## 1 Version control

| Version | Issue date | Description of changes |
|---|---|---|
| 01 | 2025-06-24 | New document |

## 2 Purpose

To establish the governing principles and requirements for the organization's Information Management System, ensuring the confidentiality, integrity, and availability of information assets in alignment with applicable legal, regulatory, and ISO/IEC 27001:2022 standards.

## 3 Scope

This document applies to the organization in its entirety.

## 4 Terms, definitions and abbreviations

| Item | Definition |
|---|---|
| Availability | Property of being accessible and usable on demand by an authorized entity. |
| CISO | Chief Information Security Officer. |
| Confidentiality | Property that information is not made available or disclosed to unauthorized individuals, entities, or processes. |
| Information security | Preservation of confidentiality, integrity and availability of information. |
| Integrity | Property of accuracy and completeness. |
| Interested party | Person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity. |
| ISMS | Information security management system. |
| Organization | Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives. |
| Process | Set of interrelated or interacting activities which transforms inputs into outputs. |
| Requirement | Need or expectation that is stated, generally implied or obligatory. |

## 5 Legal and regulatory references

- ISO/IEC 27001:2022 — 5.1, 5.2, 8.3.

## 6 Requirements

### 6.1 Top management.

**6.1.1** The General Management shall assume the role of **top management** as defined in ISO/IEC 27001 and shall demonstrate leadership and commitment to the ISMS by ensuring that:

**6.1.1.1** ISMS requirements are integrated into the organization's business processes through the implementation of appropriate policies, procedures, and controls.

**6.1.1.2** All necessary resources for the effective operation of the ISMS are made available, including hardware, software (and related updates), budgets, and time allocations.

**6.1.1.3** The importance of effective information security management and compliance with ISMS requirements is communicated throughout the organization via meetings (in person or virtual), training sessions, internal communications, or other appropriate channels.

**6.1.1.4** The ISMS achieves its intended outcomes, including the fulfillment of established information security objectives.

**6.1.1.5** All personnel receive clear direction and expectations through established lines of authority and communication.

**6.1.1.6** Personnel are adequately supported through the provision of necessary resources, training, awareness programs, communication mechanisms, and access to documented information.

**6.1.1.7** A culture of continual improvement is promoted across the ISMS scope, with emphasis on technological updates, awareness of emerging threats, and the implementation of feedback mechanisms.

**6.1.1.8** Key roles related to information security—particularly the CISO—are empowered and supported with the necessary resources and delegated authority to fulfill their responsibilities.

### 6.2 Objective setting.

**6.2.1** This policy shall serve as the foundational reference for the establishment of all information security objectives within the organization. All objectives shall be aligned with the intent and principles of this policy and shall clearly document the rationale for their alignment.

### 6.3 Information security policy.

**6.3.1** The top management **of CEMSoft Corporation** hereby establishes the following Information Security Policy:

At **CEMSoft Corporation**, we are committed to:

a) Safeguarding the confidentiality, integrity, and availability of information within the scope of our Information Security Management System.

b) Ensuring compliance with all applicable information security requirements of our stakeholders, including statutory, regulatory, and contractual obligations.

c) Proactively identifying and addressing information security risks, including threats and vulnerabilities, through the implementation of appropriate organizational, human, physical, and technological controls.

d) Pursuing continual improvement of both the ISMS and overall information security performance.

**6.3.2** This Information Security Policy shall be communicated to all internal personnel within the scope of the ISMS, made readily available to relevant interested parties, upon request or based on business needs, and treated as public information, with no access restrictions, to promote awareness and transparency.

## 6.4 Accessory documents.

### 6.4.1 Information security policies.

**6.4.1.1** This overarching policy shall be supported by a set of more specific policies that govern key aspects of information security. The following supporting policies shall be established, implemented, and maintained:

**6.4.1.1.1** Information Management.

**6.4.1.1.2** Information Infrastructure.

**6.4.1.1.3** Information Events.

**6.4.1.1.4** Secure Software Development.

**6.4.1.2** Each policy may include as many clauses and sub-clauses as required; however, they shall utilize the verbal forms recommended by ISO/IEC 27001, such as “shall,” “should,” and “may”, and follow a hierarchical clause numbering system (e.g., `6.1.2`).

**6.4.2 Documented operating procedures.**

**6.4.2.1** The organization shall develop and maintain documented procedures for all aspects of information security that constitute a defined process, including inputs, activities, and outputs. Policy provisions that do not involve procedural elements shall not be translated into procedures.

**6.4.2.2** The organization shall develop its procedures and other types of documented information in accordance with the activities established by a specific documented procedure on the subject.

## 6.5 General requirements of the information security management system.

**6.5.1 Compliance with information security policies, regulations and standards.**

**6.5.1.1** Compliance with this Information Security Policy and the supporting policies referenced in section **6.4.1.1** is mandatory for all personnel within the scope of the ISMS.

**6.5.1.2** As part of the continual improvement of the ISMS, the organization may adopt additional requirements from other recognized information security standards or frameworks, provided they do not conflict with the requirements of this policy or its supporting policies.

**6.5.1.3** The organization may also adopt information security requirements imposed by external parties (e.g., customers, suppliers, or regulatory bodies), provided such requirements are compatible with this policy and its supporting documents.

**6.5.2 Legal, statutory, regulatory and contractual requirements.**

**6.5.2.1** The organization shall identify, document, and comply with all applicable legal, statutory, regulatory, and contractual requirements related to information security.

**6.5.3 Independent review of information security.**

**6.5.3.1** To verify the adequacy and effectiveness of the ISMS, the organization shall commission an independent review or audit at least once per calendar year. Acceptable reviews include certification, surveillance, or recertification audits by accredited bodies, information security audits of suppliers, and dedicated external assessments where other audits are not conducted in the same period.

**6.5.4 Management responsibilities.**

**6.5.4.1** The CISO shall be responsible for leading and coordinating the organization's information security initiatives. This role may be internal or external, as determined by senior management.

**6.5.4.2** All employees and relevant stakeholders shall comply with the applicable requirements of this policy and all supporting documentation referenced in section **6.4**.

**6.6 Changes to the information security management system.**

**6.6.1** All modifications to ISMS-related documentation, resources, processes, or any other components of the ISMS shall:

**6.6.1.1** Be properly justified and formally documented as part of the organization's change control process.

**6.6.1.2** Ensure the continued integrity, effectiveness, and alignment of the ISMS with its intended outcomes by:

**6.6.1.2.1** Updating all relevant documented information, including policies, procedures, and records.

**6.6.1.2.2** Assigning or reassigning roles, responsibilities, and authorities as needed to support the change.

**6.6.1.2.3** Allocating or reallocating necessary resources to support the implementation and maintenance of the change.

**6.6.1.3** Be reviewed and formally approved by the CISO and/or senior management, as appropriate.

**6.7 Communication.**

**6.7.1** The Information Security Management System (ISMS) shall maintain effective communication mechanisms to support the achievement of its intended outcomes. Communication within the ISMS shall be categorized into two types: operational communication and communication of critical ISMS aspects.

**6.7.1.1** Operational communication shall be defined within each of the organization's procedures and corresponding process flowcharts. It includes, but is not limited to, emails, system logs, formal requests, and any instance where information is transferred from a sender to a recipient as part of operational activities defined in organizational manuals and process documentation.

**6.7.1.2** Communication of critical aspects of the ISMS is not addressed within the organization's operational procedures, as these aspects affect the entire scope of the management system and are not necessarily linked to a specific process. Such communication shall follow the structure and criteria established in the following ISMS Communication Matrix:

| What | Who | To whom | How | When |
|---|---|---|---|---|
| Information Security Policies | CISO | All Collaborators | SharePoint® | Upon issuance or update of policies |
| Privacy Notices | Customer Service Associates | Customers | Email, printed documents, or website | Prior to the collection of any personal data |
| Information Security Requirements for Suppliers | CEO or CISO | Suppliers | Email or contractual clauses | At the beginning of the commercial relationship and upon any changes |
| Evidence of Compliance with Personally Identifiable Information (PII) Regulations | CEO or CISO | Competent Authority | Reports or other forms of documented information | Upon official request |
| Basic Information Security Training | CISO or External Provider | New Employees | Online learning materials | Upon onboarding of each new employee |
| Ongoing Information Security Training | CISO or External Provider | All Collaborators | Online learning materials | As established in the annual training program |
| Information Security Alerts | CISO | All Collaborators | Email, in-app/system alerts or WhatsApp® | Immediately upon identification of an incident |
| Results of Internal Audits | Lead Auditor | CEO | Management review sessions and audit reports | Annually |
| Software and Hardware Updates | CISO | All Collaborators | Email or instant messaging platforms | Upon deployment of relevant updates with potential operational impact |
| Fraud and Scam Awareness | CISO | Clients and Collaborators | Newsletters, email, website, social media or WhatsApp® | When new threats or trends are detected |
| Changes in Information Security Legislation | CISO | All Collaborators | Email or meetings | When regulatory changes affecting ISMS occur |
| Feedback on Information Security Practices | Collaborators | CISO | Email, WhatsApp®, or support ticket systems | Whenever unsafe or suspicious practices or faliure of controls are detected |

**6.8 Privacy notice**

**6.8.1** The organization shall establish, implement and enforce the following privacy notice:

CEMSoft, with its registered address at **171 Bosque Real Av., Bosque Real, Chihuahua, Chihuahua 31160 Mexico**, is responsible for collecting your personal data, for the use given to such data, and for its protection.

In accordance with the provisions of the Federal Law on the Protection of Personal Data Held by Private Parties (hereinafter referred to as the "Law") and its Regulations, we kindly request that you carefully read the Terms and Conditions contained in this Privacy Notice (the "Notice"), since this Notice establishes the applicable terms and conditions regarding the Personal Data collected by CEMSoft, should you grant your consent. Your personal information will be used to provide the services and products you have requested, to inform you of changes thereto, and to evaluate the quality of the services we deliver.

As part of its normal business activities and in accordance with its lawful corporate purpose, CEMSoft, in certain cases, collects and stores information considered as Personal Data under the terms of the Law. Therefore, the Company is subject to its provisions. The Personal Data you provide to the Controller, or those generated during visits to the CEMSoft website, will vary in each case depending on your activities on the site, and may include the following:

**A.** When entering comments through the contact form: only the following Personal Data will be collected and stored: a) General Data: full name (as provided by you), email address, and any other data you voluntarily include in your comments. In all cases, the accuracy and truthfulness of the Personal Data collected will remain your responsibility, since you are the one with access to your social media profiles and the one providing your information. **B.** In all cases, upon entering the CEMSoft website, data will be collected through Cookies and Web Beacons. These elements capture your IP address, browser type, operating system, visited web pages, browsing and consumption habits and patterns, followed links, and the site visited prior to ours. Based on such Personal Data, a user profile is created and used for the purposes described herein.

Sensitive Personal Data. CEMSoft does not collect Sensitive Personal Data. Your Personal Data will be used and processed exclusively for the purposes explicitly described below: A. Primary purposes. a) When completing the contact form, to contact you, resolve your inquiries, and present a proposal or potential business relationship aligned with your needs or those of the company you represent. B. Secondary purposes. a) To identify, locate, communicate, and contact you, to send information, and for statistical and scientific use (metrics analysis); b) To develop, by itself, through affiliates, or through third parties, studies on the interests, behaviors, and demographics of Data Subjects, in order to better understand their needs and interests and provide improved informational services; c) To strengthen our business initiatives and strategies; d) To analyze visited websites, searches conducted by Data Subjects, and to enhance our content and offerings, including personalization, presentation, programming, and services; e) To send email communications regarding news or relevant events.

CEMSoft will not transfer your Personal Data without your consent, although it may use them for purposes involving third parties, such as statistical analysis and newsletter distribution, without involving the transfer of such Data. If you do not consent to your personal data being transferred under the terms outlined in this Privacy Notice, you may request this restriction through your support account.

The retention period of Personal Data will be indefinite from the date on which you provided it to the Controller. Nevertheless, you may oppose at any time, thereby requesting its blocking and cancellation. Once you provide your Personal Data to the Controller by any means, please be advised that such data will be stored in a CRM system belonging to the site, access to which will be strictly limited to the Controller. Your personal data will at all times be treated lawfully and in compliance with the principles of Lawfulness, Consent, Information, Quality, Purpose, Loyalty, Proportionality, and Accountability, as established by the Law.

Any questions regarding this Notice, your Personal Data and its processing, or the exercise of the rights described below, may be addressed by contacting us at **+52 (614) 688 2114** on business days, as applicable. You will always have access to your Personal Data, whether to request access, rectification, cancellation, or objection, in accordance with the Law (the "ARCO Rights"), either in writing or electronically, through the procedure described herein. Your request must be addressed to CEMSoft or submitted via email at **arco@cemsoft.com.mx**. Such request must include the following: a. A scanned copy or photograph of your official identification containing your photograph and signature, or if acting on behalf of another, a copy of the notarized power of attorney and/or registration with the corresponding Public Registry, along with the articles of incorporation, if applicable. b. A scanned copy or photograph of proof of address. The request must include: i) Your name or corporate name and a physical address for delivery of the response, communications, documentation, and replies; ii) The specific Personal Data to which you seek access, rectification, cancellation, review, objection, or revocation of consent; iii) If known, the purpose for which the data was originally provided and the name of the Controller to whom it was delivered; and iv) A clear, respectful, and concise statement of your request, as well as any other information or documentation that facilitates locating your Personal Data. The Controller will have twenty days from the date the request is received to resolve it or to request further information. If your request is deemed valid because you have proven your identity and your Personal Data was found in our database, execution will take place within a maximum of fifteen days. The Controller will keep you informed of the process at all times upon your request. The response and access to your Data, as well as the supporting documents, may be delivered, subject to identity verification, through certified copies issued by the company and its legal representative, electronic documents, or simple copies. Whenever the request is submitted electronically, preference will be given to electronic means for providing responses and resolutions. Should the Controller require the use of your Personal Data for purposes different from those described in this Privacy Notice, you will be contacted either in writing, by phone, electronically, or through any other means permitted by current or future technologies, and the new intended uses will be explained in order to obtain your consent.