保障信息安全

立讯精密致力于创建合规、安全、稳定的业务环境，通过信息安全与隐私保护管理体系的有效运行，保护公司、客户及其他相关方免受信息泄露等数据安全及隐私事件影响。

信息安全管理

公司依托 ISO 27001 信息安全体系标准，通过实施 BCM、信息安全稽核、数据保护管理、安全意识宣导等管理措施，提升公司信息安全稳健性。

信息安全管理亮点措施

业务连续性管理

- 进行关键业务全节点多维度应急演练，包括备份回复，网络中断，关键节点服务器故障，错误配置等

信息安全稽核

- 执行覆盖所有厂区的渗透测试、漏洞扫描和信息安全稽核，完成了 280 个改善项目

数据保护管理

- 持续落实保密区域相关设备的全区域覆盖
- 开展个人信息和数据出境风险调研，保护隐私数据

安全意识宣导

- 使用海报、漫画形式结合时事热点进行信息安全意识宣导

2024 年，基于对第三方翻译平台潜在信息安全风险的全面评估，公司自主研发了全封闭式本地化翻译处理系统，通过构建内部可控的智能处理体系，有效规避商业机密信息的泄露。此外，我们针对新产品导入相关的保密区开发了终端哨兵系统，实时监控终端安全状态，定期上报关键指标，并实现异常自愈和及时预警，针对孤点异常等难以发现的情况，亦可实现第一时间预警，充分强化了安全指标监控与可视化管理，助力安全人员迅速响应并处置，有效提升数据安全性。

报告期内，立讯精密：

未发生

任何信息泄露事件

信息安全培训

我们对员工及供应商开展了一系列信息安全培训，以提升员工的信息安全意识和技能及供应链信息安全水平。

员工

公司在多个厂区开展了包含信息安全意识、保密意识、信息安全管理体系标准、钓鱼邮件防范等方面的信息安全培训，**员工总学习时长达到 506,805 小时**。

供应商

我们实施严格的考核制度，要求供应商相关人员通过专业考试后方可进入制造现场，从而确保供应商在信息安全管理方面的合规性。2024 年，为持续优化供应商信息安全管理，立讯精密针对保密项目专案区的供应商开展了全面的培训与稽核，**完成 300 余次现场稽核与指导**，宣贯信息安全重要性与实践操作要点，确保供应商工作设备和环境的信息安全。

隐私保护管理

公司结合《中华人民共和国个人信息保护法》等国家法律法规、客户和行业标准，**制定了《商业秘密管理程序》《相关方信息安全管理程序》等一系列隐私管理制度及脱敏标准**，通过 COC、《员工手册》等规范对隐私保护内容进行要求，并通过定期培训考核切实约束员工行为，禁止泄露合作方的隐私和商业信息。

隐私保护举措

分类管理

- **隐私保护内容：**
  按照客户要求或公司标准进行分类
- **隐私保护标识**
  按确定的密级和保密期限，对商业秘密数据做好密级标识或加盖识别印章
- **脱敏资料保护**
  根据不同业务、部门和相关方制定脱敏标准

访问权限

- **授权管理**
  要求使用规范、满足复杂度要求的用户名称、密码或口令，不得将密码或口令泄露给无关或未授权人员
- **设备检修**
  涉及公司机密的计算机设备的安装、调试、检修，应由内部专业技术人员负责，其他人员不得随意拆卸和检修

人员管理

- **涉密会议管理**
  凡是涉密会议，组织部门需严格确定出席、列席会议人员，为线上会议设置会议密码和加密链接，审核与会人员
- **权限访问条款**
  为公司提供各类产品或服务，需要对公司信息资产进行物理或逻辑访问的相关方，均须签订保密协议或保密条款
- **隐私保护培训**
  要求员工完成隐私保护相关的培训和考核

资产管理

- **涉密资料管理**
  涉及人员应妥善保管因公所获得的秘密资料，个人不得将其带至家里或任何公共场所，不得对外泄密
- **涉密资料存储**
  涉密文件、记录、磁盘、光盘或其它存储媒体应存放在上锁的文件柜、保险柜或其他形式的保险家具中，指定专人保管钥匙

案例 | 立讯精密搭建网络安全态势感知平台

公司部署覆盖硬件基础设施和系统的网络安全态势感知平台，通过全域实时安全数据采集与多维度分析，动态监测潜在攻击威胁、资产暴露风险及系统脆弱性，并结合自动化闭环应急响应机制，构建起跨厂区的协同防御体系。

2024 年，我们进一步优化告警规则与安全事件检测分析，安全告警误报率降低，告警量与安全事件数量减少超过 60%。同时，我们修复漏洞 50 余项，全面提升信息安全保障能力。

网络安全态势感知平台

报告期内，立讯精密：

未发生

经证实的涉及侵犯客户隐私，丢失或泄露客户资料的投诉