赛力斯集团信息安全政策

赛力斯集团股份有限公司及其子公司(简称“赛力斯”或“公司”)，为贯彻落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规以及 ISO 27001、ISO27701 等国际标准，赛力斯制定了《赛力斯集团信息安全政策》（简称“本政策”）。

1. 适用范围

本政策由董事会审批通过，适用于赛力斯集团股份有限公司及其下属所有子公司，覆盖范围包含赛力斯自有运营、供应商及合作伙伴。董事会作为信息安全与隐私保护相关事宜的最高监督机构，负责监督并定期检讨本准则的落实情况。

2. 原则

公司严格遵守《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规以及 ISO 27001、ISO 27701 等国际标准，建立完善的信息安全与隐私保护体系。

3. 信息安全管理举措

3.1 信息安全体系持续改进

- 持续跟踪法律法规以及 ISO 27001:2022 等体系标准最新要求，并结合实际业务场景运行变化，全面审视已发布信息安全相关体系，以 PDCA 持续改进的机制，不断改进提升信息安全管理水平、补齐安全短板。

3.2 数据合规保护

- 严格遵循职责分离与最小化授权原则，确保仅经过授权员工可访问重要敏感数据，从源头上降低数据泄露风险和保护数据完整性，并通过签署《保密协议》与《网络与数据安全承诺书》，明确界定员工在数据保密、合规使用及安全防范方面的法律责任与义务。

- 明确数据生命周期的安全要求，并通过数据监测系统，监控数据保护措施落实情况，及时发现安全问题和应对潜在的安全威胁，持续提升数据合规保护水位。

3.3 员工信息安全个人责任

- 明确全体员工的信息安全个人责任，将信息安全行为规范纳入员工培训体系，面向全体员工开展网络安全与数据保护宣传、互动答题等系列活动。
- 依托内部办公平台常态化推送安全小贴士与洞察资讯，通过线上学习平台投放数据安全知识、技能培训及隐私保护等相关资源。

3.4 第三方信息安全要求

- 从网络安全、数据安全、隐私保护等安全视角，明确供应商等第三方合作伙伴安全责任边界与管控要求。
- 在合作准入阶段，要求合作的第三方公司必须签署网络与数据安全要求协议。
- 在合作期间，通过明确供应商提供产品与服务的安全要求和标准，落实供应商网络与数据安全责任义务。
- 在项目验收及评价环节，融入网络与数据安全评价项，并定期开展信息安全评价工作，持续加强信息安全与数据保护力度。

3.5 信息安全风险监测与应急处置

- 通过体系审核、专项审计、例行检查等方式，开展信息安全审计工作，并针对审计过程中发现的各类问题，明确整改要求、时限与责任主体，推动问题迅速整改落地。
- 建立漏洞扫描与渗透测试机制，及时识别并修复安全隐患，专门成立赛力斯网络安全应急响应中心(SERES SRC)。
- 制定信息安全应急响应体系，明确网络安全事件分类与分级标准，界定安全应急事件响应与处置流程，进一步提升风险响应效率。
- 将信息安全相关业务连续性计划纳入集团整体业务连续性管理与危机管理框架中，定期开展信息安全应急及数据备份恢复演练，检验预案有效性与人员熟练度，形成整改与更新闭环。

4. 隐私保护管理举措

4.1 隐私保护纳入集团风险与合规管理体系

- 将隐私保护纳入集团整体风险管控与合规管理体系，融入业务流程设计、制度建设、风险排查等各个环节，及时发现并整改隐私保护合规隐患，实行全体系化运作。

4.2 保障用户权益

- 以合法正当且最小必要为原则，且仅在提供产品或服务所必需范围内收集用户个人信息。
- 在收集用户个人信息前，明确告知信息主体收集目的、方式和范围，以及查询、更正、删除个人信息的渠道，注销账户、撤回同意的方法，并保障用户依法享有个人信息访问、更正、删除及授权范围调整等合法权益，且在用户同意后收集和使用信息。
- 在法律规定范围内的期限及达成目的所需的期限内保留用户个人信息，超出上述期限后，将删除用户个人信息或将个人信息进行匿名化处理。

4.3 用户信息保护机制

- 持续推动 SDLC 机制与 Privacy by Design 理念，将用户隐私保护融入业务与产品中。
- 严格遵循职责分离与最小化授权原则，保障仅经过授权员工可访问重要敏感数据，从源头上降低数据泄露风险。
- 通过签署《保密协议》与《网络与数据安全承诺书》，明确界定员工在数据保密、合规使用及安全防范方面的法律责任与义务，并针对重要敏感数据实施脱敏与加密处理，保障数据在传输、存储及使用环节安全性。
- 建立安全奖惩机制，针对安全违规行为依规实施惩戒，强化员工安全合规自觉性。
- 制定并演练网络与数据安全事件应急响应计划，在发生潜在或实际数据泄露时，实现快速和有序应对，最大限度控制影响。

4.4 违规零容忍及纪律处分

- 实行用户隐私违规零容忍机制，明确违规行为的界定标准，制定严厉的纪律处分措施。针对员工用户隐私违规行为，根据情节轻重给予通报批评、绩效扣分、降职、解除劳动合同等处分，如涉嫌违法将移交司法机关处理。针对第三方用户隐私违规行为，根据合作协议约定追

究违约责任，若情节严重将终止合作并追究相关法律责任。

4.5 实施监督与持续改进

- 定期开展政策合规内部审视，持续提升隐私保护合规管理水平，保障政策适用性和有效性。
- 定期开展个人信息保护检查与专项审计，及时识别潜在安全风险与违规操作，并依据国家法规监管要求定期组织开展个人信息保护合规专项审计，评估内部个人数据处理活动合规性，持续优化合规管理体系。