INFORMATION SECURITY POLICY

VALIGARA ONLINE LTD
HAMAKLEF 3
HAIFA, 3125301
ISRAEL

Version ID	Title, summary	Author	Revision date
0.1.0	Initialization, procedures	Ilya Lifshits	20.04.2017
0.2.0	Team definition	Igor Nusinovich	12.06.2017
1.0.0	Approved, distributed	Igor Nusinovich	12.07.2017
1.0.1	Review	Igor Nusinovich	07.07.2018
1.0.2	Review	Igor Nusinovich	03.09.2019
1.0.4	Review	Igor Nusinovich	28.11.2020

TABLE OF CONTENTS

1.1. Purpose

This Security Policy document is aimed to define the security requirements for the proper and secure use of the Information Technology services in the Valigara Online Ltd (following "Organization"). Its goal is to protect the Organization and users to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation and business outcomes.

1.2. Scope

This document applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. Compliance with policies in this document is mandatory for this constituency.

1.3. Responsibilities

Roles	Responsibilities
Chief Information Officer	• Accountable for all aspects of the Organization's information security.
Information Security Officer	• Responsible for the security of the IT infrastructure. • Plan against security threats, vulnerabilities, and risks. • Implement and maintain Security Policy documents. • Ensure security training programs. • Ensure IT infrastructure supports Security Policies. • Respond to information security incidents. • Help in disaster recovery plans.
Information Owners	• Help with the security requirements for their specific area. • Determine the privileges and access rights to the resources within their areas.
IT Security Team	• Implements and operates IT security. • Implements the privileges and access rights to the resources. • Supports Security Policies.
Users	• Meet Security Policies. • Report any attempted security breaches.

1.4. General Policy Definitions

1. Exceptions to the policies defined in any part of this document may only be authorized by the Information Security Officer. In those cases, specific procedures may be put in place to handle request and authorization for exceptions.
2. Every time a policy exception is invoked, an entry must be entered into a security log specifying the date and time, description, reason for the exception and how the risk was managed.
3. All the IT services should be used in compliance with the technical and security requirements defined in the design of the services.
4. Infractions of the policies in this document may lead to disciplinary actions. In some serious cases they could even led to prosecution.

1. IT Assets Policy

1.1. Purpose

The IT Assets Policy section defines the requirements for the proper and secure handling of all the IT assets in the Organization.

1.2. Scope

The policy applies to desktops, laptops, printers and other equipment, to applications and software, to anyone using those assets including internal users, temporary workers and visitors, and in general to any resource and capabilities involved in the provision of the IT services.

1.3. Policy Definitions

1. IT assets must only be used in connection with the business activities they are assigned and / or authorized.
2. All the IT assets must be classified into one of the categories in the Organization's security categories; according to the current business function they are assigned to.
3. Every user is responsible for the preservation and correct use of the IT assets they have been assigned.
4. All the IT assets must be in locations with security access restrictions, environmental conditions and layout according to the security classification and technical specifications of the aforementioned assets.
5. Active desktop and laptops must be secured if left unattended. Whenever possible, this policy should be automatically enforced.

6. Access to assets is forbidden for non-authorized personnel. Granting access to the assets involved in the provision of a service must be done through the approved Service Request Management and Access Management processes.
7. All personnel interacting with the IT assets must have the proper training.
8. Access to assets in the Organization location must be restricted and properly authorized, including those accessing remotely. Company's laptops, PDAs and other equipment used at external location must be periodically checked and maintained.
9. Whenever possible, encryption and erasing technologies should be implemented in portable assets in case they were stolen.
10. Losses, theft, damages, tampering or other incident related to assets that compromises security must be reported as soon as possible to the Information Security Officer.
11. Disposal of the assets must be done according to the specific procedures for the protection of the information. Assets storing confidential information must be physically destroyed in the presence of an Information Security Team member. Assets storing sensitive information must be completely erased in the presence of an Information Security Team member before disposing.

2. Access Control Policy

2.1. Purpose

The Access Control Policy section defines the requirements for the proper and secure control of access to IT services and infrastructure in the Organization.

2.2. Scope

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

2.3. Policy Definitions

1. Any system that handles valuable information must be protected with a password-based access control system.
2. Discretionary access control list must be in place to control the access to resources for different groups of users.
3. Mandatory access controls should be in place to regulate access by process operating on behalf of users.
4. Access shall be granted under the principle of "less privilege", i.e., each identity should receive the minimum rights and access to resources needed for them to be able to perform successfully their business functions.
5. Revoking User Access

- When an employee departs from the Organization, access to assets with a high or moderate asset classification is required to be revoked or disabled within 24 hours.
- If the departing employee had access to shared system, service and/or default accounts passwords, those passwords must be changed.

3. PHYSICAL SECURITY POLICY

3.1. Purpose

The Physical Security Policy section defines the requirements for the proper and secure control of access to the head office facilities in the Organization.

3.2. Scope

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

3.3. Policy Definitions

1. Physical Security. Access to the Haifa office facilities are restricted via a fingerprint authentication system to help ensure only authorized and active personnel can access the office facility.
2. The offices are locked 24 hours a day, 7 days a week. Employees are required to be issued a unique fingerprint identification access. The fingerprint authentication is configured to log access attempts for review in the event of an incident that requires investigation.
3. Fingerprint Access Revocation. When the employee departs from the Organization, the IT team is responsible to remove the respective fingerprint identification, to prevent further access to the Organization office facilities.
4. Visitor Access. Visitors to the Organization office facility are required to be escorted at all times while on the premise. In the event an unknown person is discovered within the Organization office space, they are removed from the office space immediately.
5. Clear Desk. Organization employees must clear Restricted and/or Sensitive documents from their desktops when left unattended. Sensitive materials are physically secured and/or destroyed when not in use.

4. PASSWORD CONTROL POLICY

4.1. Purpose

The Password Control Policy section defines the requirements for the proper and secure handling of passwords in the Organization.

4.2. Scope

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

4.3. Policy Definitions

1. Any system that handles valuable information must be protected with a password-based access control system.
2. Every user must have a separate, private identity for accessing IT network services.
3. Identities should be centrally created and managed. Single sign-on for accessing multiple services is encouraged.
4. Each identity must have a strong, private, alphanumeric password to be able to access any service. They should be as least 8 characters long.
5. Sharing of passwords is forbidden. They should not be revealed or exposed to public sight.
6. Whenever a password is deemed compromised, it must be changed immediately.
7. Identities must be locked if password guessing is suspected on the account.
8. Password Requirements
    - Passwords must be used and maintained in a manner that helps ensure the safety and security of the Organization systems and data.
    - The following is enforced:
        - Minimum password length = 8 characters
        - Production platform Lockout - 4 invalid login attempts
        - Non-production systems Lockout - 7 invalid login attempts

5. SOFTWARE DEVELOPMENT

5.1. Purpose

The Software development section defines the requirements for the proper and secure software development in the Organization.

5.2. Scope

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

5.3. Policy Definitions

1. Organization’s Product and Engineering teams perform system development activities. These teams each participate in the Agile system development life cycle (SDLC). The SDLC includes multiple teams utilizing Scrum methodologies. The development life cycle

includes a number of controls to help ensure development efforts are coded well and securely.
2. Production Release and Approval. Changes are required to be approved by authorized personnel prior to being implemented into the production environment.
3. Separation of Environments. Proprietary and Confidential development activities should be performed in an environment that is logically separate from Organization's production environment.

6. Data Backups

6.1. Purpose

The Data Backups section defines the requirements for the proper and secure backup of all existing data in the Organization.

6.2. Scope

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

6.3. Policy Definitions

1. The Organization maintains a comprehensive backup solution of both structured and unstructured data stored on the platform.
2. Full data backup is performed on at nightly basis. Incremental backups of the structured data are performed on a hourly basis
3. Monitoring. The personnel perform weekly reviews of the automated backup system and resolve the backup failure.
4. Backup Retention.
    a. Non-Structured data backups are retained on a seven-day rolling schedule.
    b. Clients' Databases backups are retained on a 30-day rolling schedule.

7. Servers and Network Security

7.1. Purpose

The Internet Policy section defines the requirements for the proper and secure access to Organization production servers and network.

7.2. Scope

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

7.3. Policy Definitions

1. Valigara Online Manager platform is built on Hetzner and Amazon Web Services (AWS). As part of Hetzner and AWS' service offering, they are responsible for physical and environmental security, availability, routing, switching and certain networking controls. AWS data centers are equipped with state-of-the-art physical security controls including, multi-factor authentication (badge access card and biometric), strict role-based access, security guard monitoring, video surveillance systems, and access logging and monitoring. In addition, AWS has environmental security controls within their data centers to ensure their systems remain fully operational that include; redundant generators, uninterruptable power supply (UPS) systems, cooling systems, and fire detection and suppression systems.
2. The policies below are the responsibilities of the Organization.
    a. The system must be configured to have only essential capabilities enabled, and have unnecessary services, functions, ports and protocols disabled.
    b. Remote access to production systems and data is required to be restricted to authorized personnel commensurate with job responsibilities.
    c. Authentication requirements require at a minimum, two-factor authentication (e.g. - user account, password and a one-time security token or a user account, password and a key pair).

8. INTERNET POLICY

8.1. Purpose

The Internet Policy section defines the requirements for the proper and secure access to Internet.

8.2. Scope

This policy applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

8.3. Policy Definitions

1. The use of Messenger service is permitted for business purposes.
2. Internet access is mainly for business purpose. Some limited personal navigation is permitted if in doing so there is no perceptible consumption of the Organization system resources and the productivity of the work is not affected. Personal navigation is discouraged during working hours.
3. Access to pornographic sites, hacking sites, and other risky sites is strongly discouraged.
4. In accessing Internet, users must behave in a way compatible with the prestige of the Organization. Attacks like denial of service, spam, fishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.

5. Reasonable measures must be in place at servers, workstations and equipment for detection and prevention of attacks and abuse. They include firewalls, intrusion detection and others.
6. Wireless access to the Organization office facility networks must be protected via the Wi-Fi Protected Access II (WPA2) protocol that utilizes AES-256 encryption for wireless network traffic.

9. INFORMATION CLASSIFICATION POLICY

9.1. Purpose

The Information Classification Policy section defines a framework for the classification of the information according to its importance and risks involved. It is aimed at ensuring the appropriate integrity, confidentiality and availability of the Organization information.

9.2. Scope

This policy applies to all the information created, owned or managed by the Organization, including those stored in electronic or magnetic forms and those printed in paper.

9.3. Policy Definitions

1. Information owners must ensure the security of their information and the systems that support it.
2. Information Security Management is responsible for ensuring the confidentiality, integrity and availability of the Organization's assets, information, data and IT services.
3. Any breach must be reported immediately to the Information Security Officer. If needed, the appropriate countermeasures must be activated to assess and control damages.
4. Information in the Organization is classified according to its security impact. The current categories are:

Categorization	Definition	Examples
confidential	Only a limited number of persons must have access to it. Management, access and responsibilities for confidential information must be handled with special procedures defined by Information Security Management.	Data - Regulated (PII etc) - Source code - Customer data Systems - AWS - GitLab - Hubspot

sensitive	Handled by a greater number of persons. It is needed for the daily performing of jobs duties, but should not be shared outside of the scope needed for the performing of the related function.	Data - Email - Financials Systems - Telegram - Hubspot - YouTrack
shareable	Can be shared outside of the limits of the Organization, for those clients, organizations, regulators, etc. who acquire or should get access to it.	Data - Price lists - Affiliate programs - Personal session videos
public	can be shared as public records, e.g. content published in the company's public Web Site.	- Marketing Assets - Press Releases - Product videos

Information is classified jointly by the Information Security Officer and the Information Owner.

10. Remote Access Policy

10.1. Purpose

The Remote Access Policy section defines the requirements for the secure remote access to the Organization's internal resources.

10.2. Scope

This policy applies to the users and devices that need access the Organization's internal resources from remote locations.

10.3. Policy Definitions

1. Organization supports employees working remotely (contingent on manager/supervisor approval). Employees that are approved to work remotely are required to adhere to the policies outlined in this information security policy.
2. Users must not connect from public computers unless the access is for viewing public content.

11. Outsourcing Policy

11.1. Purpose

The Outsourcing Policy section defines the requirements needed to minimize the risks associated with the outsourcing of IT services, functions and processes.

11.2. Scope

This policy applies to the Organization; the services providers to whom IT services, functions or processes are been outsourced, and the outsourcing process itself.

11.3. Policy Definitions

1. Before outsourcing any service, function or process, a careful strategy must be followed to evaluate the risk and financial implications.
2. The service provider should be selected after evaluating their reputation, experience in the type of service to be provided, offers and warranties. Reference checks, Internet research, comparative analysis with other vendors are used while selecting the provider.
3. Audits should be planned in advance to evaluate the performance of the service provider before and during the provision of the outsourced service, function or process.
4. The service provider must get authorization from the Organization if it intends to hire a third party to support the outsourced service, function or process.

12. INCIDENT MANAGEMENT

12.1. Purpose

The Incident Management Policy section defines the procedures undertaken in the company on the accurance of any security incident.

12.2. Scope

This policy applies to the Organization, all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

12.3. Policy Definitions

1. The Organization has developed the “Valigara Incident Response Plan”, which summarizes the policies and procedures related to this topic.
2. All security-related incidents are dealt with as quickly as possible – thus, all suspected information security incidents must be reported as quickly as possible.
3. Security incidents must be immediately communicated to Security and Trust personnel via e-mail, incident submission forms, phone or through the internal chat system.

13. Non-compliance with a Policy and/or Procedure

Any employee found to have violated a policy and/or procedure may be subject to discipline, up to and including termination of employment. A violation of this and/or procedure by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with the Organization.

14. Policy Review

The Organization Security and Trust team is responsible for reviewing and updating policies on an annual basis or when there is a significant change to the associated policy and/or procedure.

The Organization C-Level employee is responsible for approving the updated procedures as evidenced within the “Approval” table.

15. Annex

1.1. Glossary

Term	Definition
Access Management	The process responsible for allowing users to make use of IT services, data or other assets.
Asset	Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service.
Audit	Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.
Confidentiality	A security principle that requires that data should only be accessed by authorized people.
External Service Provider	An IT service provider that is part of a different organization from its customer.
Identity	A unique name that is used to identify a user, person or role.
Information Security Policy	The policy that governs the organization’s approach to information security management
Outsourcing	Using an external service provider to manage IT services.
Policy	Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, IT infrastructure etc.

Term	Definition
Risk	A possible event that could cause harm or loss, or affect the ability to achieve objectives.
Service Level	Measured and reported achievement against one or more service level targets.
Warranty	Assurance that a product or service will meet agreed requirements.

Table 1. Glossary.