1001 - Security policy

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

+34) 973 282 300 · info@lleida.net

Document 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	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

Distribution list

Departments
Lleida.net

Document classification and status

Document classification	Public

Document status	Approved

Referred documents

Documents
3001 - Management of the documentation repository
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

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 Introduction

1.1 Objective

The purpose of this policy is 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 the implementation and maintenance of 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, as well as all third parties identified in the scope of the Information Security Management System (ISMS).

1.3 Distribution

Approved by Lleida.net Steering Committee, this Policy must be accessible to all people included in the distribution list in the documentary control, through the appropriate channels established in the procedure 3001 - Management of the documentation repository.

1.4 Review

This Security Policy will be reviewed and approved annually by the Steering Committee of Lleida.net. However, if changes relevant to the Organization take place, whether these are operational, legal, regulatory or contractual, they will be revised whenever deemed necessary, thus ensuring that the Policy remains adapted at all times.

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 mail certification process.

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

Establish and 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 giving support to Lleida.net. In particular to the processes included in the scope.

2.1 Liability

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

2.2 Information Security

Security information refers to the protection of information assets against unauthorized 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 unauthorized individuals, entities or processes
- **Integrity:** To safeguard the accuracy and completeness of information assets
- **Availability:** Property of being accessible and usable by an authorized body

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.

2.4 Strategic objectives of Lleida.net

This Policy aims to establish the necessary guidelines regarding Information Security, which are considered by Lleida.net Management as an essential requirement for the achievement of 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 aimed at guaranteeing Information Security within the Organization. Therefore, it is considered that Information Security must be a priority for the organization so this Policy establishes the following guidelines:

- The information that Lleida.net is proprietary and / or depositary must be only accessible to duly authorized 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 ensured 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
- 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 as well as 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

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.

2.7 Analysis and Risk Management

Information Security is controlled and monitored by the Management of Lleida.net through the framework of Risk Analysis and Management established within the ISMS. This framework

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

allows the Management of Lleida.net to assess the degree of internal control on information assets through the use of 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 6 (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 materialization 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 and 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 all those legislative, regulatory and contractual requirements that apply to Lleida.net and the information assets managed. 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 (LOPD):
  - LEY ORGÁNICA 15/1999 of 13 December, governing of Personal Data Protection
- REAL DECRETO 1720/2007, of 21 December, approving the Reglamento de Desarollo de la LEY ORGÁNICA 15/1999, of 13 December, governing Personal Data Protection
- Law of Services of the Information Society (LSSI):
  - Law 34/2002 11 July of Servicios de la Sociedad de la Información y Comercio Electrónico
- Legislation related to electronic signature:
  - Law 59/2003, of December 19, on electronic signature

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

Likewise, compliance with any other applicable legislation or regulation must be ensured.

2.11 Awareness and training on information security

All members of Lleida.net must have the appropriate training to perform their duties. Likewise, the appropriate 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.

2.12 Security incidents

A security incident consists of any event that could threaten the confidentiality, integrity and / or availability of the information, as well as 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, of 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.

This Security Policy comes into force on the day of its publication.

3 Map of clauses of ISO27001: 2013

ISO/IEC 27001:2013 clauses
5.1 - Leadership and commitment
5.2 - Policy

4 Map of controls of ISO 27002:2013

ISO/IEC 27002:2013 Control
5.1.1 - Policies for information security
5.1.2 - Review of the policies for information security

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