LEVIAhub
SUPPLY CHAIN MASTER

信息安全管理体系政策

信息安全管理体系政策

LEVIAHUB S.p.A. 的管理层和员工将信息安全作为其各项活动的基础，其首要目标是保护公司的信息资产，以最大限度地减少由来自内部、外部或潜在威胁的有意或无意安全事件对公司本身以及使用 LEVIAHUB S.p.A. 所创建产品的公司客户造成损害的风险。应用本政策和管理该体系的责任涵盖整个公司组织，从管理层到每一位员工，各司其职。

为实现这一首要目标，LEVIAHUB S.p.A. 追求以下目标：

- 确保遵守适用的强制性法规；
- 通过适当的风险分析确定信息资产的价值，以了解公司内存在的、可能导致无法实现目标的脆弱性和潜在威胁；
- 通过设计、实施和维护适当的信息安全措施，将风险控制在可接受的水平，以确保所提供产品和服务的质量；
- 保护信息的保密性，确保信息仅可被授权人员访问，并对需要一定保密程度的信息进行分类；
- 保护信息的完整性，尽可能保护其准确性和完整性以及其处理方法；
- 保护信息的可用性，确保授权用户在需要时能够实际访问其工作所需的信息和资产；
- 在工作活动过程中出现新需求时及时、有效地采取行动；
- 制定应急计划、应变计划，并在必要时制定业务连续性计划，并尽可能保持其更新和受控。
- 定期审查政策、目标及管理体系的实施情况，以实现公司信息安全水平的持续改进。

在应用其管理体系时，LEVIAHUB S.p.A. 依据欧盟条例 679/2016（GDPR）、指令 2555/2025（即所谓的 NIS2 指令）以及任何相关法律和法规，遵守有关个人数据保护的强制性规定。因此，LEVIAHUB S.p.A. 以合法、正当和透明的方式处理数据，仅用于被认为必要的目的和必要的操作（最小化原则）。LEVIAHUB S.p.A. 还致力于 保留准确的数据，在必要时进行更新，并仅在被认为对执行公司活动严格必要的时间内保存。LEVIAHUB S.p.A. 保障数据主体在法律规定的限度内访问其个人数据，以及在特定识别的情况下进行删除和被遗忘的权利。公司致力于通过适当的技术措施并借助管理体系所规定程序的应用来保护其数据。
对于组织的改进、有效性和效率同样重要的是一种基于预防问题而非事后控制和纠正的方法，以显著减少事件或其他不符合项发生的可能性。各级人力资源是实现计划目标的基本要素：通过推动实施特定的培训项目并重视所取得的成果，使其对公司的信息安全目标提高认识。
以任何方式涉及管理体系适用范围的全体公司人员和供应商，均有责任在批准该政策的管理层的支持下实施本政策。
公司旨在管理信息安全事件，尽可能预防信息安全事故；在无法做到这一点时，至少管理所有信息安全违规和可能的薄弱环节，这些都必须在遵守强制性和规范性规定的前提下，报告给相关责任人并进行调查。

信息安全管理体系旨在为管理层提供一致的结果，以便以连贯而慎重的方式对管理体系本身进行适当评估并设定目标，从而在考虑组织环境、风险和可用机会的情况下做出适当的决策。
本政策由公司管理层制定和审查。全体人员应根据其自身了解的情况，负责向体系负责人报告在公司系统中发现的任何薄弱环节。
本政策定期接受审查，以识别影响其的任何变更，并确保其始终适合组织的目的和利益相关方的期望。

公司管理层