



政策 08 · KRB-POL-08

保密与信息安全政策



文件名称 保密与信息安全政策	文件编号 KRB-POL-08	发布日期 03.03.2025
修订号 / 修订日期 1 / 11.08.2026	编制 法务与合规部	批准 董事会

8.1 目的

本政策旨在确定保护 Karub Enerji 所拥有或受第三方委托保管的机密信息、商业秘密、知识产权资产和个人数据的原则、规则和职责，并保障信息的保密性、完整性和可用性。

作为研发密集型科技企业，电池片和组件生产配方、工艺参数、测试数据、设计文件和客户信息等信息是 Karub Enerji 最宝贵的资产之一。

8.2 适用范围

本政策涵盖公司拥有或控制的所有信息（无论其载体为纸质、电子、口头或视觉形式），以及有权访问此类信息的全体员工、管理人员、实习生、顾问、供应商和业务伙伴。相关义务在业务关系结束后继续有效。

8.3 依据

- 第6698号《个人数据保护法》及其配套法规以及个人数据保护委员会的决定
- 第6698号法第9条关于跨境传输的标准合同、约束性公司规则和明示同意机制
- 第5651号《互联网出版物管理法》
- 第6102号《土耳其商法典》第396条（竞业禁止）及关于不正当竞争的规定（第54条及以下）
- 第6098号《土耳其债法典》第396条（员工忠实义务）和第444-447条（竞业禁止）
- 第5237号《土耳其刑法典》第135-140条（涉及个人数据的犯罪）和第239条（泄露商业秘密信息）
- 第6769号《工业产权法》和第5846号《智力与艺术作品法》
- 欧盟《通用数据保护条例》（GDPR）——在适用范围内
- ISO/IEC 27001 信息安全管理体系标准

8.4 机密信息的定义与分级

机密信息是指未公开的、一旦披露可能损害公司、其员工、客户或业务伙伴利益的任何信息。特别包括：生产配方和工艺参数、技术图纸和设计、研发项目成果和测试结果、尚未申请专利的发明、成本和定价数据、报价和投标信息、客户和供应商名单、合同条款、财务数据和商业计划、员工人事和薪酬信息以及信息系统安全信息。

信息分为“公开”、“内部使用”、“机密”和“绝密”四个等级。针对每一等级分别确定访问、存储、传输、复制和销毁规则，并对文件进行相应标识。

8.5 基本保密义务

- ◆ 机密信息仅在工作所需范围内并依据“需知”（need-to-know）原则使用。
- ◆ 机密信息不得与未经授权的人员共享——包括公司内部其他员工。
- ◆ 与第三方共享信息必须以事先签署的书面保密协议（NDA）为依据。
- ◆ 机密信息不得复制到个人设备、个人电子邮件账户、未经批准的云服务或移动存储介质。
- ◆ 机密信息不得在社交媒体、会议、新闻发布或面向公众的人工智能工具中分享。
- ◆ 业务关系结束时，所有机密信息及其所有载体应归还公司；不得保留副本。
- ◆ 保密义务在劳动合同终止后无限期持续有效。
- ◆ 禁止通过非法途径从第三方获取和使用竞争对手信息。

8.6 个人数据保护

公司作为数据控制者，对其处理的个人数据遵守 KVKK 第4条规定的一般原则：合法与诚信；准确并在必要时保持更新；出于特定、明确和合法的目的处理；与目的相关、有限且适度；仅在法规规定或处理目的所需的期限内保存。

- ◆ 仅在符合 KVKK 第5条和第6条所列处理条件之一时处理个人数据。
- ◆ 在数据处理活动之前依据 KVKK 第10条告知数据主体；必要时取得明示同意并告知同意可以撤回。
- ◆ 编制并持续更新个人数据处理清单；在纳入范围的情况下履行 VERBIS 登记义务。
- ◆ 依据《个人数据保存与销毁政策》确定保存期限；期满后删除、销毁或匿名化处理数据。
- ◆ 与作为数据处理者提供服务的各方签订符合 KVKK 的数据处理协议。
- ◆ 跨境传输依据 KVKK 第9条，以充分性认定、适当保障措施（标准合同、约束性公司规则）或例外条款为基础进行，并履行向监管机构的通知义务。
- ◆ 数据主体的申请依据《向数据控制者申请程序与原则通告》在最迟三十日内处理完毕。
- ◆ 员工监控活动（摄像、日志记录、车辆追踪、电子邮件监控）仅出于合法目的、以适度方式并在事先告知员工的前提下进行。
- ◆ 公司网站的 Cookie 使用通过单独的《Cookie 政策》和 Cookie 管理工具透明管理；对非必要 Cookie 取得明示同意。

8.7 知识产权与工业产权保护

员工在履行工作职责过程中创造的发明、设计、软件和作品的权利，在法规和合同规定的框架内归公司所有。员工发明的申报和报酬流程依据《工业产权法》的规定办理。拟申请专利的技术方案在申请日之前绝不披露；对选择作为商业秘密保护的信息实施访问限制。尊重第三方知识产权；禁止使用未经授权的软件。

8.8 信息安全措施

- ◆ **技术措施：** 防火墙和网络分段、终端防护和恶意软件检测、磁盘和传输加密、多因素认证、权限和基于角色的访问管理、日志记录和监控、补丁和漏洞管理、定期备份和备份恢复测试。
- ◆ **管理措施：** 信息安全意识培训、钓鱼邮件演练、清洁桌面和清屏制度、保密承诺书、入职和离职权限流程、供应商安全评估。

- ◆ **物理措施：**生产区域、服务器机房和研发实验室的门禁卡管控、访客登记和陪同制度、关键区域视频监控、纸质文件使用带锁文件柜和碎纸机。
- ◆ 禁止在生产和实验室区域未经授权拍照和录像。
- ◆ 制定业务连续性和灾难恢复计划并定期测试。

8.9 事件管理

任何已发生或疑似的信息安全和数据泄露事件应立即报告信息技术部和法务/合规部。事件按照包括发现、遏制、根本原因分析、修复和报告各阶段的应急响应程序进行管理。发生个人数据泄露时，应尽快且在任何情况下于七十二小时内向个人数据保护委员会报告；在合理的最短时间内通知相关数据主体。保存事件记录，并采取措施防止类似事件再次发生。

8.10 处分、监控与生效

违反本政策可能导致直至以正当理由解除劳动合同的纪律处分、损害赔偿责任，以及就构成犯罪的行为承担刑事责任。第三方违规时适用合同处罚措施，并可终止合作关系。

本政策的有效性通过泄露事件数量和响应时间、意识培训完成率、钓鱼演练成功率、数据主体申请数量和响应时间以及审计发现进行监控。本政策每年至少审核一次，或在法规变更时立即审核，经董事会批准生效。

编制

法务与合规部

姓名 / 签字 / 日期

批准

董事会

姓名 / 签字 / 日期