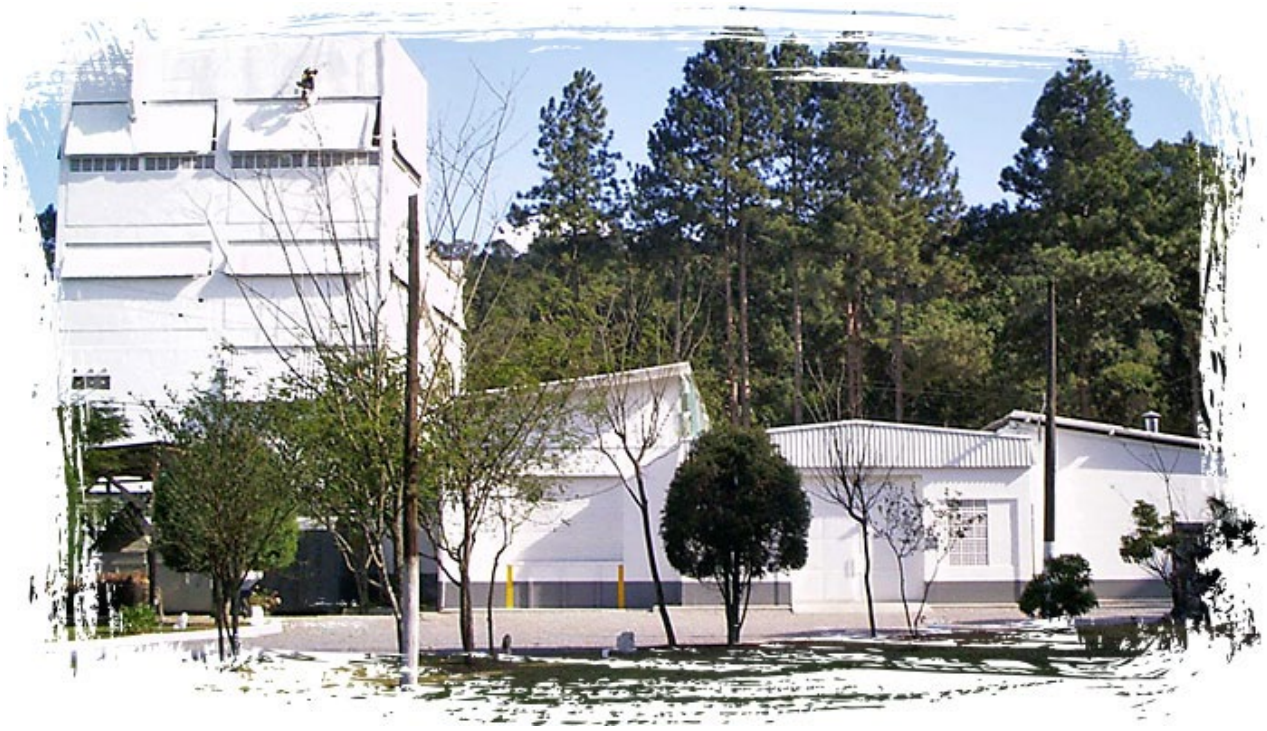

OXY QUÍMICA E METALÚRGICA LTDA

Information Security Policy

December/23

TABLE OF CONTENTS

1. Introduction

Oxy Química is committed to safeguarding and protecting all data – whether personal or not – that is under its custody.

Therefore, Oxy Química's Information Security Policy presents general conduct guidelines, as well as obligations to be followed to mitigate possible risks and damages related to external or internal threats, either deliberate or accidental, that may impact the **confidentiality, integrity and availability** of information of any nature, ensuring its protection.

The ISO 27001:2022 standard, an international standard for information security management processes, will serve as a parameter for Oxy Química to protect sensitive information, such as customer data, intellectual property, commercial secrets and financial information, against internal and external threats.

2. Goal

This Policy aims to establish behavioral guidelines related to information security, which are appropriate to the needs of the business and which provide legal protection for the company and the individual.

3. Application and Scope

This Policy applies to administrators, employees, suppliers, service providers or any other people who are users of Oxy Química information.

4. References

- Oxy Química Code of Ethics and Conduct;
- Current Legislation;
- ABNT NBR ISO IEC 27001:2022 Information Security, cybersecurity and privacy protection – Information security management systems – Requirements.

5. Definitions

Threat: An event that has the potential in itself to compromise Oxy Química's objectives, whether causing direct damage to assets or indirect losses resulting from unexpected situations.

Information Assets: Any information that has value for the organization, including equipment, information and data.

Backup: Copying data from one storage device to another so that it can be restored if the original data is lost, which may involve accidental deletion or data corruption.

Mobile Devices: Notebooks, smartphones, among others.

Security Incident: Event that could harm the company or even violate safety rules.

Authenticity: Property that the information was produced, sent, modified or destroyed by a specific natural person, or by a specific system, body or entity.

Information Classification: Identification of the levels of protection required by the information, its classes and ways of identifying them, in addition to determining the necessary protection controls for each of them.

Confidentiality: Property that information can only be accessed by authorized people, for the necessary period.

Availability: Property that information is available to authorized people when necessary;

Integrity: Property that the information is complete, accurate, and has not been modified or destroyed improperly, in an unauthorized or accidental manner during its life cycle.

Compliance: Process that aims to verify compliance with established standards.

Access control: Method of encoding information to prevent it from being understood or altered by unauthorized people.

General Personal Data Protection Law (Law No. 13,709/2018): Provides for the processing of personal data, including in digital media, by natural persons or legal entities governed by public or

private law, in order to protect fundamental rights of freedom and privacy and the free development of the personality of the natural person.

Commercial Partners and Third Parties: In the context of Oxy Química, these are those contracted (individuals or legal entities) who act on its behalf, for example, commercial representatives and suppliers.

6. Guidelines

Oxy Química's Information Security Policy considers information security through the following aspects:

- **Confidentiality:** guarantee that information is only accessed by authorized people;
- **Integrity:** safeguarding the accuracy and integrity of information and processing methods;
- **Availability:** ensuring that authorized users have access to information and respective assets whenever necessary.

Information security is achieved through the implementation of a series of controls, which can be technological, physical or administrative. Oxy Química is committed to safeguarding and protecting the information under its custody. This Information Security Policy is supported by compliance with the Oxy Química Code of Ethics and Conduct and applicable laws and regulations in force that relate to data protection.

Information security consists of adopting measures to protect the property, confidentiality, availability and integrity of information, in any form and medium presented (physical or digital), from the various existing threats, in order to avoid its misuse, as well as inappropriate or illegal use, or in non-compliance with internal policies and procedures.

6.1 Specific guidelines

- **Use of resources and information**

It is everyone's commitment to ensure that information and resources are used only for professional purposes, making appropriate use of IT (information technology), physical (hardware) or logical (software) resources. Employees, suppliers, service providers must observe and respect intellectual property rights, whether regarding information owned by Oxy Química or by third parties. These rights

apply to both tangible and intangible assets, including brands, patents, source codes and licensing agreements, among others.

- **Classification and processing of information**

All information found in Oxy Química's physical and logical environments, including that related to its suppliers, partners and customers, must be classified according to its criticality and sensitivity. It is a commitment of all employees, suppliers and service providers to ensure that information receives labels consistent with its classification, which are divided into the following levels:

1) **Public:** when classified as 'public' there is no confidentiality in the information, it is open to both internal and external audiences;
2) **Internal:** the internal use classification has low level of confidentiality. This information will be available to all administrators and employees of Oxy Química, but the external public will not be able to access such information;
3) **Restricted:** restricted classification has medium level of confidentiality. Only authorized people will be able to access the information;
4) **Confidential:** Confidential classification has the highest level of confidentiality. Information has high value for the organization.

- **Users and Passwords**

Physical and logical access will only be granted to resources and information necessary and indispensable to perform the activities and in accordance with the interests of Oxy Química, considering the principle of least privilege. Passwords and other forms of authentication are individual, secret, non-transferable and are protected with a level of security compatible with the respective information. The employee is responsible for ensuring the correct use of their identification and the confidentiality of their password.

- **Internet**

It is a work tool and should be used as a research method and complement to professional activities. Access to pages and websites is the responsibility of each user, and access to websites with inappropriate content, such as pornography, games, betting, among others, is prohibited.

- **E-mail**

It is a work tool and must be used to support the development of functional activities. The employee is fully responsible for the use of the service, and is fully responsible for any action or damage carried out, responding for any legal or illegal act. The addresses and PO boxes made available to users are the property of the company.

- **Mobile devices:**

Employees must commit to use mobile devices in accordance with the interests of Oxy Química, as well as to ensure their custody, taking care of their physical integrity and the inviolability of the information contained in them. Employees must also return them when requested by the company.

- **Management and protection of IT resources**

The acquisition, installation, configuration, movement and maintenance of Oxy Química's Information Technology resources is the exclusive responsibility of the IT area.

- **Information Security Incidents**

Incidents are considered to be any events that negatively affect the confidentiality, integrity and availability of information assets. It is everyone's commitment to immediately report any Information Security incident.

- **Information Security Controls**

To reduce vulnerabilities and information security incidents, Oxy Química has some tools such as antivirus, email filters and internet access filters, as well as automatic backups on SSD (Solid Disk).

- **Monitoring**

Oxy Química may:

1) Monitor technological resources to identify users and their accesses, as well as manipulated material;
2) Carry out physical and logical inspection of the machines you own;
3) Install protective, preventive and detectable systems to ensure the security of information and access perimeters.

- **Working from Home**

It is a modality offered by Oxy Química for its employees to work outside the corporate environment. The employee is responsible for looking after the equipment provided by the company, as well as the information they are accessing.

- **Disposing of information**

Information must be disposed of using measures that make it impossible to reconstruct it, according to the needs of physical or digital support. The information must be disposed of considering minimum legal or regulatory deadlines, as well as its need for the business or area, whichever is greater.

- **Suppliers and external parties**

Contracts with service providers that have access to Oxy Química's information, systems and/or environment must contain clauses that ensure compliance with information security rules, as well as penalties in case of non-compliance.

7. RESPONSIBILITIES

7.1 Employees covered by this Policy

• Comply with Information Security rules;
• Protect information against unauthorized access, modification, destruction or disclosure;
• Ensure that technological resources, information and systems available are used for business purposes only;
• Comply with laws and regulations that regulate intellectual property;
• Do not discuss, mention or share confidential matters in external environments, including social networks;
• Do not share confidential information of any kind;

7.2 Information Technology Area

• Manage Information Security controls and tools, as well as handle incidents, problems, changes and any requests and/or reports related to Information Security;
- Monitor the resources and environments under their responsibility, ensuring protection against possible threats and inappropriate use, as well as keeping them up to date with updates and changes in legislation and/or business requirements;

7.3 Directors

• Provide wide dissemination of the Information Security Policy and Standards;

• Promote information security awareness actions for employees and service providers;

• Propose actions to improve information security;

• Define employee access privileges according to the activities they perform.

• Establish standards and procedures related to information security instrumentation, covering the ownership and use of information, access and identity management and information security incidents.

• Ensure that contracts with service providers that have access to the Organization's information, systems and/or environment contain clauses that ensure compliance with this Policy and the Information Security Standards, as well as penalties in case of non-compliance.

• Approve this Information Security Policy, as well as its revisions.

8. FINAL PROVISIONS

The provisions above apply immediately to the entire Organization, upon publication of this Policy. Protecting information must be part of employee conduct. Undue disclosures may cause disadvantages, financial losses and/or damage to Oxy Química's image. Whenever a leak of confidential information is known, such fact must be reported to those responsible, so that the appropriate measures can be taken.