	Information Security Policy and Data Protection	
Date of Approval: 23/01/2026	Approved by: Dafna Picker דפנה פיקר מנהלת משאבי אנוש	QIT – 02EN REV 1

Purpose

This document defines the information security principles, controls, and responsibilities governing the protection of all organizational information assets - including those managed within the SharePoint / Microsoft 365 environment - in accordance with the principles of ISO/IEC 27001 and applicable privacy regulations. The policy aims to ensure the confidentiality, integrity, and availability of organizational information and to demonstrate the organization's commitment to responsible information management.

Work Environment and System

The organization applies information classification principles in practice through access controls, folder permissions, and system-level restrictions - ensuring that not all employees have access to all content. The following classification levels serve as the guiding framework for access and handling decisions:

Information Security Principles

Organizational information security is based on the following principles (applicable across all systems and environments, including SharePoint):

- Segregation of Duties - assigning permissions according to role and areas of responsibility.
- Least Privilege - each user is granted access only to the information required for their role.
- Identity and access management.
- Monitoring and control of information usage.
- Implementing access controls and information protection according to business needs, organizational structure, and authorization levels.

Information Classification

Organizational information is classified into the following levels, each with corresponding handling and protection requirements:

- Public - Information approved for external distribution (e.g., marketing materials, public reports).
- Internal - General organizational information for internal use only; not for external sharing without authorization.
- Confidential - Sensitive business information (e.g., financial data, contracts, personal data); restricted to authorized personnel only.
- Restricted - Highly sensitive information (e.g., trade secrets, personal health data); access strictly limited on a need-to-know basis with additional controls.

Authentication Mechanisms

Access to the system is controlled through:

- Multi-Factor Authentication (MFA)
  Each user is required to authenticate using a password and an additional verification method, such as a one-time code sent to a mobile device or an authentication app.
- Secure password management
  Strong password requirements, periodic updates, and user lockout after failed attempts.
- Centralized identity management
  Users are managed under the organization's identity system (Azure AD / Entra ID).

Permissions and Information Access

The logical security of information is based on:

- Defining permissions at the library and folder level
  Access is granted only to authorized users according to business need.
- User groups (Security Groups)
  Access is managed through groups by department/role for convenient control and supervision.
- Separation of sensitive information
  Dedicated libraries for sensitive information with stricter access restrictions.
- External sharing control
  Sharing information outside the organization is restricted, controlled, and requires special permissions.

Monitoring, Control, and Documentation

- Audit Logs
  Recording user actions such as viewing, editing, and sharing files.
- Alerts for unusual activity.
- Periodic access permission reviews.
- Tracking document changes (Version Control).

Information Protection and Regulatory Compliance

- Encryption of data in transit and at rest.
- Infrastructure exists to support information classification and protection mechanisms, including DLP capabilities, according to organizational requirements, business needs, and regulatory requirements.

- Compliance with the service provider's information security standards (Microsoft).
- Alignment with privacy protection principles and applicable regulations, including the Israeli Privacy Protection Law and the General Data Protection Regulation (GDPR) where applicable.

Personal Data Protection and Privacy

Plasel is committed to protecting the personal data of employees, customers, and other stakeholders in accordance with applicable privacy laws. Key principles include:

- Personal data is collected and processed only for lawful, specified purposes and retained only as long as necessary.
- Data subjects have the right to access, correct, and request deletion of their personal data.
- Personal data is not shared with third parties without a lawful basis or explicit consent, except where required by law.
- Data retention and deletion schedules are defined and enforced according to regulatory requirements.

Security Incident Management

Security incident management is practiced within the organization, including employee awareness of reporting obligations and established procedures for handling incidents. The process includes the following steps:

- Detection and Reporting - All employees are required to report suspected security incidents immediately to the IT department.
- Containment and Remediation - The IT department assesses the incident, contains the threat, and restores affected systems as quickly as possible.
- Notification - In the event of a personal data breach, affected parties and relevant authorities are notified within the timeframes required by applicable law (e.g., 72 hours under GDPR).
- Post-Incident Review - All significant incidents are reviewed to identify root causes and prevent recurrence. Findings are documented and used to improve controls.

Third-Party and Supplier Security

The organization manages information security risks associated with third-party suppliers and service providers:

- Suppliers with access to organizational data or systems are required to agree to contractual security requirements and confidentiality obligations (NDA). As of the date of this policy, the process of ensuring NDA coverage for all relevant suppliers is

ongoing; the organization is committed to expanding this coverage as a priority action.

- Supplier security risks are assessed prior to engagement and reviewed periodically.
- Third-party access to organizational systems is granted on a least-privilege basis and revoked immediately upon contract termination.

Training and Employee Awareness

- Annual information security training for all employees, delivered via an e-learning module.
- Guidelines for proper use of information and file sharing.
- Raising awareness of cyber risks such as phishing, unauthorized access, and similar threats.

Risk Management and Continuous Improvement

The organization performs:

- Periodic information security risk assessments.
- Procedure updates in response to changing threats.
- Continuous improvement of security controls.

Summary

The organization is committed to maintaining a high level of information security across all systems and environments. This policy is aligned with the principles of ISO/IEC 27001 and applicable privacy regulations (GDPR / Israeli Privacy Protection Law), ensuring the protection of organizational and personal data, responsible information management, and continuous improvement of security controls. This policy is reviewed annually and updated as required in response to changes in the threat landscape, regulatory environment, or business operations.

Responsibility

Policy Owner: The IT Manager / CISO is responsible for maintaining, reviewing, and updating this policy on an annual basis. Department Managers are responsible for ensuring compliance within their teams. All Employees are responsible for adhering to this policy and reporting any suspected security incidents or violations to the IT department promptly.