

关于互联网保险业务中消费者信息安全的保障措施

我公司根据银行等支付机构支持的满足互联网支付需求的支付产品为客户提供安全高效的支付服务。我公司已建立相应数据安全管理制度和统计管理制度，具体是围绕信息系统保障建立了包含总体安全策略、终端安全管理、信息系统开发安全、用户认证、数据安全、信息系统运行安全、网络安全、物理安全、灾备与应急等九类 33 项制度。其中《新华人寿保险股份有限公司信息安全管理规定》为信息系统保障总体安全策略，并分章节明确了各方面安全保障要求。《新华人寿保险股份有限公司信息系统电子数据管理规范（试行）》，规范了我公司信息系统中的电子数据的数据安全、数据标准、数据质量、数据使用、数据存储和备份。

我公司始终重视数据安全工作，一方面通过数据防泄漏系统，实现对关键数据流向的风险管理和日常可视化监控，有效保护我公司客户数据等重要文件的数据安全，提高员工对于处理机密数据的安全意识。另一方面利用数据库审计和分析工具，监控我公司数据库调用的安全合规，提升我公司数据安全防护水平，降低了我公司敏感信息应用安全风险。2021 年度我公司将启用敏感数据发现功能，实现对敏感信息文档的实时水印和加密管理，同时将对敏感数据的对外邮件发送启用邮件审批策略。以上策略的实施将大幅提高我公司

的数据安全管理能力，降低数据泄露风险。

我公司每年例行进行网络安全检查，对发现的安全漏洞转交相关系统责任人进行整改，截至目前已发现的安全漏洞已基本修复。对于各互联网众测平台所发现的应用系统漏洞，我公司第一时间响应，均在短时间内进行了修复。2016年起我公司每年开展众测服务项目，通过与众测平台签订合同，加强我公司外网漏洞发现的及时性。

我公司已基本形成了安全态势的主动监测，安全威胁的自动通知功能体系，搭建了安全管理平台，该平台采用智能分析引擎，破除数据孤岛，发现未知威胁和潜在威胁，有效弥补不同类型的安全设备在安全防护上的局限性，互相印证。基于收集的数据建立了“账号暴力破解”、“WEB 攻击扫描”、“核心账号异常登录”等安全模型 300 余个，实现安全运行状态的实时分析，实时展示，实时告警，能够及时发现安全事件，并自动通知相关责任人，提升事件发现、响应效率。该平台的建立，也满足了《网络安全法》、《等级保护基本要求》以及行业监管相关要求。

我公司通过网络监控系统对全网设备进行监控，并发送异常状态告警。告警主要分为三个等级重大告警、紧急告警和一般告警，各级告警响应时效分别不得超过 1 分钟、5 分钟、10 分钟。在网络硬件和漏洞修复方面，我公司通过定期巡检，与网络设备厂商核实版本信息，及时发现安全漏洞和

隐患，对发现的安全漏洞和隐患，通过升级软件版本及时进行修补，同时定期对全网设备进行巡检，并对网络设备进行安全评测。

我公司数据中心安排 7*24*365 值班人员，重点监控我公司重要信息系统及服务设备运行情况。按照“早发现、早报告、早处置”的原则，加强每日安全监测，对各类突发事件和可能引起突发事件的信息进行收集、分析、判断和持续监测，并形成每日监测书面材料。