1001 - 安全政策

Parc Científic i Tecnològic Agroalimentari de Lleida H1 栋, 2 楼 B 25003 莱里达 (西班牙)

(+34) 973 282 300 • info@lleida.net

文件记录

日期	版本	修改	作者
2014/12/19	1.0	创建者	曼内尔·塞维拉·迪亚兹（Manel Cervera Diaz）
2016/1/4	1.1	审查与更新	曼内尔·塞维拉·迪亚兹（Manel Cervera Diaz）
2016/3/16	1.2	隔离文件目标	曼内尔·塞维拉·迪亚兹（Manel Cervera Diaz）
2016/12/2	1.3	审查与更新	乔迪·拉蒙（Jordi Ramon）
2017/12/22	1.4	审查	乔迪·拉蒙（Jordi Ramon）
2018/7/23	1.5	更新已接受的风险阈值并更新保密性。	乔迪·拉蒙（Jordi Ramon）
2018/11/9	1.6	与范围内的服务保持一致，更新受影响的条例，以采购承诺取代 ISMS 的维护。	伊娃·潘妮（Eva Pané）
2018/12/20	1.7	对安全事件的通报进行预测。 数据保护合规性更新	伊娃·潘妮（Eva Pané）
2019/12/17	1.8	参考隐私政策和应用开发中的设计隐私概念。 提及本政策经安全委员会批准并在 Lleida.net 网站上公布。	伊娃·潘妮（Eva Pané）
2020/5/29	1.9	增加了关于出入控制和实体安全的具体内容。	伊娃·潘妮（Eva Pané）
2021/2/22	1.10	最新的信托服务监管参考资料	伊娃·潘妮（Eva Pané）

分发列表

部门
Lleida.net

文档的分类和状态

文档分类	公共文档

文件状态	已审

参考文件

文件

3001 - 文档管理
1008 - Lleida.net 目标
2005 - 应用开发安全
DP-1001 隐私政策

目录

1 介绍

1.1 目标

此政策的目标是确立 Lleida.net 董事会的委员会代表对信息的安全性和资产保护的承诺，并且这些信息资产是履行该公司服务范围所述功能必须信息。

通过实施和维护符合国际标准 ISO / IEC 27001：2013 的信息安全管理系统（ISMS），将实现这一承诺。

1.2 适用范围

Lleida.net 的所有成员以及信息安全管理系统（ISMS）范围内确定的所有第三方。

1.3 分配

Lleida.net 指导委员会批准，本政策必须通过文件控制中指定的发行清单中包括的所有人员，通过程序 3001 - 文件库管理中建立的相应渠道进入。

1.4 审查

本安全政策将由 Lleida.net 的指导委员会每年审核并批准。但是，如果发生与本组织有关的变更，无论这些变更是业务性的，法律性的，监管性的还是合约性的，只要认为必要就会进行修改，从而确保政策始终适用。

2 信息安全政策

Lleida.net 保证通过必要的措施确保其责任范围内的所有资产，并始终保证遵守所有的法规和所有适用的法律。因此，Lleida.net 的战略业务目标是在通知和电子合同流程管理、短信解决方案和数据验证方面获得 ISO 27001:2013 认证。

为了遵守 ISO 27001：2013 标准，Lleida.net 承诺：

维护一个信息安全管理系统（ISMS），该系统包括必要的过程，资源，程序，技术和工具，以保证 Lleida.net 信息资产和技术资产的机密性，完整性和可用性。特别是对业务范围中包含的过程。

2.1 责任

本安全政策的履行由所有 Lleida.net 员工以及信息安全管理系统范围内的外部人员负责。Lleida.net 董事会希望所有内部和外部人员熟悉本安全政策。

2.2 信息安全

“信息安全”是指保护信息资产，防止未经授权的披露，修改或破坏，无论是无意还是故意造成的。与信息资产相关的安全属性是：

- **保密性：**未向未经授权的个人，实体或流程披露信息的资产
- **完整性：**保障信息资产的准确性和完整性
- **可用性：**信息资产可悲已授权的实体个人/企业访问或使用。

2.3 信息资产

本政策中提及的信息资产包括以物理格式（纸张，合同，名片等）或电子（服务器，笔记本电脑，手机等）支持的任何信息，并且 Lleida.net 要求 以履行其职能并实现其战略和业务目标。

2.4 Lleida.net 的目标

本政策旨在确立关于信息安全的必要指导原则，Lleida.net 管理层认为这是实现战略和运营目标的基本要求。这些可以在文档 1008 - Lleida.net 目标中查阅。

2.5 安全策略指南

Lleida.net 董事会认为，实现集团的目标需要遵守旨在保证本组织内部信息安全的各种要求。通过这种方式，认为信息安全必须成为组织的优先事项，为此，本政策制定了以下准则：

- Lleida.net 专有和/或保存的信息只能由正式授权的人员访问，无论他们是否属于本公司

- 本安全政策以及 ISMS 规范性主体（程序，指南等）的其余部分必须能够在 ISMS 范围内的所有 Lleida.net 成员以及通过它的一些过程访问与其无关的人员。
- 本组织必须遵守所有适用的法律，监管和法定要求以及合同要求
- 必须始终保证信息的机密性
- 信息的完整性必须通过所有管理，处理和存储过程来保证
- 信息的可用性必须通过适当的支持措施和业务连续性来保证
- Lleida.net 的 ISMS 范围内的所有人员必须对信息安全事宜进行适当的培训和意识
- 任何可能危及或损害信息的机密性，完整性和/或可用性的事件或弱点都应进行登记和分析，以采取相应的纠正和/或预防措施。也会在相应的期限内通知有关方面。
- Lleida.net 中的每个成员都属于指导委员会和执行集团，属于 ISMS 范围，负责实施，维护和改进本政策并确保遵守该政策。
- 在 ISMS 范围内的每个 Lleida.net 会员都有责任确保 ISMS 的正确实施，维护和改进，并符合 ISO/IEC 27001：2013 标准。

2001 年条例 -- -- SGSI Lleida.net 的职责中规定了与安全政策准则有关的作用。

2.6 信息安全监管机构

作为这项政策的一部分，所产生的文件涉及适用于 ISMS 范围内描述的流程的条例和程序。所述文件将通过适当的渠道并基于知识的需要分发给所有感兴趣的各方。

2.7 风险管理和分析

信息安全由 Lleida.net 董事会通过 ISMS 内建立的风险分析和管理框架进行控制和监控。该框架允许 Lleida.net 董事会通过使用风险分析方法评估信息资产的内部控制程度，该风险分析方法提供客观，可测量和可重复的结果。

2.8 已接受剩余风险

假设完全缓解任何风险无法实现，Lleida.net 董事会确定与 ISMS 范围内包含的任何信息资产相关的剩余风险水平不应高于第 6 级（约 比例为 25）。对于 Lleida.net 董事会，这一水平代表了剩余风险的门槛，其缓解成本高于其实际发生时的损失。如果与任何信息资产相关的剩余风险超过所接受的风险水平，Lleida.net 管理层将评估所述风险的缓解措施，并提供必要的资源，使其低于剩余风险水平接受。

2.9 政策和纪律程序的违反

此安全政策的任何例外都必须注册并通知 Lleida.net。同样，违反相同规定可导致根据适用法律适用相应的纪律处分。

Lleida.net 的所有成员有责任通知管理层任何可能会违反本政策规定的任何指导方针的事件或情况。

2.10 法律和法规遵从

本政策规定需要遵守适用于 Lleida.net 和托管信息资产的所有立法，监管和合同要求。从这个意义上说，乐达网的管理层致力于提供必要的资源，以遵守适用于乐达网活动的所有法律和法规，并为所有成员规定了这种合规责任。

在这方面，将确保遵守所有适用的法律和法规，主要包括以下几个方面：

- 有关保护个人资料的立法：
  - 欧洲议会和理事会 2016 年 4 月 27 日关于在处理个人数据方面保护自然人和此类数据的自由流动并废除第 95/46/EC 号指令(GDPR)的第(EU)2016/679 号条例。
  - 12 月 5 日第 3/2018 号组织法，保护个人数据和保障数字权利。
  - - 皇家法令第 1720/2007 号于 12 月 21 日批准的“个人数据保护组织法”的制定条例，。
- 信息社会服务法（LSSI）：
  - -关于信息社会和电子商务服务的第 34/2002 号法律， 7 月 11 日。
- 与信托服务有关的立法。
  - 欧洲议会和理事会 2014 年 7 月 23 日关于内部市场电子交易的电子身份识别和信托服务并废除第 1999/93/EC 号指令的第 910/2014 号条例(欧盟)
  - 11 月 11 日第 6/2020 号法律，规范电子信托服务的某些方面
- 与电信有关的立法：
  - 5 月 9 日关于电信的第 9/2014 号法律

同样，必须确保遵守任何其他适用的法律或法规。

2.11 信息安全方面的意识，教育和培训

Lleida.net 的所有成员都必须接受适当的培训才能履行职责。同样，在信息安全和良好实践方面，应确保 Lleida.net 成员的适当意识。

同样，Lleida.net 的成员必须能够获得并了解本政策的定期更新以及 ISMS 规范性和纪录性机构的其他部分。

2.12 安全事件

安全事件包括任何可能损害信息的机密性，完整性和/或可用性的事件，并影响 Lleida.net 目标的实现。

本政策规定了 Lleida.net 的所有成员以及包含在 ISMS 范围内的第三方的义务和责任，以确定并通知 Lleida.net 管理人员任何可能危及安全的事件。 Lleida.net 的信息资产以及可能导致不符合 ISMS 程序和 ISO / IEC 27001：2013 标准的任何情况。

2.13 隐私

Lleida.net 对数据处理的隐私承诺反映在通过公司网站向公众提供的隐私政策（DP 1001-隐私政策）中。

同样，本组织将在 2005 年开发的应用程序中应用隐私原则———开发和维护应用程序的安全。

2.14 访问控制

Lleida.net 采取措施，通过控制对信息的逻辑和物理访问、信息处理资源和基于业务需求必须控制的业务流程，建立系统访问管理应遵循的准则，以及用户的角色和责任，并确定控制措施，以保证信息的安全性。

2.15 实体安全

必须通过建立针对必须访问的不同角色的设施的访问协议，对 Lleida.net 的不同设施中的物理安全进行管理，区分特别安全的区域，并确定工作站的可接受用途。

该安全策略已由 Lleida.net 安全委员会批准，并在 Lleida.net 网站主页上发布的同一天生效。

3 ISO 27001：2013 的条款图

ISO 27001:2013 条款
5.1 - 领导和承诺
5.2 - 政策

4 ISO 27002：2013 的控制图

ISO 27002:2013 控制
5.1.1 - 信息安全政策
5.1.2 - 审查信息安全政策