DATA SECURITY POLICY

Version 1st

FEBRUARY 2025

VERSION. REVISION / DATE:	ISSUE	APPROVAL
01.02 / 01.02.2025	QA	GENERAL MANAGER

Contents

1. Versions – Amendments

VERSION HISTORY					
VERSION	APPROVAL	REVISED BY	DATE	AMENDMENT	ISSUE
1	General Manager	QA	01.02.2025	Initial version	SustChem SA

2. List of Recipients

A/A	Company Position	Number of Copy	Name- Signature of Recipient	Date
01.02	Management/ RDPM	1	RDPM	01/02/2025

3. Purpose

This document describes the policy of **COSTAS A. PAPELLINAS (HELLAS) S.A. (CPO Greece)** regarding the organization of data security management that falls within the scope of the Security Management System.

4. Interested parties

The interested parties have been identified by the company's management and are reviewed in the system review conducted annually.

5. Scope/ Exemptions

The Management Systems of **COSTAS A. PAPELLINAS (HELLAS) S.A. (CPO Greece)** include its Organizational Structure, the security policies and procedures followed, as well as the resources (human resources, facilities, and means) available to the company for achieving Information Security Management.

5.1. Exemptions from the Management Systems

Exemptions from Annex A of the standard are mentioned in the SOA - Statement Of Applicability document.

5.2. Organizational Structures

The Management Systems cover all the organizational units of the company, as shown in the company's organizational chart. The organizational chart is reviewed annually during the Management Review. They also cover the following partners of the company, to the extent that they are involved in processes that fall under the Management Systems:

- Equipment suppliers
- Service providers
- External partners the company works with on specific projects, with whom cooperation agreements/contracts are signed.

Finally, it includes the customers of **COSTAS A. PAPELLINAS (HELLAS) S.A. (CPO Greece)** who receive services that fall within its area of operation.

5.3. Data and Telecommunication Infrastructures

The management systems concern the following equipment/software elements:

- Data systems and applications supporting business processes
- Central equipment and system software
- User workstations and laptops and related software (operating systems, office automation software)
- Peripheral equipment (copiers, multi-function devices, printers, scanners)
- Systems for power outage protection
- Cabling infrastructure, active and passive network equipment, wireless networks, air conditioning, and other telecommunications equipment as related to the scope of the Management Systems.

5.4. Data in Electronic Format

The company's operation relies on the maintenance and processing of a range of data for both internal use and customer data. These data are mainly kept in electronic format in the company's information systems and include (indicatively):

- General use files
- Contract documents, Project Management, Financial
- Administrative files and documents
- Product files and documents
- Completed project documents
- Ongoing project documents

- Contracts (projects, partners, etc.)
- Labor-related documents, social security files, etc.
- Payroll
- Customer data

5.5. Data in Physical (Non-Electronic) Format

The category of non-electronic data covered by the Management Systems includes various types of documents related to and affecting the company's operations (e.g., incoming physical documents by mail and fax, documents requiring physical signatures, project contracts, invoices, etc.). Indicative files kept in physical format include:

- Tax files (income tax, VAT, etc.)
- Invoices
- Labor-related documents, social security files, etc.
- Copies of contracts
- Service provision documents
- Completed project documents
- Ongoing project documents
- Customer data

6. Data Security Policy

6.1. Structure of the Data Security Policy

The information security policy of **COSTAS A. PAPELLINAS (HELLAS) S.A. (CPO Greece)** consists of:

- This general security policy, which includes the company's objectives for the protection of its information, the commitment of the management for the implementation of the Data Security Management System, as well as the fundamental principles and provisions of the security policy
- A series of specific security policies aimed at defining detailed security policies in various areas of information security
- The implementation of the security policy is supported by specific procedures and records where required.

6.2. Data Security Objectives

Data Security is defined by international literature as ensuring the following attributes:

- **Confidentiality**: Ensuring that information is accessible only to those who have the appropriate authorization.
- **Integrity**: Ensuring that information is complete, accurate, and valid.
- **Availability**: Ensuring that information is available whenever an authorized user attempts to access it.

In addition to the three main security objectives, the following are considered complementary objectives for information security:

- **User identification and authentication**: Ensuring that the user attempting to access information/system/application is who they claim to be.

- **Access control**: Ensuring that the user attempting to access information/system/application is authorized for that action.
- **Audit & monitoring**: Monitoring and recording user actions.
- **Protection of personal data**: Protecting personal data and sensitive data from unauthorized collection, storage, and processing, in accordance with the applicable law.
- **Non-repudiation**: Ensuring that a user cannot deny having performed an action related to access/processing of information/system/application.

Achieving all of the above security objectives (both primary and complementary) leads to the maximum possible protection of information, systems, and applications.

6.3. Management Commitment to Data Security

The management of **COSTAS A. PAPELLINAS (HELLAS) S.A. (CPO Greece)** fully recognizes the objectives of the Data Security Management System, supports the implementation of these according to this security policy, and ensures continuous improvement of the system.

In particular, the management of the company is responsible for:

- Controlling and approving the security policy, both the initial version and any subsequent revisions
- Controlling and approving roles and responsibilities related to the management of the management systems
- Monitoring significant changes in the company's organization or infrastructure that create the need for system review
- Monitoring incidents related to security
- Initiating actions to enhance the security of the company's data resources by adopting additional measures

6.4. Data Security Organization

COSTAS A. PAPELLINAS (HELLAS) S.A. (CPO Greece) has defined the organizational structures and roles responsible for or associated with the management of its data security. Through these structures and roles, the company aims to protect its information from unauthorized access, disclosure, alteration, or destruction. The organization of the company for data security has been communicated to the company's staff and partners.

6.5. Human Resources Security

All company personnel are required to comply with the company's security policy if they manage or are associated with data resources that fall under the scope of the Management Systems, according to their role. The same obligation applies to external partners not belonging to the company's staff. Personnel (staff or partners) who must comply with the company's security policy must, at a minimum:

- Be aware of the company's security objectives and policies.
- Apply the Management Systems and the prescribed security procedures.
- Use the company's data resources according to the corresponding acceptable use policies, where applicable.
- Be constantly alert to recognize and report security incidents.

6.6. Data Resources Management

COSTAS A. PAPELLINAS (HELLAS) S.A. (CPO Greece) maintains a record of all company resources that are protected by the security policy. Each data resource is assigned to the responsibility of a specific company executive.

6.7. Access Control

The granting of rights to company executives and partners for access to data resources follows a clear and documented process approved by the company's Management. Access to data resources is controlled with appropriate means and user identification mechanisms. Users are responsible for protecting their access credentials to the company's data resources.

6.8. Physical and Environmental Security

Access to the facilities of **COSTAS A. PAPELLINAS (HELLAS) S.A. (CPO Greece)** is permitted only to authorized individuals and only using the measures set by the company. All staff and computer rooms are equipped with an appropriate air conditioning system. The central computing, networking, and telecommunications equipment is supported by backup power sources.

6.9. Operational Security

The operating procedures of the company's data systems are properly documented, updated in case of changes, and available to all users who need them, through the respective manufacturers' websites. The company's management ensures that the systems are sufficient to meet operational needs while taking all appropriate measures to protect against malicious software, handle data loss incidents, and fully log every action in relevant files (logs) for monitoring and control purposes.

6.10. Communication Security

The company has taken several measures to protect its network from unauthorized access. In the same way that internal data is protected, appropriate measures have been taken to protect corporate data transmitted via email, the Internet, or other communication channels.

6.11. Procurement and Maintenance of Systems

When procuring new systems or expanding/upgrading existing systems, the company ensures the maintenance of the security level of its data resources, including but not limited to:

- Security requirements in the system specifications
- Security clauses in contracts with system suppliers
- Security testing scenarios during system testing before they go into production

6.12. Supplier Relations

In cases where suppliers gain access to company resources, such access is governed by specific terms and only for the purposes foreseen in the collaboration. The company informs its suppliers about their obligations regarding the protection of its data resources. Likewise, suppliers must comply with the relevant provisions of the company's security policy.

6.13. Data Security Incident Management

All company executives, regardless of their position in the hierarchy and role, must report any incident related to suspected violations of data security in any way. Third parties (partners and suppliers) also have the same obligation if their collaboration with the company includes such terms.

For this purpose, the management of **COSTAS A. PAPELLINAS (HELLAS) S.A. (CPO Greece)** has established an appropriate incident reporting procedure, which has been communicated to all involved parties. Additionally, security incidents are investigated by the appropriate company personnel through a related process, which determines, where necessary, the security measures that need to be taken.

6.14. Data Security in Business Continuity Management

COSTAS A. PAPELLINAS (HELLAS) S.A. (CPO Greece) places special importance on maintaining an adequate level of security when managing the impact of a security incident. In this context, it ensures that the company's business continuity plan includes roles, procedures, and measures that ensure the desired level of security for the company's resources.

6.15. Compliance

The policy, procedures, and other security measures of **COSTAS A. PAPELLINAS (HELLAS) S.A. (CPO Greece)** take into account and comply with the company's institutional, regulatory, or contractual obligations. Likewise, executives who take on roles related to security management are responsible for implementing the security policy in their domain.