移动安全联盟漏洞信息披露和处置自律公约

第一章 总则

第一条 遵照“趋利避害、有效管理、积极引导”的基本方针，为维护用户个人信息安全和合法权益，保障网络与信息安全，促进行业健康发展，进一步规范国内外相关厂商、检测机构在漏洞信息发布和处置方面的行为，根据《中华人民共和国网络安全法》等法律法规有关规定，制定本公约。

第二条 本公约所称移动终端安全漏洞（以下简称漏洞）是指移动终端在硬件、软件、通信协议的设计与实现过程中或在系统安全策略上存在的缺陷和不足；非法用户可利用安全漏洞获得移动终端的额外权限，在未经授权的情况下访问或提高其访问权，破坏系统，危害信息系统安全。

第三条 本公约所称相关厂商主要指软硬件产品生产厂商、互联网服务提供商。检测机构指从事移动终端安全检测相关业务的实验室或安全公司。

第四条 倡议国内外相关厂商和检测机构加入本公约，从维护国家、行业和用户利益的高度出发，积极加强自律，共同营造良好的网络安全环境。

第五条 移动安全联盟负责监督本公约的实施。移动安全联盟作为本公约的执行机构，负责组织实施本公约。

第二章 自律条款

第六条 自觉遵守我国有关互联网管理的法律、法规和政策，自觉维护国家、行业和互联网用户的网络安全合法权益。

第七条 相关厂商和检测机构应协同一致做好漏洞信息的发布、处置等环节工作，做好漏洞信息披露和处置风险管理，避免因漏洞信息披露不当和处置不及时而危害到国家安全、社会安全、企业安全和用户安全。

第八条 各方在漏洞信息披露方面应遵循的原则：

客观披露原则。对公开发布的漏洞信息要进行披露审核，确保漏洞信息的真实性和完整性，漏洞信息涉及的目标对象、风险情况描述不出现重大偏差；对漏洞可

导致的潜在风险不能作为安全攻击事件进行披露和引导，以免引起媒体舆论和社会公众的误读和恐慌。

适时披露原则。在相关方未接收到漏洞信息、完成漏洞处置前或预定时限前不应提前公开发布漏洞相关信息。针对不同类型漏洞的修复规律和所需周期，各方研判后协商拟定灵活实际的漏洞公开披露时间。

适度披露原则。不得披露国家政策法规和主管部门禁止披露的漏洞，不得披露违反知识产权保护法律法规及商业机密协定的信息，不得制作和发布利用产品漏洞的方法、程序和工具。在漏洞处置完成前，对可通过公开信息（标题、描述等）猜解到具体目标系统、攻击手法的信息进行弱化处理，避免相关漏洞被黑客利用实施网络攻击。

第九条 相关厂商在漏洞处置方面应遵循的自律义务：

漏洞修复和防范。高度重视软硬件产品漏洞可能对用户可能造成的危害，积极回应漏洞平台以及漏洞报送者提供的漏洞信息，及时核实确认并提供和发布漏洞补丁或解决方案。对于需要用户采取漏洞修补或防范措施，并且可以向社会或用户公开发布的，应当及时将漏洞风险及修补或防范措施向社会发布或通过客服等方式告知所有可能受影响的用户，并提供必要的技术支持。

应从产品研发、测试和发布等环节加强协同管理，及时应对新出现的漏洞，在产品升级更新方面做好技术准备和主动服务，确保漏洞修复措施的有效性和覆盖面。

漏洞应急响应。建立快速应急响应机制，通过网站、邮件等方式及时披露和推送本单位生产、提供的软硬件产品的漏洞描述信息或预警信息，并同时向主管部门报备，以保障产品用户和系统用户的知情权和安全利益。

第十条 相关单位和从业者应共同防范和抵制漏洞信息的不当传播，积极举报和反对通过黑客地下产业购买、交易漏洞的行为，反对非法侵入或破坏他人信息系统。

第三章 公约执行

第十一条 移动安全联盟负责组织实施本公约，负责向公约签署单位传递互联网安全管理的法规、政策及行业自律情况，及时向政府主管部门反映，组织实施相关自律工作，并对签署单位遵守本公约的情况进行督促检查。

第十二条 公约签署单位之间发生争议时，应从维护国家、行业和用户利益出发，本着协商原则解决争议，也可以请求公约执行机构进行调解。

第十三条 公约签署单位接受社会和签署单位的监督，对违反本公约的，任何其他单位和个人均有权向公约执行机构进行检举，请求公约执行机构进行调查；公约执行机构也可以直接进行调查，并将调查结果公布。

第十四条 公约成员单位违反本公约，造成不良影响，经查证属实的，由公约执行机构视不同情况给予在内部通报或取消公约签署单位资格的处理。

第十五条 本公约所有签署单位均有权对公约执行机构执行本公约的合法性和公正性进行监督，有权向执行机构的主管部门检举公约执行机构或其他工作人员违反本公约的行为。

第四章 附则

第十六条 本公约经公约发起单位法定代表人或其委托的代表签字并加盖公章后生效，并在生效后的 30 日内由移动安全联盟向社会公布。

第十七条 本公约生效期间，由公约执行机构发起动议，本公约三分之二以上成员单位同意，可以对本公约进行修订。

第十八条 本公约内容与国家有关政策法规和政府主管部门规定不一致的，从其规定。

第十九条 相关单位接受本公约的自律规则，均可以申请加入本公约；本公约成员单位也可以退出本公约，并通知公约执行机构；公约执行机构定期公布加入及退出本公约的单位名单。

第二十条 本公约由移动安全联盟负责解释。

第二十一条 本公约自公布之日起施行。