网络安全与隐私保护政策

目 录

世纪互联集团股份有限公司（以下简称“世纪互联”或“集团”或“我们”）秉持“专业、创新、高效、安全”的管理理念，认真落实网络安全要求，恪守数据合规使用规范，筑牢用户隐私保护屏障。我们期待与所有相关方携手合作，共同应对网络安全与隐私保护的挑战，守护每一位用户的权益，推动企业与社会的可持续发展。

1 适用范围

本政策适用于集团及其子公司和所有附属机构。同时，我们鼓励商业伙伴、供应商、客户等，在与世纪互联开展合作时共同参照本政策承诺，提升网络安全与隐私保护能力。

2 网络安全与隐私保护治理

世纪互联建立了完善的网络安全与隐私保护治理架构，推动网络安全与隐私保护的监督和执行工作。董事会授权董事会审计委员会履行网络安全风险的监督职能，管理层接受董事会审计委员会监督，定期向其报告有关网络安全的事项。集团的网络安全计划由首席信息安全官（CISO）领导，同时，我们成立网络及信息系统安全领导小组，设置网络及信息系统安全工作组，负责网络安全与隐私保护工作的统筹协调。

3 网络安全与隐私保护承诺

我们深知网络安全和隐私保护的重要性，始终致力于守护用户隐私，并保障网络安全、稳定、高效可用。依据集团安全方针和目标、基于可适用的法律法规要求，我们承诺：

- 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》等可适用的法律法规及相关政策要求，落实网

络安全等级保护制度，采取符合业界标准、合理可行的防护措施以保护用户信息及网络数据、防止用户隐私安全和网络安全事件发生。

- 将网络安全与隐私保护视为集团合规管理及风险管理的重要组成部分，定期进行网络安全、隐私保护等合规性审核，开展内外部安全审计，持续投入以推进网络安全体系建设，提升网络及数据安全管理水平。
- 定期开展风险评估和安全检测，识别、处置合规与信息安全风险，推动管理性、技术性保护措施更新，以适应不断变化的威胁环境，有效应对新风险、新问题。
- 规范体系化管理，落实技术防护措施，保障信息的保密性、完整性、可用性。建立、维护并持续优化各项管理体系的有效运行，如信息安全管理体系（ISO/IEC 27001）、业务连续性管理体系（ISO 22301）等。
- 建立突发事件应急机制，提升应急管理能力和快速响应能力。
- 根据《员工手册》《信息安全管理要求》等管理文件，规范员工行为，提升安全意识，持续检查制度执行情况，及时发现和整改执行偏差，推动形成闭环管理机制，使安全日常化、常态化。
- 设立激励机制，表彰嘉奖在网络安全与隐私保护工作中做出突出贡献的团体和个人。同时，对于员工泄露隐私信息、破坏网络安全等行为采取“零容忍”态度；对迟报、谎报、瞒报和漏报安全事件或者存在其他失职、渎职行为的有关责任人，给予相应的处分或惩罚。
- 建立内部员工报告机制，员工可通过内部通讯软件、邮件、电话等渠道，举报和反馈信息安全事件、漏洞、可疑内容，由专职部门审核和处置上报内容和来源。
- 持续提升员工对网络安全与隐私保护的意识和能力，结合不同岗位所面临的差异性数据安全风险，提供针对性培训。
- 制定《供应商行为守则》，规范供应商遵守各自业务经营地所在国家、地区适用的网络安全及隐私保护相关的法律法规，并要求供应商适时接受世纪互

联对于网络安全或隐私保护相关的培训。我们与确认合作的供应商签订包括《保密协议》在内的相关法律文件，明确信息与隐私的保密义务。必要时，面向适用类别供应商开展信息安全专项评估，全面审视其在网络安全与隐私保护方面的表现及能力。

- 高度重视保护员工、用户和其他相关信息主体的个人信息，持续优化隐私保护措施进行个人信息的收集、存储、使用、传输、提供、删除等处理。有关于用户隐私保护的相关内容，请详见《隐私声明》。

4 附则

本政策的发布和实施由董事会审阅并批准，集团将定期审阅本政策，并在必要时予以审查和修订。

未尽事宜依照相关法律法规及相应证券交易所发布的规定与指引执行，世纪互联保留对本政策相关文本的解释权。