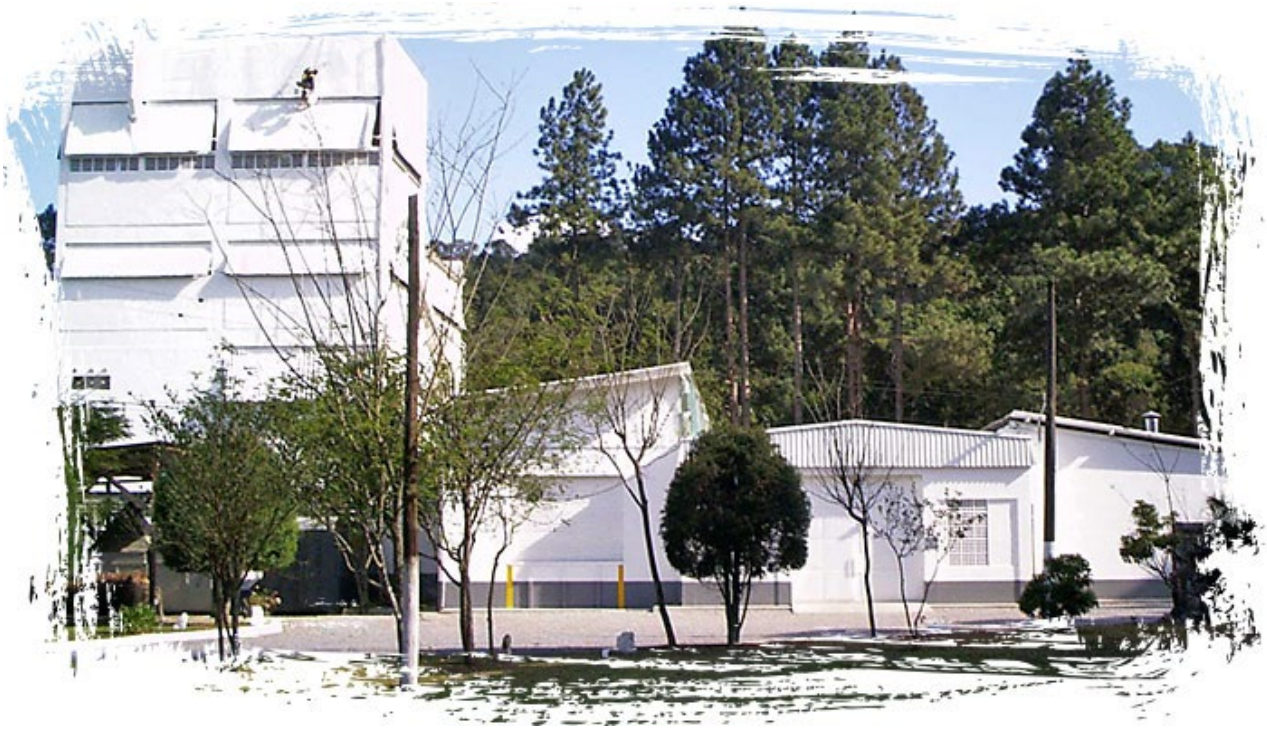

OXY QUÍMICA E METALÚRGICA LTDA

Informationssicherheitspolitik

Dezember/23

INHALTSÜBERSICHT

1. Einleitung

Oxy Química ist dem Schutz personenbezogener und sonstiger von ihr aufbewahrten Daten verpflichtet.

Deshalb enthält die Informationssicherheitspolitik von Oxy Química allgemeine Verhaltensrichtlinien sowie zu befolgende Pflichten, um eventuelle Risiken und Schäden im Zusammenhang mit externen oder internen absichtlichen oder zufälligen Bedrohungen, die sich auf die **Vertraulichkeit, Unversehrtheit und Verfügbarkeit** der Informationen jeglicher Art auswirken können, zu minimisieren und deren Aufrechterhaltung zu gewährleisten.

Die Norm ISO 27001:2022, Internationale Norm für Informationssicherheitsmanagementprozesse, dient Oxy Química als Parameter zum Schutz sensibler Informationen wie beispielsweise Kundendaten, geistiges Eigentum, kaufmännische Geheimnisse und Finanzinformationen vor internen und externen Bedrohungen.

2. Zweck

Zweck der vorliegenden Politik ist die Festlegung von Verhaltensrichtlinien in Bezug auf Informationssicherheit, die den Geschäftsbedürfnissen angemessen sind und dem Unternehmen und den einzelnen Personen rechtlichen Schutz liefern.

3. Anwendung und Umfang

Vorliegende Politik gilt für Geschäftsführer, Mitarbeiter, Lieferanten, Dienstleister oder sonstige Personen, die Informationen der Oxy Química benutzen.

4. Referenzen

- Ethik- und Verhaltenskodex der Oxy Química;
- Geltende Gesetze;

- ABNT NBR ISO IEC 27001:2022 Informationssicherheit, Internetsicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen.

5. Definitionen

Bedrohung: Ereignis mit Eigenpotenzial zur Gefährdung der Ziele der Oxy Química durch direkte Schäden an Vermögenswerten oder indirekte Verluste infolge unerwarteter Situationen.

Informationswerte: Jegliche Information, die für das Unternehmen einen Wert darstellt, dazu zählen Geräte, Informationen und Daten.

Backup: Übertragung der Daten von einem Datenspeicher auf einen anderen, um bei Verlust der ursprünglichen Daten, beispielsweise durch versehentliches Löschen oder Korruption der Daten, deren Wiedererlangung zu ermöglichen.

Mobile Geräte: Notebooks, Smartphones, u.a.

Sicherheitszwischenfall: Ereignis, durch das dem Unternehmen Schaden entstehen kann oder das die Sicherheitsregeln verletzten kann.

Authentizität: Eigenschaft, dass die Information produziert, ausgegeben, modifiziert oder zerstört wurde durch eine bestimmte natürliche Person oder ein bestimmtes System, Behörde oder Einrichtung.

Einstufung von Informationen: Identifizierung der Schutzniveaus, die die Informationen erfordern, ihre Klassen und die Formen, sie zu identifizieren, ferner die Bestimmung der jeweils erforderlichen Schutzkontrollen.

Vertraulichkeit: Eigenschaft, dass die Information nur befugten Personen und im erforderlichen Zeitraum zugänglich ist.

Verfügbarkeit: Eigenschaft, dass die Information den befugten Personen bei Bedarf verfügbar ist;

Unversehrtheit: Eigenschaft, dass die Information vollständig, genau und unversehrt ist und dass sie während ihrer Nutzungsdauer nicht unbefugt oder versehentlich modifiziert bzw. zerstört wurde.

Konformität: Prozess zur Überprüfung der Einhaltung der festgelegten Vorschriften.

Zugangskontrolle: Methode zur Kodifizierung der Information, um deren Kenntnisnahme bzw. Änderung durch unbefugte Personen zu verhindern.

Allgemeines Datenschutzgesetz (Gesetz Nr. 13.709/2018): Betrifft den Umgang mit personenbezogenen Daten, einschließlich in den digitalen Medien, durch natürliche oder juristische Personen des öffentlichen Rechts oder Privatrechts mit dem Ziel, die Grundrechte auf Freiheit und Privatsphäre und die freie Entwicklung der Persönlichkeit der natürlichen Person zu schützen.

Geschäftspartner und Dritte: Im Zusammenhang mit Oxy Química handelt es sich um Vertragsnehmer (natürliche oder juristische Personen), die in ihrem Namen tätig sind, beispielsweise Handelsvertreter und Lieferanten.

6. Richtlinien

Die Informationssicherheitspolitik der Oxy Química berücksichtigt hinsichtlich der Informationssicherheit nachstehende Aspekte:

- **Vertraulichkeit:** Gewährleistung, dass die Information nur befugten Personen zugänglich ist;
- **Unversehrtheit:** Wahrung der Genauigkeit und Unversehrtheit der Informationen und der Verarbeitungsmethoden;
- **Verfügbarkeit:** Gewährleistung, dass die befugten Benutzer bei Bedarf Zugang zu den Informationen und den entsprechenden Geräten erhalten.

Informationssicherheit wird erzielt mittels Umsetzung einer Reihe von Kontrollen, bei denen es sich um technische, physische oder administrative Kontrollen handeln kann. Oxy Química verpflichtet sich, die von ihr gespeicherten Informationen zu schützen. Ihre Informationssicherheitspolitik stützt sich auf die Einhaltung des Ethik- und Verhaltenskodexes von Oxy Química sowie der einschlägigen, geltenden Gesetze und Regelungen bezüglich des Datenschutzes.

Informationssicherheit beruht auf der Anwendung von Maßnahmen zum Schutz des Eigentums, der Vertraulichkeit, Verfügbarkeit und Unversehrtheit der Informationen in jeglicher Form und auf jeglichem Träger (physischer bzw. digitaler Art) vor den verschiedenen existierenden Bedrohungen, um ihre unbefugte, unangemessene, rechtswidrige bzw. gegen die Schutzpolitik und die internen Vorgehensweisen verstoßende Benutzung zu verhindern.

6.1 Spezielle Richtlinien

- **Benutzung von Ressourcen und Informationen**

Alle sind dazu verpflichtet sicherzustellen, dass die Informationen und Ressourcen nur zu beruflichen Zwecken benutzt und die physischen (Hardware) und logischen (Software) IT (Informationstechnologie) Ressourcen angemessen eingesetzt werden. Mitarbeiter, Lieferanten und Dienstleister haben die geistigen Eigentumsrechte der Oxy Química bzw. Dritter zu beachten und zu respektieren. Diese Rechte betreffen sowohl materielle als auch immaterielle Vermögenswerte, einschließlich Markenrechte, Patente, Quellcodes und Lizenzverträge, u.a.

- **Einstufung und Umgang mit Informationen**

Sämtliche in den physischen und logischen Umgebungen von Oxy Química befindlichen Informationen, einschließlich die auf Lieferanten, Geschäftspartner bzw. Kunden bezogenen Informationen, sind entsprechend ihrer Kritikalität und Sensibilität einzustufen. Sämtliche Mitarbeiter, Lieferanten und Dienstleister sind dazu verpflichtet sicherzustellen, dass die Informationen ihrer Einstufung entsprechend nachstehenden Stufen zugeordnet gekennzeichnet werden:

1) **Öffentlich:** in der öffentlichen Einstufung sind die Informationen nicht vertraulich und sowohl dem internen als auch dem externen Publikum zugänglich;

2) **Intern:** die zur internen Benutzung eingestuften Informationen unterliegen einem geringen Vertraulichkeitsmaß. Sie sind allen Geschäftsführern und Mitarbeitern der Oxy Química zugänglich, doch das externe Publikum darf zu diesen Informationen keinen Zugang haben;

3) **Eingeschränkt:** für die mit eingeschränktem Zugang eingestuften Informationen gilt die mittlere Vertraulichkeitsstufe. Nur befugte Personen sind zugangsberechtigt;

4) **Vertraulich:** für die als vertraulich eingestuften Informationen gilt die höchste Vertraulichkeits-stufe. Die Informationen sind für das Unternehmen von hohem Wert.

- **Benutzer und Passwörter**

Physischer und logischer Zugang wird nur zu den für die Verrichtung der Tätigkeiten im Interesse der Oxy Química erforderlichen und unentbehrlichen Ressourcen und Informationen gewährt, unter Berücksichtigung des Grundsatzes der geringsten Privilegien. Passwörter und sonstige Formen der Authentifizierung sind individuell, geheim, nicht übertragbar und mit dem den jeweiligen

Informationen entsprechenden Sicherheitsgrad geschützt. Es obliegt dem Mitarbeiter, für die korrekte Benutzung seiner Identifizierung und die Geheimhaltung seines Passwortes zu sorgen.

- **Internet**

Es handelt sich um ein Arbeitswerkzeug, das zu Forschungszwecken und zur Ergänzung der beruflichen Tätigkeiten einzusetzen ist. Jeder Benutzer haftet für den Zugang zu den Internetseiten, wobei der Aufruf von Webseiten mit unangemessenen Inhalten, beispielsweise Pornographie, Spiele, Wetten, u.a. untersagt ist.

- **E-Mail**

Es handelt sich um ein Arbeitswerkzeug, das zur Unterstützung der jeweiligen Aufgabenverrichtung einzusetzen ist. Der Mitarbeiter ist in vollem Umfang haftbar für die E-Mail-Benutzung, wobei er für jegliche Handlung bzw. jeglichen verursachten Schaden in vollem Umfang verantwortlich ist und für jede rechtmäβíge oder rechtswidrige Handlung haftet. Die den Benutzern zur Verfügung gestellten E-Mail-Adressen und Mailboxen sind Eigentum des Unternehmens.

- **Mobile Geräte**

Der Mitarbeiter ist verpflichtet, die mobilen Geräte entsprechend den Interessen der Oxy Química zu benutzen, für deren Aufbewahrung, physische Unversehrtheit und Unverletzlichkeit der darauf enthaltenen Informationen zu sorgen und sie auf Aufforderung des Unternehmens zurückzugeben.

- **Management und Schutz der IT-Ressourcen**

Anschaffung, Installation, Konfiguration, Bewegung und Wartung von Informationstechnologie Ressourcen der Oxy Química unterliegen der ausschlieβlichen Zuständigkeit des IT-Bereichs.

- **Informationssicherheitszwischenfälle**

Als Zwischenfälle werden jegliche Vorkommnisse betrachtet, die die Vertraulichkeit, Unversehrtheit und Verfügbarkeit der Informationsressourcen beeinträchtigen. Allen obliegt, jeglichen Informationssicherheitszwischenfall sofort mitzuteilen.

- **Informationssicherheitskontrollen**

Um Anfälligkeiten und Informationssicherheitszwischenfälle zu reduzieren, benutzt Oxy Química Werkzeuge wie beispielsweise Antivirenschutz, E-Mail-Filter und Filter zum Aufruf von Internetseiten, neben automatischen Backups auf SSD (Solid State Drive).

- **Überwachung**

Oxy Química kann:

1) Technische Ressourcen überwachen, um Benutzer und die jeweils vorgenommenen Zugänge sowie manipuliertes Material zu identifizieren;
2) Physische und logische Inspektionen der Geräte ihres Eigentums vornehmen;
3) Präventive und detektierbare Schutzsysteme installieren, um die Sicherheit der Informationen und der Zugangsberechtigungen zu gewährleisten.

- **Telearbeit / Home Office**

Eine Modalität, die Oxy Química den Mitarbeitern bietet, um ihre Arbeiten von außerhalb der Betriebseinrichtungen zu verrichten. Der Mitarbeiter ist für die ordnungsgemäße Pflege der vom Unternehmen zur Verfügung gestellten Geräte sowie der aufgerufenen Informationen zuständig.

- **Entsorgung der Informationen**

Die Entsorgung der Informationen hat mithilfe von Maβnahmen zu erfolgen, die deren Wiederherstellung unmöglich machen, entsprechend den Erfordernissen des physischen bzw. digitalen Supports. Die Entsorgung von Informationen hat unter Einhaltung der gesetzlichen bzw. regulatorischen Mindestfristen sowie unter Berücksichtigung ihres Erfordernisses für die Geschäfts- bzw. Bereichstätigkeit zu erfolgen.

- **Lieferanten und Dritte**

In den Verträgen mit Dienstleistungsunternehmen, die Zugang zu Informationen, zu Systemen bzw. Einrichtungen der Oxy Química haben, sind Klauseln vorzusehen, die die Einhaltung der Regeln bezüglich Informationssicherheit gewährleisten und Strafen für Regelverstöβe festlegen.

7. ZUSTÄNDIGKEITEN

7.1 Mitarbeitern obliegende Pflichten

• Einhaltung der Regeln bezüglich Informationssicherheit;
• Schutz der Informationen vor Zugängen, Änderung, Zerstörung bzw. Weitergabe ohne Befugnis;
• Sicherstellung, dass die ihnen verfügbaren technischen Ressourcen, Informationen und Systeme nur zu Geschäftszwecken benutzt werden;

• Einhaltung der Gesetze und Vorschriften, die das geistige Eigentum regeln;
• Vertrauliche Angelegenheiten nicht in externen Umgebungen, einschließlich sozialen Netzwerken, zu besprechen, zu zitieren bzw. mitzuteilen;
• Vertrauliche Informationen jeglicher Art geheim zu halten.

7.2 Bereich Informationstechnologie

• Management der Informationssicherheitskontrollen und -werkzeuge sowie Klärung von Vorkommnissen, Problemen, Vornahme von Änderungen und Eingehen auf Anträge bzw. Berichterstattung bezüglich Informationssicherheit;

- Überwachung der Ressourcen und Umgebungen unter ihrer Zuständigkeit zum Schutz vor möglichen Bedrohungen bzw. unangemessener Benutzung, sowie Vornahme deren Aktualisierungen und Beachtung der Gesetzesänderungen bzw. Geschäftsanforderungen.

7.3 Vorstand

• Umfassende Bekanntmachung der Informationssicherheitspolitik und -vorschriften;
• Bewusstmachung der Mitarbeiter und Dienstleister bezüglich Informationssicherheit;
• Förderung von Verbesserungsmaβnahmen zur Informationssicherheit;
• Festlegung der Zugangsprivilegien der Mitarbeiter entsprechend ihren Aufgabenverrichtungen;
• Festlegung von Vorschriften und Vorgehensweisen zur Informationssicherheitsinstrumentierung, mit Bestimmungen bezüglich des Eigentums und der Benutzung der Informationen, Management von Zugängen, Identitäten und Informationssicherheitsvorkommnissen;
• Sicherstellung, dass in Verträgen mit Dienstleistungsunternehmen, die Zugang zu Informationen, Systemen bzw. Betriebseinrichtungen haben, Klauseln vorgesehen sind, die die Einhaltung der Informationssicherheitspolitik und -vorschriften sicherstellen und Strafen für Verstöβe festlegen;
• Genehmigung vorliegender Informationssicherheitspolitik und ihrer Revisionen.

8. ABSCHLIESSENDE BESTIMMUNGEN

Obige Bestimmungen finden ab Veröffentlichung vorliegender Politik sofort auf das gesamte Unternehmen Anwendung. Der Schutz der Informationen ist Teil des Mitarbeiterverhaltens. Durch unbefugte Bekanntmachungen können Nachteile, finanzielle Verluste bzw. Schädigungen des Rufes der Oxy Química entstehen. Werden Datenlecks geheimer Informationen bekannt, ist dies den Zuständigen mitzuteilen, um die erforderlichen Maβnahmen zu ergreifen.