泰康人寿保险有限责任公司

消费者安全保障措施

一、安全管理框架

泰康人寿保险有限责任公司（以下简称“公司”）依据《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》等国家法律法规，结合国家主管部门的监管要求和实际业务需求，建立并不断完善公司信息安全管理体系建设。公司以 ISO 27001 信息安全管理体系框架标准为依托，并先后通过 CMMI 3（开发体系）、TMMI 3 级（测试体系）、ISO 20000（运维体系）、ISO 27001（信息安全管理体系）等国际权威认证，同时泰康保险集团（以下简称“集团公司”）数据中心先后通过 CSA-Star 云安全体系、Uptime M&O（数据中心运维体系）等国际标准认证，并每年接受第三方机构的监督检查，表明公司在保险业务应用及 IT 服务运营，特别是保障信息系统安全、客户数据安全方面，达到了国际先进水平。

公司重要信息系统均按照国家及行业监管要求向公安机关进行了网络安全等级保护备案，并按照等级保护要求每年聘请公安部信息安全等级保护评估中心、信息产业信息安全测评中心等国家权威测评机构进行等级保护测评，确保持续符合相关标准要求，为用户提供专业的、安全的、高效的信息技术支持与服务。

二、安全管理组织

为加强信息安全工作统筹协调，提升公司信息安全管理水平，有

效防范信息安全风险，确保公司长治久安，经公司研究决定，成立泰康人寿保险有限责任公司信息安全工作委员会（以下简称“委员会”），委员会设立信息安全领导组和信息安全执行组，信息安全领导组是公司信息安全管理的最高领导机构，负责公司经营管理中与信息安全工作相关的顶层设计、总体布局、统筹协调、整体推进和督促落实；信息安全执行组根据领导组要求，制定信息安全目标，建设信息安全体系，统筹、协调、监督信息安全重点项目，落实信息安全相关工作，控制信息安全风险。

三、具体安全措施

公司使用符合业界标准的安全防护措施保护客户的个人信息、交易信息和交易的安全，防止数据遭到未经授权的访问、损坏或丢失。具体安全措施如下：

（一）网络安全检测和监控

公司自主培养了专业渗透测试人员，配置了专业漏洞检测设备，针对公司官方网站和重要信息系统进行安全检测，对发现的安全漏洞及时更新。公司与多家安全厂商及科研院所建立合作关系，委托供应商在互联网进行安全检测。

公司在基础网络建设中部署了多层次、不同类型的网络安全检测系统，包括最外层的流量攻击检测设备、入侵防护系统、网络应用攻击检测系统等专业安全设备，还部署了多种基于应用系统、终端、网络层的安全监测与防护系统。建立了快速、高效网络安全应急响应机制，确保对系统、机制层面可能存在的问题，早发现、早解决，避免对信息系统的数据安全造成影响。

（二）重要数据保护

公司制定了《泰康人寿保险有限责任公司数据安全管理办法》、《泰康人寿保险有限责任公司客户信息安全技术管理规范》，明确了重要业务数据、生产数据、用户信息及涉及对公司运营过程中涉及到各类数据的安全管理细则与具体要求。

运维层面，公司严格限制运维人员直接访问生产系统及数据，所有操作行为均要通过运维审计平台，做到可记录、可追溯、可审计；依托行业领先的数据库脱敏平台，避免敏感信息意外泄露；应用层面，公司实行应用系统权限分级管理，特权账号定期审核等手段，加强数据处理全流程的数据安全保护；终端层面，逐步在公司范围内部署终端数据防泄漏系统，在 Web、邮件和终端通道上对敏感数据的外发进行管控。

（三）数据备份恢复

在加强数据可用性及完整性层面，公司业务数据采用了整体备份与增量备份相结合的方式，根据既定的规定和备份计划执行数据备份。针对重要的业务数据，采用了同城及异地数据级备份的方式。公司定期进行备份数据进行回装测试，确保备份数据的可用性。