波司登
BOSIDENG
Bosideng International Holdings Limited
波司登國際控股有限公司
(於開曼群島註冊成立之有限責任公司)
(股份代號：3998)

信息安全政策

1. 适用范围

1.1 本隐私政策（「本政策」）适用于波司登国际控股有限公司（「本公司」）及其附属公司（统称「本集团」）。本政策延伸至所有供应商、承包商及第三方合作伙伴，其接触集团信息系统或数据时需签订等效安全协议。

2. 概述

2.1 本集团严格承诺遵守《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》、《中华人民共和国密码法》等适用的国家法律法规、监管规定及相关行业标准（包括但不限于网络安全等级保护、关键信息基础设施安全保护等要求），以及我们开展业务所在国家/地区适用的其他法律法规（如欧盟《通用数据保护条例》（GDPR）、美国相关州隐私法案等，如适用）。

2.2 集团亦遵循信息安全管理体系标准GB/T 22080-2016与ISO/IEC 27001的相关要求，建立覆盖全业务流程的信息安全管理体系。同时建立全域适用，覆盖所有运营环节（含供应商管理）隐私保护体系，实施零容忍违规惩戒机制，并通过内部及第三方年度审计验证合规性。

2.3 本集团致力于通过清晰定义信息安全组织架构、岗位职责和管控流程，有效启动并统筹管理全组织范围内的信息安全活动。通过体系的持续有效运行和动态改进，我们旨在构建并实践一套系统的、动态的、制度化的、全员参与的、以预防为核心的信息安全管理方法，持续保障公司及所有利益相关方信息的机密性、完整性和可用性。

3. 信息安全管理

3.1 信息安全管理方针

3.1.1 提高信息安全意识：信息安全管理的关键要素在于人，集团信息安全的首要任务是提高全员的信息安全意识。通过培训、宣贯、教育、明确职责，将信息安全的工作落实到每一个人；

3.1.2 落实信息安全控制：信息安全管理的方法在于控制，集团信息安全工作就是将各项安全控制措施落到实处，明确分工，落实技术控制措施，做到有流程、有规范、有工具、有检查、有改进；

3.1.3 降低信息安全风险：信息安全的目标在于降低风险，集团信息安全指导思想在于将信息安全事件损失控制到可接受的程度，建立与集团业务信息化发展相适应的信息安全控制能力；

3.1.4 保障业务连续稳定：信息安全保障的核心在于业务，集团信息安全围绕业务的要求，采取技术保障措施，确保在紧急情况下业务的连续稳定运行。

3.1.5 保障数据主体权利：建立隐私影响评估（PIA）机制，确保数据收集、处理符合数据最小化原则，赋予用户访问/删除个人数据的权利（响应时效≤72 小时）。

3.2 信息安全目标

3.2.1 保护信息资产机密性、完整性和可用性：防止敏感信息（包括客户数据、商业秘密、员工信息）的未授权泄露（内部或外部）、篡改和丢失；确保授权用户能及时可靠地访问所需信息。

3.2.2 提升威胁抵御与事件响应能力：构建强大的防御体系抵御外部攻击和入侵；建立高效的事件检测、响应和恢复机制，最大限度减少安全事件的影响和损失。

3.2.3 确保业务合规与隐私保护：严格遵守所有适用的信息安全与隐私保护法律法规及合同承诺；建立有效的控制措施防止违反法律法规和监管要求的操作。

3.2.4 管控特权与用户行为风险：实施严格的权限管理和最小特权原则；建立有效的监控与审计机制，及时发现和处置特权滥用及其他高风险用户行为。

3.3 信息安全组织

3.3.1 组织架构：集团信息安全组织架构由决策层、管理层、执行层共同组成。

3.3.2 职责划分

决策层：

- 审议并批准公司信息安全方针、战略规划及重大政策；
- 监督重大信息安全事件的处理过程，审议处置报告及改进措施；
- 审批信息安全管理体系建设与维护的关键资源投入（预算、人力等）。

管理层：

- 贯彻执行决策层决议，统筹协调全集团信息安全管理工作；
- 组织建立、实施、运行、监控、评审及持续改进信息安全管理体系（ISMS）；

- 主导信息安全风险评估、控制措施落实、事件响应协调及审计工作；
- 定期向决策层报告信息安全绩效、风险态势及体系运行情况；
- 监督集团隐私保护政策实施,审查隐私影响评估（PIA）报告，执行惩戒决定。

执行层：
- 各部门信息安全接口人：监控本部门隐私数据流向，配合信息安全工作小组管理层完成信息安全体系建设与日常运行工作
- 信息安全&信息技术团队：执行本部门的信息安全相关工作，包括但不限于担任集团隐私保护责任部门，统筹隐私政策实施，完成隐私内外部年审；安全事件应急响应与取证调查；安全技术体系标准落地与基线配置核查；为各部门提供专业安全技术支持与解决方案。
- 监察部门：信息安全及合规风险监察等。
- 其他部门各司其职，协同作战，确保信息安全体系高效运转.

3.3.3 组织间合作：公司与执法部门、管理部门、信息服务商和相关供应商等外部单位建立合作关系并进行有效沟通，保证在发生安全事件或隐私泄露事件时，能迅速采取行动和获得帮助。公司对能够接触公司敏感信息或信息系统的第三方（包括供应商、合作伙伴、服务商等）实施有效的安全管理，明确其安全责任和义务，并通过合同或协议进行约束。

4. 信息安全体系

4.1 管理体系建设：本集团借鉴 GB/T 22080-2016 与 ISO/IEC 27001 信息安全管理体系标准框架搭建覆盖全业务流程的信息安全管理体系。通过完善文件控制程序与记录管理制度，实现管理流程的标准化与可追溯性；每年组织全员分级分类安全培训，从基础安全意识教育到专业技术能力提升，再到岗位资质认证培训，全面提升人员安全素养；同时，在人力、物力、财力等方面给予充足资源保障，确保信息安全管理体系高效、稳定运行，形成安全体系的主体架构。

4.2 风险评估与处置：本集团严格遵循 GB/T 20984-2022《信息安全技术 信息安全风险评估方法》、ISO 31000:2018《风险管理指南》、ISO/IEC 29134:2023《隐私影响评估指南》，同时深度对标《网络安全等级保护制度》（等保 2.0）要求，将风险评估作为安全体系建设的首要环节，构建常态化风险评估机制。评估覆盖管理流程漏洞、技术架构缺陷及隐私合规缺陷三大维度，重点针对核心业务场景与高敏感数据处理活动（含客户隐私收集、跨境数据传输等）开展风险识别。完成评估后，依据风险等级制定包含处置策略、责任部门及完成时限的专项处置方案，同时循环持续监控风险状态，将风险控制在企业可承受阈值内，为信息安全体系建设奠定坚实基础。

4.3 绩效评估与优化：本集团制定涵盖事件响应时效、用户数据权利请求处理时效（≤72 小时）、隐私影响评估完成率等关键指标的量化评估体系。通过定期召开管理评审会议，结合“内部审计 + 第三方独立审计”的双重验证机制，运用数据分析深度剖析体系运行成效，精准识别薄弱环节。基于评审结论，动态调整安全策略与控制措

施，同时根据业务发展新需求、技术变化新趋势，推动安全体系与企业业务发展需求同步迭代升级，确保信息安全体系在持续优化中不断适应内外部环境变化，始终保持有效性与先进性。

5. 联系方式

5.1 如需咨询信息安全&隐私政策相关事宜，可通过邮箱 ：IS@bosideng.com 联系本集团信息安全部门。

6. 跟踪关注与信息披露

6.1 本集团将根据实际情况，持续完善、更新及改进信息安全政策与措施，确保各利益相关方权益。

7. 传阅与修订

7.1 本集团保留随时修订、更改或废止本政策的权利。本集团将定期审阅本政策，并在必要时予以修订。本政策的最新版本于本公司官方网站(http://company.bosideng.com)进行披露。

（如本政策的英文及中文版本有任何不一致，概以中文版本为准。）