1001 - Security policy

Parc Científic i Tecnològic Agroalimentari de Lleida · Edifici H1 2a planta B · 25003 Lleida (Spain)

(+34) 973 282 300 · info@lleida.net

Lleida.net

Change control

Date	Version	Changes	Author
19/12/2014	1.0	Author	Manel Cervera Díaz
04/01/2016	1.1	Review and update	Manel Cervera Díaz
16/03/2016	1.2	Separation of document objectives	Manel Cervera Díaz
02/12/2016	1.3	Review and update	Jordi Ramón
22/12/2017	1.4	Review	Jordi Ramón
23/07/2018	1.5	Updating the accepted risk threshold and updating confidentiality	Jordi Ramón
09/11/2018	1.6	Alignment with scope services, normative update affects, substitution commitment to obtain maintenance of the ISMS.	Eva Pané
20/12/2018	1.7	Forecast of communication of security incidents. Updating of data protection compliance.	Eva Pané
17/12/2019	1.8	Reference to the Privacy Policy and the concept of privacy in the design of the development of applications. Reference to the approval of this policy by the Steering Committee and its publication on Lleida.net website	Eva Pané
29/05/2020	1.9	Specific references are added to access control and physical security.	Eva Pané
22/02/2021	1.10	Updated normative reference of trusted services.	Eva Pané
18/02/2022	1.11	Review without changes	Eva Pané

Distribution list

Departments
Lleida.net

Document classification and status

Document classification	Public

Document status	Approved

Lleida.net · Parc Científic i Tecnològic Agroalimentari de Lleida (PCiTAL) · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

Lleida.net

Contents

Lleida.net · Parc Científic i Tecnològic Agroalimentari de Lleida (PCiTAL) · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

1 Presentation

1.1 Aim

This policy aims to establish the commitment of Lleida.net Steering Committee regarding the security of information and the protection of information assets necessary for the performance of the functions described in the scope to achieve its objectives.

This commitment comes into being through implementing and maintaining an Information Security Management System (ISMS) in compliance with the international standard ISO / IEC 27001: 2013.

1.2 Scope of Application

All members of Lleida.net and all third parties are identified under the scope of the Information Security Management System (ISMS).

1.3 Distribution and review

Document 1006 - Document Inventory displays the distribution list, the responsibility for review and approval of this document, and the status of updating referenced ISO/IEC 27001:2013 documents and/or controls.

Lleida.net · Parc Científic i Tecnològic Agroalimentari de Lleida (PCiTAL) · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

2 Information security policy

Lleida.net is committed to securing all the assets under its responsibility through the necessary measures, guaranteeing compliance with regulations and applicable laws. Therefore, the strategic business objective of Lleida.net is to obtain the ISO 27001: 2013 certification for the management of the Data certification process, SMS solutions and data validation.

To comply with ISO 27001: 2013, Lleida.net is fully committed to:

maintain an Information Security Management System (ISMS) that includes the processes, resources, procedures, technologies and tools necessary to guarantee the confidentiality, integrity and availability of the information assets and technological assets, supporting Lleida.net. In particular to the processes included in the scope.

2.1 Responsibility

Compliance with this Security Policy is the responsibility of Lleida.net staff and the external personnel included in the scope of the Information Security Management System. Lleida.net Management expects internal and external personnel to be familiar with this Security Policy.

2.2 Information Security

Security information refers to protecting information assets against unauthorised disclosure, modification or destruction, whether accidentally or intentionally caused. The security attributes associated with the information assets are:

- **Confidentiality:** Information is not made available or disclosed to unauthorised individuals, entities or processes.
- **Integrity:** To safeguard the accuracy and completeness of information assets.
- **Availability:** Property of being accessible and usable by an authorised body.
- **Authentication.** A feature allowing the identification of the generator of the information.
- **Traceability** Feature whereby the history of changes in the information and its relevant modifications based on pre-established procedures can be known.

2.3 Information assets

The information assets referred to in this policy include any information supported in physical format (paper, contracts, business cards, etc.) or electronic (servers, laptops, mobile phones, etc.) and that Lleida.net requires for the performance of its functions and the achievement of its strategic and operational objectives. Specific guidelines related to the acceptable use and treatment of information assets are laid down in the 2004 - Information Assets Regulations.

2.4 Objectives of Lleida.net

This policy aims to establish the necessary guidelines regarding Information Security, which Lleida.net Management considers an essential requirement for achieving strategic and operational objectives. Available in document “1008 - Lleida.net Objectives”.

Lleida.net · Parc Científic i Tecnològic Agroalimentari de Lleida (PCiTAL) · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

2.5 Security Policy Guidelines

Lleida.net Management considers that the achievement of the company objectives is subject to compliance with various requirements to guarantee the organisation's information security. Therefore, it is assumed that Information Security must be a priority for the organisation, so this policy establishes the following guidelines:

- The information that Lleida.net is proprietary and/or depositary must be only accessible to duly authorised persons, whether or not they belong to the Organization
- This Security Policy, as well as the rest of the Regulatory Body of the ISMS (procedures, guides, etc.), must be accessible to all Lleida.net members within the scope of the ISMS, as well as the external personnel related to it through some of its processes
- The Organization must comply with all those legal, regulatory and statutory requirements applying to them, as well as the contractual requirements
- The confidentiality of information should be observed at all times
- The integrity of the information must be ensured through all the processes that manage, process and store it
- The availability of information must be guaranteed through adequate support measures and business continuity
- All personnel within the scope of the ISMS of Lleida.net must have the appropriate training and awareness of Information Security
- Any incident or weakness that could threaten or have threatened the confidentiality, integrity and/or availability of the information should be registered and analysed to apply the corresponding corrective and/or preventive measures. Likewise, the parties involved will be informed in due time.
- Any member of Lleida.net within the scope of the ISMS, both belonging to the Steering Committee and the Operative Group, is responsible for implementing, maintaining and improving this policy and ensuring compliance with it.
- Any member of Lleida.net within the scope of the ISMS is responsible for ensuring the proper implementation, maintenance and improvement of the ISMS, as well as its compliance with ISO / IEC 27001: 2013

The roles related to the guidelines of the Security Policy are established in Regulation "2001 - Responsibilities SGSI Lleida.net".

2.6 Information security regulatory body

As part of this policy, documentation has been generated for Regulations and Procedures that apply to the processes described in the scope of the ISMS. Such documentation will be distributed to all the parties concerned through the appropriate channels and based on their needs.

Lleida.net · Parc Científic i Tecnològic Agroalimentari de Lleida (PCiTAL) · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

2.7 Analysis and Risk Management

Information Security is controlled and monitored by the Management of Lleida.net through the Risk Analysis and Management framework established within the ISMS. This framework allows the Management of Lleida.net to assess the degree of internal control on information assets through a risk analysis methodology that provides objective, measurable and reproducible results.

2.8 Residual risk accepted

The Management of Lleida.net, assuming that the complete mitigation of any risk is not attainable, establishes that the level of residual risk associated with any of the information assets included in the scope of the ISMS should not be higher than level 8 (scored on a scale of 25) For the Management of Lleida.net, this level represents the threshold of residual risk whose mitigation cost is greater than the loss incurred in case of materialisation thereof. If any residual risk associated with any of the information assets exceeds the level of accepted risk,Lleida.net Management will evaluate the mitigation options of the risk. It will provide the necessary resources to place it below the level of residual accepted risk.

2.9 Violations of the Policy and Disciplinary Process

Any exception to this Security Policy must be registered and informed to the Management of Lleida.net. Likewise, any breach may lead to disciplinary actions pursuant to the applicable legislation.

It is the responsibility of all the members of Lleida.net to notify the Management of Lleida.net of any event or situation that could suppose the breach of any of the guidelines defined by this policy.

2.10 Legal and statutory compliance

This policy establishes the need to comply with legislative, regulatory and contractual requirements for Lleida.net and managing information assets. In this respect, the Management of Lleida.net is committed to providing the necessary resources to comply with all legislation and regulations applicable to the activity of Lleida.net and establishes the responsibility for such compliance on all its members.

Thereupon, compliance with all applicable legislation and regulations will be ensured, which mainly includes the following aspects:

- Legislation related to the protection of personal data:
    - Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 concerning the protection of natural persons concerning the processing of personal data and the free circulation of these data and which repeals Directive 95/46 / EC (GDPR).
    - Organic Law 3/2018, of 5 December, protection of personal data and guarantee of digital rights.

Lleida.net · Parc Científic i Tecnològic Agroalimentari de Lleida (PCiTAL) · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

  - REAL DECRETO 1720/2007, of 21 December, approving the Regulation implementing the Organic Law 15/1999, of 13 December, governing Personal Data Protection

- Law of Services of the Information Society (LSSI):
  - Law 34/2002 of 11 July on Services of the information society and electronic commerce.
- Legislation related to trusted services:
  - Regulation (EU) 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 / EC.
  - Law 6/2020, 11 November, regulating certain aspects of electronic trusted services.
- Legislation related to telecommunications:
  - Law 9/2014 9 May on Telecommunications.

Likewise, compliance with any other applicable legislation or regulation must be ensured. More info Regulation "2015 - Regulations on Regulatory and Contractual Compliance" outlines such requirements, particularly those related to the management of intellectual property and personal data.

2.11 Awareness and training on information security

All members of Lleida.net must have the appropriate training to perform their duties. Likewise, the proper awareness of the members of Lleida.net should be ensured in terms of Information Security and good practices.

Likewise, the members of Lleida.net must have access to and knowledge of the regular updates of this policy and the rest of the Regulatory and Documentary Body of the ISMS. Specific guidelines on training and awareness are set out in the Regulation "2003 - Information Security Awareness and Training".

2.12 Commitment to continuous improvement

Lleida.net aims for continuous improvement in terms of its ISMS. These are ensured through the following actions:

- Assessment of the improvement aspects detected in internal and external audits. The organisation analyses the root cause of the non-conformities and opportunities for improvement that third parties notice, defining action plans to improve these aspects.
- The organisation schedules regular reviews throughout the year to detect potential areas for improvement

In doing so, the organisation seeks to continually improve its ISMS's effectiveness and appropriateness to the surrounding context. 2018 - Information security control regulation and improvement".

Lleida.net · Parc Científic i Tecnològic Agroalimentari de Lleida (PCiTAL) · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net

2.13 Security incidents

A security incident consists of any event that could threaten the confidentiality, integrity, and/or availability of the information and threaten the achievement of Lleida.net objectives.

This policy establishes the obligation and responsibility of all the members of Lleida.net, as well as third parties included in the scope of the ISMS, the identification and notification to the Lleida.net managers of any incident that could threaten the security of the information assets of Lleida.net, as well as any situation that could lead to non-compliance with the ISMS procedures and the ISO / IEC 27001: 2013 standard.

The "2014 - Incident Management Regulation" sets specific guidelines on security incident management.

2.14 Privacy

The commitment to the privacy of the processed data that Lleida.net should deal with is reflected in the Privacy Policy (DP 1001- Privacy Policy) available to the public through the corporate website.

Likewise, the organisation will apply the principle of privacy in developing applications developed in "2005 - Security in the development and maintenance of " applications.

2.15 Access control

Lleida.net takes steps to ensure the security of the information by controlling the logical and physical access to it, the information processing resources and the business processes that must be controlled based on the business requirements, through the establishment of the guidelines to be followed for the management of access to the systems, as well as the roles and responsibilities of the users and the defined controls. The specific set of guidelines related to access control is detailed in the "2009 - Access Control Security Regulations".

2.16 Physical security

Measures must be taken to manage the physical security in Lleida.net facilities through protocols to access the facilities for each role, providing information on the secured areas and defining each workplace role. Therefore, the guidelines related to physical access control are set out in Regulation "2009 - Access Control Security Regulations" and further complemented by the procedure "3009 - Physical Security Procedure".

Lleida.net · Parc Científic i Tecnològic Agroalimentari de Lleida (PCiTAL) · Edifici H1, 2a planta B · 25003 Lleida (Spain) · (+34) 973 282 300 · info@lleida.net