (Part of ISO27001 framework).

3.14 **Personal data information** any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

# 4. Board and Management Commitment

4.1 Consistent with their responsibility for proper management of the company, the company's management and board of directors are committed to maintaining a high level of information security.

4.2 The company's management is obliged to provide adequate resources to maintain an appropriate level of information security in the company and to budget for an annual work plan.

4.3 The company's management has defined the ISMS as a cornerstone of its security and technological viewpoint.

# 5. Information Security Goals

The company's information security goals are as follows:

5.1 Protect the company's and customers' information from unauthorized and malicious activity by effectively and efficiently enforcing an information security policy.

5.2 Enable the company's business strategy and maintain services for customers in a manner consistent with the proper application of security and privacy guidance and risk management.

5.3 Allow the company to maintain the confidentiality, integrity, and availability of information.

5.4 Serve as the basis for information security procedures and controls.

5.5 Provide guidance on how to locate and manage risks and exposures of information stored in the system, including prints, scans, tapes, or other hard copies.

5.6 Define tools and processes required to actively enhance the security awareness of the company's personnel and suppliers.

5.7 Define the steps required for an annual work plan that includes the following actions:

5.7.1 Purchasing, installing, and integrating security products.

5.7.2 Maintaining information security products.

5.7.3 Maintaining a risk assessment program.

5.7.4 Performing special projects.

6. 
# Information Security Business Principles

The company's information security business principles are as follows:

6.1 Create a security culture through information security governance.

6.2 Assess risks through understanding, evaluating, and testing.

6.3 Ensure effective implementation of the critical information security basics by following policies, procedures, and guidelines.

6.4 Enforce the information security policy through technological processes (where applicable) education, monitoring, and metrics.

6.5 Adhere to applicable regulatory requirements that include international and State laws and regulations.

7. 
# Major Risks

7.1 The company has business, financial, and personal information. Unauthorized access or a security breach may affect the confidentiality, integrity, and availability of that information. Here are the main information security risks that exist in the company.

7.2 Technological risks:

7.2.1 Decrease in availability and credibility of the systems as a result of full or partial damage.

7.2.2 Low performance of computers either from internal or external security breaches.

7.2.3 Harming the privacy of the company's employees or customers or other relevant parties, whose details are stored in the company's systems, as a result of information disclosed to unauthorized individuals.

7.2.4 Data corruption in production environment information systems which could lead to invalid actions or faulty decision taking.

7.2.5 Harming the survivability of the company's systems due to technical failure or damage.

7.3 Human and organizational risks:

7.3.1 A security breach pertaining to the following: employees, customers, internal R&D documentation and specifications, financial data, intellectual property, and so on.

7.3.2 Unauthorized access to the company's sites or secure or restricted areas.

7.3.3 User error leading to an information security breach.

7.3.4 Malicious behavior by authorized personnel or third parties.

7.3.5 Transferring certain types of information in an insecure manner or to an unauthorized recipient.

7.3.6 Loss or theft of stationery or portable IT equipment and sensitive information.

7.3.7 Failing to comply with applicable legal or regulatory requirements.

## 8. Key Elements in Establishing an ISMS

8.1 In general, information security measures and methods are implemented to minimize risks and shall be adapted based on the risk and sensitivity level over time.

8.2 The four key elements implemented to achieve effective information security protection are:

8.2.1 **Prevention** information security components are designed to prevent malicious or accidental damage to company's information by employees or outsourcers, such as access control systems, authorization systems, and anti-virus software.

8.2.2 **Detection** detecting breaches that were not identified by the prevention layer.

8.2.3 **Reaction** a reaction (or correction) layer that may be independent or part of the detection layer. Allows response to the breach as a function of the event:

8.2.4 **Real time reaction** by changing the prevention capabilities of the system.

8.2.5 **Post event reaction** shall be based on information logged during the event, analyzing it, and drawing conclusions.

8.2.6 **Documentation** the documentation layer shall allow analyzing the events (prevention, detection, or reaction events) to allow a broad perspective of the event.

## 9. Organizing Information Security

9.1 The company's organizational chart is in the appendix to this policy.

9.2 In order to perform the requirements of the policy, the company shall define a suitable infrastructural framework, based on the following:

9.3 Information security steering committee:

9.3.1 The information security steering committee (the "Steering Committee") is the highest body authorized to approve initial changes to the policy and to decide how to implement the company's information security system.

9.3.2 The members of the Steering Committee are:

- CEO
- VP Product
- IS MANAGER (by VP R&D)

9.3.3 The committee's roles are:

- Approving the information security policies and procedures and overviewing implementation.
- Approving and monitoring the annual work.
- Proving information classification levels and setting the required security level for the company's systems.
- Be a deciding authority in cases of disagreement about information security subjects.
- Updating information security breach events and discussing appropriate reaction.
- Convening annually for an information security review.

9.3.4 IS Manager's responsibilities are as follows:

- Presenting information security topics to the management.
- Providing the board of directors with an annual information security review.
- Leading the Steering Committee.
- Implementing the information security policy and procedures (physical and logical) and providing guidance on implementation to relevant personnel.
- Initiating and implementing an annual work plan.
- Performing audits on information security implementation in the Company.
- Investigating and handling information security events and breaches.
- Conducting information security awareness trainings.
- Defining and developing security processes and tools in the field of information systems.
- Defining and developing and integrating processes and tools related to information security.
- Defining information security levels of the IS and its components in compliance with decisions of the Steering Committee.
- Developing processes and tools for enforcing and controlling the IS system.
- Being involved in technological changes in the company's computer systems, to whatever degree necessary.
- Executing backups according to the company's information security policy.
- Handling responses to security incidents and malfunctions.
- Specifying processes and methods about the levels of sensitivity and information classification to which third parties may be exposed.

9.4 Steering Committee's roles and responsibilities:

- Lead the process of dealing with IS incidents and events while performing investigations and establishing lessons to be learned.
- In the event of a risk of damage to the company's databases or information systems while being serviced, disconnecting users and managing that process.
- Initiating disciplinary proceedings as may be required.

## 10. Data Classification

10.1 The company has the following classes of data:

- Sensitive information
- Personally identifiable information
- Public information

10.2 Sensitive information consists of:

- Internal confidential information
- Customer confidential information

10.2.1 Internal confidential information is information which is confidential within the company and protected from external access. If such information were to be accessed by unauthorized persons, it could influence the company's operational effectiveness, cause a financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence and reputation. External access to this information is to be prevented, but should this information become public, the consequences are not critical.

10.2.2 Customer confidential information is customer information that is provided to the company by a customer under an executed non-disclosure agreement or information pertaining to the customer's employees, generated within the process of providing customer service. All such customer confidential information should be protected from external access. If such information were to be accessed by unauthorized persons, it could influence the company's operational effectiveness, cause a financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence and reputation.

10.3 Personally identifiable information ("PII") means any type of information that may be used to identify specific people and their personal traits as defined by applicable laws and regulations. Such data will be considered as sensitive data and will be limited in usage within the company, accessible on a need to know basis only.

10.4 Public information

10.4.1 Information on these systems which has been approved for release to the public.

10.4.2 This does not include any information that could be used for competitive purposes against the company.

10.4.3 Customer confidential information and PII shall be registered as required by The Israeli Law, or as otherwise required by applicable law.

10.4.4 As part of the general purpose of ensuring the security of documents, all documents created within the company are defined as internal confidential information, unless specifically designated otherwise.

## 11. Data Protection

11.1 Customer data is only accessible by customer users and customer support. All stored data is kept encrypted.

11.2 Each customer is provisioned with a unique ID. All application processes are based on that unique ID per customer to help ensure no cross-customer data events occur.

11.3 Data is encrypted in transit.

11.4 Data at rest (on servers, file storage, database) is encrypted using 256 AES.

11.5 Data backups are created in accordance with this policy.

11.6 All stored files are backed up by the relevant cloud provider.

## 12. Risk Assessment Approach

12.1 A periodic risk assessment is the basis for an ongoing information security activity. The assessment is applied to both the technological and non-technological aspects of information security.

12.2 Risk assessment shall include internal and external tests, penetration tests, system configuration reviews, and so on, and shall represent risks based on the potential risk and occurrence likelihood. The assessments and surveys shall be performed in accordance with business requirement and professional advice.

12.3 The risk assessment shall aid with building the work plan that aims to minimize organizational and technological risks, as well as plan specific IT activities.

## 13. Security of Human Resources

Aspects of information security are implemented by the company in all the procedures and stages of recruitment and employment of employees, as specified hereunder:

13.1 Prior to employment:

13.1.1 It is the responsibility of the company to ensure that each employee of the company and third-party employee (contractor's employee) is suitable for the employee's intended position, and that the employee fully understands the responsibilities imposed on the employee, in order to prevent events of failure, fraud, or abuse of information and assets of either the company or its customers.

13.1.2 The management of the company shall define with respect to each of its office holders:

- The necessary qualifications
- Responsibility and authority
- Requirements of reliability
- Access rights to information systems

13.1.3 Employee reliability will be determined through a process of multiple interviews and gathering of recommendations. Employees of third-party providers engaged in delivering services to the company will be interviewed, and two references will be obtained and checked.

13.1.4 Each employee, at any hierarchic level whatsoever, shall sign a confidentiality agreement, whereby he will maintain the rules of information security and privacy, as a condition of his work with the company.

13.1.5 Prior to commencement of work with the company, a new employee will undergo a security and privacy training, in order to become familiarized with the company and its policies, including but not limited to information security.

13.2 Within the process of employment:

13.2.1 It is the responsibility of the management of the company to ensure that employees of the company and third-party employees are aware each of the following:

- Threats to information security
- Their own individual responsibilities as an employee regarding information security
- The company's policies and procedures about information security

13.3 CEO is responsible for the holding of periodic training for all the employees of the company, at all levels of the company, in order to increase their awareness of the following issues:

- Information security policy.
- Familiarization with possible risks and threats to the company and to the information.
- Proper and ethical utilization of assets of the company.
- Manner of protection against possible failures.
- Manner of conduct upon occurrence of an exceptional event.
- Proper and correct use of protections and controls.
- Rules of usage of information systems of the company.

13.4 CEO is responsible for:

13.4.1 Ensuring that all employees receive training in information security and privacy at least once a year.

13.4.2 Examining and reporting on the effectiveness of such training.

13.5 Completion of employment or change of positions:

13.5.1 The management of the company is responsible for ensuring that employee, contractual employee or third-party users of the information systems will leave the organization or change positions in an orderly and safe manner.

13.5.2 If an employee changes position in the company, access authorizations and controls given to the employee in the employee's previous position should be examined to determine whether it is suitable to continue them. As a default, the authorizations of the previous position shall be revoked, and new authorizations suitable for the new position will be given to the employee.

13.5.3 If an employee leaves the company, for any reason, the management of the company should verify that:

- All possibilities of the employee accessing information, supporting systems and assets from the company or outside of it were blocked.
- The employee returned all the assets and equipment that belong to the company (computer equipment, documents, etc.).
- The employee received guidance with respect to ongoing commitment to the information of the company and its protection.

13.6 Training and awareness

13.6.1 Every employee will attend annual information security awareness training.

13.6.2 Every new employee must attend an information security awareness training within one month of commencing employment at the company.

13.6.3 On completion of the information security awareness training, each employee must sign a statement confirming that they have attended the training, understood the material presented, and had an opportunity to ask questions.

13.6.4 CEO must provide refresher courses and other such materials to regularly remind all employees about their obligations about information security.

## 14. Computer Security (Servers and Workstations)

### 14.1 Workstation security

14.1.1 All company issued workstations:

- Will be configured by authorized personnel only.
- Will use full disk encryption and time-based screen savers with information security policy compliant passwords.
- Will be set to automatically install security and operating system updates.
- Must have some form of software-based firewall with intrusion prevention and anti-virus software running at all times on the system.

14.1.2 Any attempt to disable or circumvent the controls referred to in clause 14.1.1 shall be monitored by the IT Manager. If a user disables these controls without approval and such action causes damage to the company's resources, such as a virus outbreak, the user may face disciplinary action up to and including termination of employment.

14.1.3 All installations of operating system level applications will be vetted by the IT Manager.

14.1.4 Where applicable, employees will run applications only with non-elevated permissions.

### 14.2 Server security

14.2.1 Servers will be set up by authorized personnel only and will use either replicated images of existing servers or new images. Servers will be installed with minimal.

14.2.2 All servers will be set to automatically install security and operating system updates.

14.2.3 All software that is run on any company system must be approved by the IT Manager.

14.2.4 Servers will be checked manually for security updates at least once a quarter. In cases where a security update addressing a high level of vulnerability is identified, this will be uploaded within a week.

14.2.5 An external security audit shall be performed on an annual basis to ensure that the company is following industry standards for server security. This also assists the company with identifying any security threats that the company might not be aware of. The IS Manager is responsible for delivering these reports to the proper managers for corrective actions.

14.2.6 Server installation and access control will be managed by authorized personnel only.

### 14.3 Firewalls and encryption

14.3.1 Servers and workstations must be located behind a firewall with a clear security policy. For workstations, standard policy recommended by end point protection software, and for servers each rule base will be based on the minimal set of open ports required to support business transactions.

14.3.2 Access to operating systems will use encrypted protocols (TLS/SSH/RDP).

14.3.3 Firewall rules review and administrator's access should be approved once a quarter by the IS Manager (same as all networking equipment).

## 15. Network Security

15.1 Requirements for network acces

15.1.1 The company bases its networking on a cloud infrastructure and remote access to that infrastructure via public networks.

15.1.2 Access to public networks is not limited in itself, and it is assumed employees connect to non-secure networks.

15.1.3 Access to internal services will be based on strong authentication with additional security processes on top of that (e.g. WAF or device health check, or remote desktop services, as applicable).

15.1.4 All users, regardless of permissions will use strong authentication for sensitive services and all services will require mandatory session encryption.

15.2 Network configuration

15.2.1 The network will be segmented, so that access to production, staging, or development networks will be authorized only based on strong authentication and for authorized personnel.

15.2.2 Authorized IT personnel must attach all new workstations and servers to the network, including uncontrolled development lab environments. Likewise, all new user accounts and new needs for access rights must be created and maintained by authorized IT personnel. The IS Manager must ensure that all systems have current patching and anti-virus controls installed.

15.2.3 All new extranet connectivity shall undergo a security review by the IS Manager. The reviews are to ensure that all access matches the business requirements in the best possible way. All proposed connectivity must be submitted through the change management process.

15.2.4 Outbound connections will be limited to support necessary connections only.

15.3 Wireless security

15.3.1 Wireless communication will be used for employees' workstations only and as such will be considered as non-secured.

## 16. System Access Control

16.1 End-user passwords

16.1.1 Passwords to all the company's information systems must be at least eight alphanumeric characters.

16.1.2 Access to the internal network and sensitive services will be based on strong authentication.

16.1.3 Secure password storage solution will be provided to all employees – such a solution will be used to store passwords and will itself use strong authentication.

16.1.4 Passwords must never be shared with unauthorized users. To do so exposes the authorized user to responsibility for the actions that the other party performs with the disclosed password.

16.1.5 All passwords must be changed immediately if they are suspected of being disclosed or have known to have been disclosed to anyone besides the authorized user.

16.2 Accounts management

16.2.1 All information systems permanently or intermittently connected to the company's networks must have password access controls. Multi-user systems must employ user-IDs and passwords unique to each user, as well as user privilege restrictions. Systems must also have password protected screen savers or screen locks when the system is unattended. Upon assignment of new user accounts, a default password shall be used. The user must be forced to change the password after the first login.

16.2.2 Each administrator's rights must be reviewed once every quarter by the appropriate manager and approvals must be forwarded to the IS MANAGER. Any misuse or unauthorized use of a privileged account or unauthorized information systems access may result in disciplinary action up to and including termination of employment.

16.2.3 When creating and maintaining user accounts, the principle of least privileges required to perform a function must be used when granting permissions.

16.2.4 All default passwords shall be changed immediately after product installation.

16.2.5 Access for non-company's employees, such as contactors or third parties, must be re-authorized annually.

16.2.6 The user's immediate manager must re-evaluate the system privileges granted to every user every 180 days. This re-evaluation involves a determination whether currently enabled system privileges are still needed to perform the user's current duties.

16.2.7 When authorized users are terminated or leave the company, their access must immediately be terminated. This includes all network login accounts, remote access accounts, and system administration level accounts. All root and administrative passwords known to the individual must also be changed.

16.3 Users' data access policy

16.3.1 Corporate data will be stored on shared, authenticated, and secure folders.

16.3.2 Authorized users must not use the company's information systems in order to give access to other information systems to which they do not have authorized access. This includes damaging, alerting, or disrupting any operations of the company's information systems. Likewise, users are prohibited from capturing or obtaining passwords, encryption keys, or any other access control method, which would enable them to have unauthorized access.

16.3.3 Users must not scan for or exploit vulnerabilities or deficiencies in information systems security in order to damage systems or information, to obtain resources beyond those they have been authorized to obtain, to take resources away from other users, or to gain access to other systems for which proper authorization has not been granted. All such vulnerabilities and deficiencies should be promptly reported to the IS MANAGER in accordance with the reporting of security incidents procedures.

16.3.4 Flash drives may not be used for any company related material and their use is generally not recommended.

16.4 Remote access

16.4.1 All access to company servers is considered remote access and will be secured accordingly.

16.4.2 Remote access will be controlled by centrally managed robust solutions that use a combination of different security schemes (WAF, 2FA, device health check, etc.).

16.4.3 Access to sensitive data will be permitted through remote desktop hardened solutions, preventing accidental data copy from the internal network to external devices. This rule shall strictly apply to third parties, and for internal employees shall be at the discretion of the IS Manager.

## 17. Software Security

17.1 License management

17.1.1 The company should strongly support strict adherence to software vendors' license agreements and copyright holder's notices. If the users make unauthorized copies of software, the users are doing so on their behalf, since the company strictly forbids all such copying. Likewise, the company allows reproduction of copy written material only to the extent legally considered "fair use" or with the permission of either the author or publisher.

17.1.2 Software licensed by the company may not be sold, copied, or used for personal reasons or gain.

17.2 Third-party software product security

17.2.1 Each software installation required by company employees will be reviewed and authorized by the IS Manager. The vetting process for third-party software will give preference to known vendors ahead of unknown vendors and will give due consideration to the vendor's performance and compliance with information security standards, processes, and procedures.

17.3 SaaS solutions security

17.3.1 Approval of the IS Manager is required for the use of each third-party SaaS service. For each such service, approval may only be given after receiving suitable confirmation that such service's performance and compliance with information security standards, processes, and procedures are at least on a par with acceptable industry standards.

17.3.2 For SaaS solutions that hold sensitive information the following standards shall apply, at a minimum:

a The company has a security policy

b Strong authentication is supported

c Encrypted protocols are the only ones supported

17.3.3 SaaS solutions will be classified according to their sensitive information level and employees will be notified.

17.3.4 All sensitive data services used by company employees for business processes will be vetted by the IS Manager+ and will be configured to support the highest level of security available, focusing on managing permissions and securing authentication.

## 18. R&D Security

18.1 The company shall have a secure development policy, adhering to standard best practices. The policy shall be maintained by the VP R&D and reviewed by the IS Manager on an annual basis.

18.2 Third party code packages will be updated regularly and scanned for vulnerabilities once a year at least.

18.3 Any software package used in the company's production environment will be authorized by the VP R&D.

18.4 Application access control

18.4.1 All applications must support user authentication and permission management.

18.5 Application firewalls

18.5.1 All applications that are accessible through an external network and are intended for customer or non-authenticated use must have a web-application-based firewall in addition to a network-based firewall in order to prevent unauthorized users from exploiting vulnerabilities and/or gain unauthorized access through the applications.

18.6 Internal and external applications vulnerability testing

18.6.1 All applications must go through an application vulnerability assessment in order to identify known exploits. All applications that process, transmit, or store privacy information must have all vulnerabilities identified and corrected.

18.7 Development change control guidelines

The following actions will be taken:

18.7.1 The product owner will complete a form requesting approval of changes in system applications and infrastructures.

18.7.2 The product owner will submit the request to the project manager, who will assess the change's feasibility.

18.7.3 If the change is feasible, the project manager will pass on the request to the development manager and IS Manager.

18.7.4 If complying with the request involves a change that affects a different application, the system owner of that application's approval is also required.

18.7.5 Existing controls will be audited to make sure they are not compromised by the changes.

18.7.6 Identifying the applications and infrastructures that need to be modified following the change requested.

18.7.7 Making sure the system documentation is updated upon completing each change.

18.7.8 Version management of all software updates.

18.7.9 Maintaining an audit path of all change requests.

18.7.10 Making sure the operational documentation and user procedures have been updated as required.

18.7.11 Making sure the change is being implemented in a way that minimizes disturbances to the normal work routine in the company and in the unit in particular.

18.7.12 Information security tests must be carried out following the changes.

## 19. Electronic Mail Systems and Internet Usage

19.1 Electronic mail systems

19.1.1 Users must not use an email account assigned to another user to either send or receive messages.

19.1.2 When users receive an email which security software has identified as malicious or they suspect to be malicious, they should report to the IS Manager immediately and wait for instructions.

19.1.3 Users must use their discretion when sending customers' confidential information by email. When in doubt, users must consult the IS Manager or the VP R&D.

19.2 Internet connections

19.2.1 Although the internet is an informal communications environment, the laws for copyrights, patents, trademarks, and the like still apply. To this end, users of the company's information systems must for example (1) repost material only after obtaining permission from the source, (2) quote material from other sources only if these sources are identified, and (3) reveal internal company's information on the Internet only if the information has been officially approved for public release.  This also forbids the online trading of copyrighted material. An example of this is file-swapping copyrighted material through the internet.

19.2.2 Users must not place any company materials on any publicly accessible internet computer system unless the IS Manager or a company Vice-President first approved the posting.

## 20. Third Party Security

20.1 Contractual obligations:

20.1.1 Exchanges of in-house software or internal information between the company and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange as well as the ways in which the software or information is to be handled and protected. This policy does not cover the release of information designated as public (marketing materials, social media postings, recruitment material, and so on).

20.1.2 All new connection requests between third parties and the company require that the third party and the company's representatives agree to and sign the company's NDA Agreement form. This agreement must be signed by a designated senior manager in the company as well as a representative from the third party who is legally empowered to sign on behalf of the third party. All third parties may only be connected to the internal network upon approval of the IS Manager.

20.2 Remote access

20.2.1 Inbound access or inbound internet privileges must not be given to third-party vendors unless the IS Manager determines that these vendors have a legitimate business need for such access. This type of access must be enabled for specific authorized users for the time period required to accomplish the approved task. All approved third-party access must be documented and reviewed on a quarterly basis.

20.2.2 Each individual connecting to the company's network will be briefed by the IS Manager regarding security, privacy and authorized actions.

## 21. Physical Security

21.1 Access security to company offices

21.1.1 The entrance to company premises shall be secured and monitored at all times (during work hours and thereafter).

21.1.2 The entrance doors to the offices shall be closed and locked at all times

21.1.3 Upon completion of the workday, the offices of the company shall be locked and the alarm of the security company shall be activated.

21.1.4 Monitoring cameras shall be placed in order to trace access to the offices of the company during and after work hours.

21.2 Security in work areas

21.2.1 Employees of the company work at different locations, at home or at public places. In public places employees should make sure to have their laptops with them at all times, including when getting up from their seats.

21.2.2 If a situation arises that requires an employee to leave a laptop unattended, that computer should be locked using a password protected screensaver.

21.2.3 When going on vacation, employees shall turn off their computers or put them into hibernate mode (as this forces encryption sequence).

21.3 Clean desk

21.3.1 Every employee is responsible for the information security in their own work environment, the equipment provided to the employee by the company and also to any resource of the company used or held by or accessible to the employee in the work environment.

21.3.2 As a general rule, employees will not leave company documents unattended in public places, even for a split second.

21.4 Proper disposal of physical information

21.4.1 Any physical information that contains any information other than public information must be properly disposed of. This includes placing all paper with all confidential content to be shredded or placed in a secured shred bin. All the company's confidential information must be shredded prior to being removed from the premises. All removable media that contains any information other than public information must be controlled until the information has been erased or the physical media has been destroyed.

## 22. Reporting of Security Incidents

22.1 Employee responsibilities

22.1.1 All suspected information security events must be immediately reported through the proper company internal channels to the IS Manager or to the CEO. The preferred method is to report suspected incidents using phone or WhatsApp.

22.1.2 Company users have the duty to properly report all information security violations and problems to the IS Manager on a timely basis so that prompt remedial action may be taken.

22.1.3 Unauthorized disclosures of any company's information must be reported to the IS Manager who shall notify the involved information owners.

22.1.4 Any attempt to interfere with, prevent, obstruct, or dissuade a staff member in their efforts to report a suspected information security problem or violation is strictly prohibited and is cause for disciplinary action.

22.1.5 Any retaliation against an individual reporting or investigating information security problems or violations is also prohibited and is cause for disciplinary action.

22.1.6 The company shall protect users, who report in good faith, what they believe to be a violation of information security policies. This means that such employees shall not be terminated, threatened, or discriminated against because they report what they perceive to be a wrongdoing or dangerous situation.

22.2 Reporting and corrective actions

22.2.1 Whenever evidence clearly shows that a computer has been a victim of a communications crime, the IS Manager must immediately conduct proper forensics and assist with the reporting processes. The investigation must provide sufficient information so that management can take appropriate action to ensure that (1) such incidents shall not be likely to happen again, and (2) effective security measures have been re-established (3) provide required information to customers and legal authorities as required by law and regulations.

22.2.2 Information describing all reported information security problems and violations must be retained for a period of two years.

## 23. Malware

23.1 Malware is an unauthorized program that uses various techniques to steal, change or delete information. The symptoms of malware infection might include slow response times, inexplicable loss of files, changed modification dates for files, increased file sizes, and the total failure of a computer, and so on.

23.2 To assure continued uninterrupted service for all information systems, all workstations must have approved virus-screening software enabled on their computers. All removable media needs to be scanned for viruses before use in any information system. Disabling the anti-virus software can lead to disciplinary actions, including termination.

23.3 Server protection will be based on whitelisting permitted outbound access, automatic security patching, and automated monitoring to detect Command & Control instances.

23.4 Employees must immediately update the IS Manager if malware is detected on a computer they use. This action allows steps to be promptly taken in order to ensure that no further infection occurs.

23.5 Endpoints shall have automatic update of current virus definition files as the source vendor issues them.

## 24. Data Backups

24.1 On laptops, information will only be backed up if saved in One Drive.

24.2 Database backups will occur daily for live databases (excluding read-only databases) or will be replicated to a computer in a different geographical region.

24.3 Source code is backed up on a daily basis by Gihub.

24.4 Information retrieval

24.4.1 Once every six months a restore operation will take place for main data components to verify that backup tools are working as expected.

24.4.2 The following full retrieval activities shall be executed: retrieval of server or system, including all their contents, executed only after crash of server/system or once a year, in order to verify the ordered condition of the backup.

## 25. Monitoring

25.1 The object of monitoring is to discover unauthorized information-processing activities.

25.2 Threat monitoring tools will be enabled on internal and external interfaces. Where applicable, security monitoring alerts will be written to allow quick visibility.

25.3 All the actions of users of the information systems of the company are recorded on the monitoring system, in order to uphold a process of monitoring and documentation upon occurrence of information security incidents or a deviation from the information security policy adopted by the company.

25.4 Whenever an employee has a good reason to believe that an information system has been compromised, the employee should report the incident to the IS Manager in accordance with the reporting of security incidents procedures. The only exception to this policy is if the system causes immediate damage to the company's resources, in which case, in addition, the system is to be disconnected from the network.

## 26. Security Training

26.1 Security training for employees or third-party employees shall include the following:

26.1.1 Proper use of company resources, including licenses, and personal use.

26.1.2 Proper use of the company's mail service.

26.1.3 Backup guidelines.

26.1.4 Installation of applications, including desktop applications and SaaS add-ons.

26.1.5 Public posting of information about the company.

26.1.6 Selection and storage of access keys, passwords, and so on.

26.1.7 Usage of flash drives.

26.1.8 Reporting of security incidents.

## 27. 27 Development

27.1 Development tools and techniques

27.1.1 Before a new system is developed or acquired, R&D manager must clearly specify the relevant security requirements. Alternatives must be reviewed with the developers or vendors so that an appropriate balance is reached between security and other objectives.

27.1.2 Management must ensure that all software development and software maintenance activities performed by in-house staff adhere to the company's security policies, standards, procedures, and other system development conventions.

27.1.3 Any deployment of code to production will go through a review process by the VP R&D or the CTO.

27.1.4 Different code branches will be managed for staging and production and appropriate methods will be employed to make sure staging doesn't go into production and vice versa.

27.1.5 Access to staging areas and production will be restricted and secured with appropriate safeguards.

27.2 Testing of newly developed software

27.2.1 All software developed will require minimal privileges and will be tested in staging with the same permission set required for production. Programming usability shortcuts may only exist in local environments.

27.2.2 Business application software development staff shall not be granted access to production information with the exception of the production information relevant to the particular application software, on which they are currently working.

## 28. Change Control

28.1 Change control policy

28.1.1 All computer and communication systems used for production processing at the company must employ a formal change control procedure, which ensures that only authorized changes are made. This change control procedure must be used for all changes to software, hardware, communication networks, and related procedures.

28.1.2 All security problem-fix software, command scripts, and the like provided by operating system vendors, official computer emergency response teams, and other trusted third parties must go through change management. If vulnerability needs immediate attention, it should be escalated to change management review for prompt approval of the changes.

## 29. Management of Business Continuity

29.1 The purpose of the operation is to minimize disruptions to the operations of the business and to protect critical business procedures from the effect of serious failures of the information systems or disasters, assuring recovery of the necessary resources for continuation of functioning of the company.

29.2 Within the framework of management services, resources of the company that are essential on emergency shall be defined, as well as defining a recovery program upon occurrence of a disaster, pursuant to the continuance of rendering a reliable and efficient service to customers of the company.

29.3 As part of the company's business continuity plan, the following main scenarios were examined:

29.3.1 **Activity disabling the company's server** In this case the company's operations will be stopped until the backup server has been recovered. The servers will be set up within 48 hours of downtime.

29.3.2 **Disabling employee abilities to work (mass internet outages in Israel, an event of war** In such cases the company's management would consider alternatives and would move to minimal viable service mode until national issues resolve.

## 30. Adjustment

30.1 Adjustment to the requirements by law and regulatory requirements:

30.1.1 The management of the company applies the laws, standards and additional regulatory respondents, applying to the company.

30.1.2 The CEO of the company is responsible for verifying that all the employees of the company are aware of the applicable laws, regulations, and procedures.

30.1.3 Identification of laws and regulations on information issues:

- Rights of intellectual property
- Legal evidence and records of the company
- Right to privacy
- Business and economic confidentiality
- Prevention of abuse of information-processing possibilities.

30.1.4 By adopting this information security system, the management of the company fulfills and implements the following aspects of information security, which it is interested and obligated to meet:

- Information security management standards - Israeli Standard ISO 27001
- The Computers Law, 1995
- Privacy Protection Law, 1981
- Copyrights Law, 2007
- Working according to overseas regulatory requirements.
- European General Data Protection Regulation, 2016

30.2 At least once a year, a "management survey" on issues of information privacy, quality and security is held in order to examine and report on the degree of adjustment of the policy that was adopted to the actual occurrences.

30.3 Internal tests are executed in the organization at least once a year, in order to examine the degree of adjustment of the assistance and procedures to the organizational security policy.

30.4 Within the framework of the surveys and the adjustment tests, the degree of strength of the infrastructure of the information systems against hazards and malicious software will be examined.

## 31. Controls and Auditing

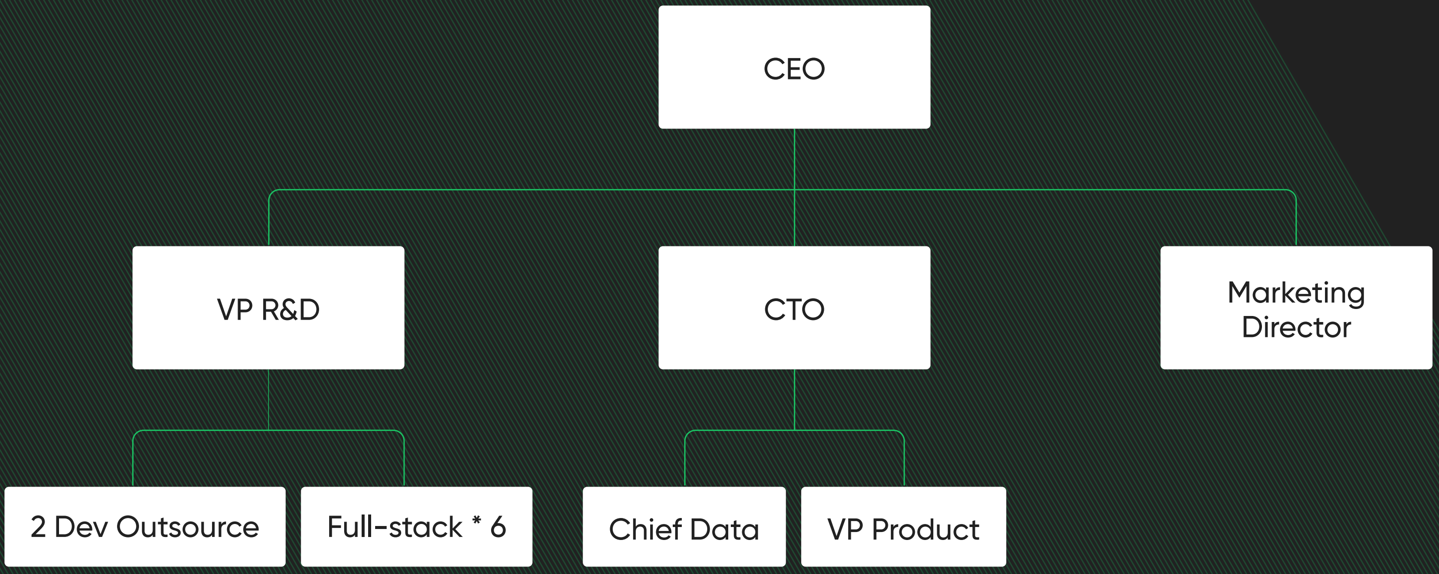
31.1 All procedures shall have controls designated to assure the proper implementation of the procedure.

31.2 Audit trails shall be implemented in the various systems and shall be regularly monitored and controlled.

## 32. Responsibility

32.1 The IS Manager is responsible for implementing and maintaining this policy.

## Appendix – Organizational Chart


CEO
VP R&D
CTO
Marketing Director
2 Dev Outsource
Full-stack * 6
Chief Data
VP Product