serena

Information Security Policy

serena

Summary

1. Introduction 4
2. Target audience 5
3. Basic rules of information security 5
   - 3.1. Principles of information security 5
   - 3.2. Information life cycle 5
   - 3.3. Classification of information 6
   - 3.4. Information security incidents 6
4. Information security management sistem 6
5. Internal guidelines on information security and cyber security 7
   - 5.1. Safe behavior 7
   - 5.2. *Security & privacy by design* 8
   - 5.3. Data protection 8
   - 5.4. Identification/Assessment of threats and vulnerabilities 9
   - 5.5. Business continuity management (BCM) 9
   - 5.6. Prevention and Protection Actions 9
   - 5.7. Records control 10
   - 5.8. Personal mobile devices (BYOD) 10
   - 5.9. Monitoring & testing 11
   - 5.10. Action and incidente response plan 11
6. Training and awareness program 13
7. Disciplinary measures 13
8. Annex I – Access Management 15
9. Annex II – Change management 16
10. Annex III – Operation management 18

Introduction

This Information Security Policy ("Policy") defines standards and guidelines that seek to ensure the confidentiality, integrity, and availability of the data and information systems used by Serena. Adequate protection of the assets and data used is essential to enable the identification, protection, detection, response and recovery of events in the event of an information security failure.

In addition, the Policy complements Section 13 of the Company's Code of Conduct, with regard to the guidelines and conduct expected of co-entrepreneurs, third parties, partners, suppliers and service providers, regarding the protection of assets and data in order to ensure the confidentiality, integrity, authenticity and availability of information.

This Policy will be made available on the website and internal social media platform for all Serena Team Members.

The Information Technology area will maintain a review/update program to ensure that the technical and legal security requirements implemented are being met and in compliance with current legislation, also including the periodic review of action plans and their adherence to initiatives to share information on cyber incidents.

Adherence to this Policy and any misconduct will be addressed by Serena's Technology Department and, whenever necessary, reported to the Audit and Risk Management Committee.

The terms used in capital letters have the meanings defined in the glossary of the Code of Conduct or in this Information Security Policy.

Target audience

This Policy applies to all advisors, officers, directors, and team members of Serena Energia S.A. and all companies that are part of the Serena Group. This Policy is also extended to all our business partners, including suppliers, service providers, and any other third parties who have relationships with or act on behalf of or represent Serena.

Basic rules of information security

1.1. Principles of information security

Our commitment to the proper handling of information from Serena, customers and the general public is based on the following principles:

a) **Confidentiality**: property by which it is ensured that the information will not be disclosed to persons, systems, bodies or entities without the prior authorization of its owners or of Serena.
b) **Integrity**: property by which it is ensured that the content of the information has not been altered or destroyed in an unauthorized or accidental manner and is therefore complete and authentic.
c) **Availability**: property by which it is ensured that information is accessible and usable, on demand, by a natural person or a particular system, body or entity duly authorized.

1.2. Information life cycle

For the purposes of this Policy, the following shall be considered as the information life cycle:

a) **Handling**: This is the stage where information is created and manipulated.
b) **Storage**: it is the storage of information, whether in a database, on paper, in external electronic media, among others.
c) **Transportation**: occurs when information is transported to some location, regardless of the medium where it is stored.
d) **Disposal**: is the elimination of printed documents (deposited in the recycling bin and/or kept in a storage company), electronic documents or the destruction of storage media (e.g., CDs, DVDs, floppy disks, pen-drives) completely.

1.3. Classification of information

The classification of information should be evaluated according to its content, relevance to external knowledge, and the specific elements of the document. The access, disclosure and treatment of documents (physical or scanned), data or information are restricted to co-entrepreneurs who need to know them due to their activities within Serena, and this access is guided by the rules set forth in this Policy and other company rules.

All information for corporate use must be classified according to the degree of confidentiality for the company's business, considering three levels:

a) **Confidential**: It is the highest degree of secrecy, applied to information of a strategic nature and that must be handled by a restricted group of users. Unauthorized access to this information can have critical consequences for the business, including causing strategic damage to the company's image.
b) **Internal**: This is specific information for internal use, with exclusive circulation within the company. This information may be available to all employees and contractors and should only be used for Serena's activities. This content, even if it is freely circulated within the company, should not be disclosed to external parties without due care, including, when necessary, the signing of confidentiality agreements or formal authorization previously evaluated by the responsible area.
c) **External**: This is information that circulates freely and is in the public domain. This type of information does not require security controls or restrictions for its access or safekeeping.

1.4. Information security incidents

For the purposes of this Policy, a security incident is defined as any adverse event resulting from the action or omission of co-entrepreneurs and third parties, even if intentional, or from a threat that attacks the principles of Information Security.

Information security management sistem

The Information Security Management System is the set of processes and good practices to establish, implement, operate, monitor, review, maintain and improve information security with actions on four major fronts:

- Governance of information security policies and procedures;
- Information security features and components;
- Continuous monitoring of the information technology environment;
- Crisis management and business continuity.

Internal guidelines on information security and cyber security

3.1. Safe behavior

Co-entrepreneurs and partners must take a proactive and engaged attitude with regard to information security, as well as privacy and data protection.

Comments on matters related to Serena and its operations outside of the workplace or in the presence of people who are not connected to them are prohibited.

Internal and/or confidential information must be stored on corporate servers and systems. Information saved locally on the equipment is not considered adequately protected and is not included in corporate backup processes. Information containing personal data of customers, co-entrepreneurs and partners should not be saved locally on the equipment.

Co-entrepreneurs and partners of Serena must not exchange, publish or store strategic, industrial secret and confidential information about Serena, including partners and customers, except on formally defined occasions (such as in the case of disclosure of results of promotions, advertisements, etc.), on social networks, personal e-mail, external systems and equipment.

Electronic mail (e-mail) is a tool made available exclusively for professional use, and is, therefore, subject to analysis/consultation by the company. It must not be used to send spam, chain letters, pyramids, rumors, defamatory, offensive, racist, obscene, illegal material, etc., as provided for in the [IT Asset Acceptable Use Standard] and the Audit and Risk Management Committee.

The use of instant messaging (chat) is restricted to professional use and must be used ethically and responsibly, in accordance with the IT Asset Acceptable Use Standard. It is forbidden to use non-approved instant communication applications to send documents, photos, PDFs, Word, Excel, Power Point files (and

similar platforms), which must be sent by corporate email or by an application approved by the Company.

Co-entrepreneurs and, where applicable, partners should adopt the clean tables and screens policy. Such measures aim to mitigate the risk of unauthorized access, loss and damage of information during and outside working hours. Business information (sensitive or critical, e.g., on paper or removable storage media) should not remain unprotected (e.g., on desks or on whiteboards), and computers should be password locked during the user's absence. Ideally, this information should be stored in a safe, closet, or other security furniture, especially when the office is unoccupied.

The use of corporate equipment should be done only by the professional. Assigning its use to a third individual for any activity unrelated to the professional purpose characterizes an infraction subject to the applicable administrative sanctions.

3.2. Security & privacy by design

Information security and data protection must be proactively followed and implemented from the beginning of the design, development and architecture of new products and processes, incorporating good information security, privacy and data protection practices throughout the entire cycle.

3.3. Data protection

The handling of data, throughout its life cycle, must follow the requirements of the Data Protection Policy.

All information containing personal data that is processed by Serena must be classified according to the degree of confidentiality of its content and thought out according to its value, legal requirements, sensitivity and confidentiality, as provided for in the applicable internal policies and standards.

All co-entrepreneurs and partners are responsible for maintaining the privacy and ensuring the protection of the data processed, as well as ensuring the confidentiality of Serena's information classified as confidential and internal.
Contracts with partners must have a formal confidentiality agreement established before the start of the service provision, as well as the partner must

accept the Company's Information Security Policy, respecting its guidelines and controls.

3.4. Identification/Assessment of threats and vulnerabilities

Serena's Information Security area will be responsible for identifying, assessing, recording and reporting the risks to which processes and assets are subject and possible threat scenarios.

The vulnerabilities and risks identified must be mitigated and monitored, considering current legislation and obligations with regulators.

The correct handling and forwarding of events, their formal documentation, classification and communication to the teams responsible for corrections must be supported, using best practice models and procedures appropriate to the respective threats.

Serena has reviewed or will revise the mandatory contractual clauses for the contracting of suppliers and service providers in order to adapt all to the current policies. For strategic contracts and/or contracts involving the processing of personal data, Serena, prior to signing the contract, will assess the need to proceed with the prior assessment of the supplier and/or provider, to validate the controls applicable to the information and/or data processed by them.

3.5. Business continuity management (BCM)

Serena will make reasonable efforts to ensure the continuity of critical business processes in accordance with applicable internal standards and policies.

The business and support areas are responsible for establishing the operational continuity plans for their area and for regularly testing these plans within the established schedules.

3.6. Prevention and Protection Actions

Standardized routines for the prevention and protection of processes and assets will be adopted, as provided for in the internal standard, carrying out vulnerability analyses, penetration tests and other specific assessments that certify

compliance with security requirements and previously established responsibilities.

Highlighting the periodic execution of attack and invasion tests, in order to monitor the efficiency of its system to protect against cyber vulnerabilities, Serena performs tests, both internally (in the Gray Box mode) and externally (in the Black Box mode).

3.7. Records control

System and application logs will be generated in accordance with legal, regulatory, commercial or business requirements and protected against unauthorized copying, loss, destruction and falsification that seek to ensure the traceability and security of sensitive information as per.

You may not delete, hide, or modify any audit trail on servers and systems. If this occurs, the person responsible will be subject to the applicable internal sanctions.

3.8. Personal mobile devices (BYOD)

In order to have access to Serena's corporate applications and systems through personal mobile devices (Bring Your Own Device – BYOD), the employee and/or partner must accept the "Term of Responsibility " in which they formalize that such choice is of their exclusive initiative, assuming their knowledge and agreement with the Information Security Policy, the Code of Conduct and other applicable standards.

The employee and/or partner must ensure the security of Serena's information, practicing safe behavior, not traveling or storing company information in non-secure channels or places.

The employee and/or partner must ensure compliance of his/her personal device with the items of the Personal Mobile Device Use Policy (network usage, operating system update, device lock settings).

The company may restrict the use of old equipment or equipment that does not offer minimum safety and management control.

3.9. Monitoring & testing

In order to assess the safety of the controls adopted in each of the operational procedures, internal and external audits may be carried out on a regular basis.

Effective internal controls must be implemented to protect Serena's RTICs (Information and Communication Technology Resources), ensuring their confidentiality, integrity, authenticity and availability, always observing the best market practices and current regulations.

The Information Security area can monitor or inspect the RTICs that are on its premises or that interact with Serena's environments whenever it deems necessary.

The activities carried out on workstations and servers, as well as the access and use carried out in corporate e-mail, internet and data stored in Serena's network folders and systems as a whole are monitored, recorded and may be used in case of legal requirement, regulator or demand from the Company.

Mission-critical applications must implement audit trail generation/maintenance, source code versioning, and segregation between production and approval environments. Cyber threats must be analyzed together with the vulnerabilities detected by Information Security in information assets and must have proactive monitoring by the Information Security area.

3.10. Action and incidente response plan

The technological environment must be continuously monitored to detect events, abnormalities, and Information Security Incidents.

The management, response, treatment and reduction of security incidents establishes and provides conditions in which events can be analyzed, correlated, classified, signaled and forwarded to the correct service within a managed and standardized structure for the treatment of such incidents.

Actions, routines, records, definition of responsible persons and teams, communication channels, sharing of information with external agents and issuance of reports must be defined in accordance with internal policies, regulatory requirements and/or other complementary controls that may be required.

Without prejudice to the provisions contained in specific internal rules, Information Security Incidents must be identified and recorded for monitoring action plans and vulnerability analysis, respecting the level of exposure to risk defined by Serena.

a) **Incident reporting**: Users must immediately report incidents to the Information Security Officer and the DPO, through the following channel: dpo@srna.co. Incidents should be assessed and investigated in order to build a consistent analysis of cause, risks, parties involved and response plans. The assessment should be directed to the Director responsible for Cybersecurity, as well as to the company's DPO, so that together they can deliberate on initial actions to be taken. Once the relevance of the incident has been classified, Serena shall issue a communication to those involved, informing the situation that occurred and defined actions, at least in a preliminary manner, informing/notifying them of the activities that will be taken later. In addition, the Information Security Officer shall prepare and disseminate to the Board of Directors the annual report on the action and incident response plans.
b) **Attempt to circumvent**: The mere attempt to circumvent the guidelines and controls established by Serena, when found, shall be treated as a violation/incident.
c) **Treatment of identified vulnerabilities**: The treatment and proactive correction of the main weaknesses or weaknesses of the information assets to be used must be recorded, and the risk must be assessed.
d) **Conflicts of interest**: Serena must have an access process that uses clear and objective criteria to identify conflicts of interest arising from technical limitations or duly authorized situations. Access activities and cyber threats should be monitored.
e) **Incident Registration and Preparation of Action Plan**: Once an Information Security Incident has been identified, and with due communication to the Information Security Officer and the DPO, such incident must be formally recorded, with all the necessary and available information about what happened, without prejudice to updates as new information emerges. The action plan should be prepared by the Information Security managers and the DPO, and other departments may be involved if necessary to implement the solutions and to manage any problems. Such a plan should contain an explicit definition of the roles and responsibilities in resolving the impasse, providing for the activation of key employees and relevant external contacts, if applicable. The threat scenarios foreseen in the risk assessment should be taken into account, and there are criteria for classifying incidents depending on their severity. The action plan should provide for the cases of

need to use the contingency facilities in the most severe cases, as well as the process of returning to the original facilities after the end of the incident. Documentation related to incident management should be archived for auditing purposes.

f) **Notice to External Bodies**: Serena will communicate relevant incidents and interruptions of relevant services that constitute a crisis situation, as well as measures taken for the resumption of these activities to external bodies, when necessary, through the Legal Department and Communication Department.

Training and awareness program

Training and awareness programs for the correct handling of information will be established, in order to continuously develop the culture and responsibility in information security by the co-entrepreneurs.

Through its internal platforms, Serena promotes a recurring awareness plan on the importance of Information Security aimed at the entire internal public, in addition to a security summary published on the company's portals.

Disciplinary measures

Violations of the provisions of this Policy may lead to disciplinary sanctions, including warning, suspension or immediate termination of employment or contract of service, according to established criteria.

In the case of partners, violations of the Policy and the information security clauses provided for in the contract may result in warnings ranging from warnings to the cancellation of the contract and the application of the applicable penalties in accordance with the Law.

Updates and version history

This Policy will be reviewed as needed, with each update, its internal target audience should explicitly adhere to its standards, and it will be made available to other relevant audiences.

Approval Date:	Approved by:	Version:	Validity:	Description:
June 12, 2024	Board of Directors	2nd	June 12, 2024 to June 12, 2026 or until the publication of a new version if earlier than the end of the validity	Current version
December 19, 2021	Board of Directors	1st	December 19, 2021 until June 11, 2024	Previous version

Annex I – Access Management

Purpose: The process of granting access to Serena's information assets aims to ensure appropriate access to employees and third parties, in accordance with their roles in the company, while maintaining data security and integrity.

Procedures:

1. **Automated Access Request:**

- During the onboarding process, movement or new access requests, an automated flow is triggered.
- The application is initiated electronically, containing details such as full name, date of birth, role, and reason for the request.
- The system forwards the request for approval by the responsible managers, ensuring a fast and efficient process.

2. **Access Account Creation:**

- Accounts are automatically created after approval in the automated flow.
- The recruitment/management team follows the process to ensure that the essential information is correct.

3. **Change of Access Account:**

- Derived from transfers or changes in the roles of co-entrepreneurs.
- The previous manager validates pending issues and the new manager approves the changes in the automated system.

4. **Automated Access Account Lockout:**

- During the termination or role change process, an automated flow is triggered.
- Access is automatically blocked after the pending issues have been validated by the people management team and manager.

5. **Approval Flow:**

Access requests are routed to the appropriate managers for approval, ensuring that only authorized people have access to the necessary resources.

Annex II – Change management

Goal: Change management aims to ensure the preservation of controls related to the availability, integrity, confidentiality, and authenticity of data during any change to relevant systems or technological infrastructure. All changes will be managed by the Information Technology Department in a planned, approved, tested manner and in accordance with the change management process.

Change Management Process: We have differentiated processes for Cloud environments and On Premise environments.

On-Premise and IaaS Environments: For Serena's physical and internal environments, Cloud IaaS and Enterprise Systems, we will follow the Change Management process. This includes the change log, test run, rollback methods, and approving or disapproving the change. The registry also allows for requests for emergency changes, which require immediate intervention and are subject to leadership approval. All cases are recorded for future audits and lessons learned.

Software Engineering – Cloud: In DevOps environments, we follow the CI/CD (Continuous Integration/Continuous Deployment) process. This involves automation in the scheduling of the release, review of changes in the DEV environment by a developer other than the creator of the code, merge of the DEV environment to STAGING environment, approval by the QA team in STAGING environment and, finally, merge of the STAGING environment to PROD environment. In unplanned cases, the Tech Lead is responsible for executing the rollback process, using the merge of the previous release in the PROD environment. All steps are recorded with audit logs for future analysis and lessons learned.

SaaS Environments: For SaaS environments, we follow the procedures determined by the contracted partners. We are notified of releases, usually quarterly for the entire environment, in advance for testing and validation. The Tech team is responsible for managing pre-validations with key users when necessary and communicating with the company about these updates.

Monitoring & Reporting: On a monthly basis, during the GMUD Committee meetings, a detailed report will be presented that includes the amount of normal changes, emergency changes, canceled changes, and changes executed without

due process and approval. These reports aim to ensure transparency and accountability in our change management processes.

Annex III – Operation management

Goal: Carry out the management of the life cycle (acquisition, maintenance, updating, support and disposal) of the company's technology and telecommunications resources and ensure that the company's users make full use of said resources, taking into account good market practices, information security practices and, when applicable, privacy and data protection practices defined in this Policy.

Process:

- **Crisis support and management:**

The technology area responds to the requests of users, considering that they must make adequate use of technology resources, through the registration of incidents, doubts, difficulties or problems in the use of resources and technology.

The technology area provides and organizes communication channels for the organization of the daily operation:

- Groups on communication platforms: There are fixed groups for monitoring the operation and specific groups created for the management of specific crises.
- Call reporting system: There is the company's own system, managed by the technology area, and the ticketing systems of service providers, such as NOC and SOC.

- **Monitoring:**

The company has 24 x 7 monitoring on two fronts:

- **Network Operations Center** (**NOC**): Team that monitors the availability and performance of the technology environment. When alarms and events occur, the NOC notifies the technical team of the company's technology area and immediately initiates action (with telecommunications providers,

technology suppliers and other service providers). The NOC also acts reactively when users report problems or doubts in the use of the company's communication resources.

- **Security Operations Center** (**SOC**): This team monitors, through tools such as SIEM and CAS, the technology environment with a focus on information security, constantly monitoring the events generated in the environment (alerts, alarms and other data from the various platforms used by the company, whether in the cloud or on premise). Each alarm or alert is properly analyzed and handled. According to the levels of criticality of each event, more or less energetic actions can be taken. Relevant events are notified by email. Critical events require telephone contact with the company's technology area, usually after the mitigation and containment measures of the risk, threat or incident have been taken.

A weekly meeting is held to monitor indicators related to information security.