东方财富信息股份有限公司数据安全与用户隐私保护声明

作为中国专业的互联网财富管理综合运营商，东方财富信息股份有限公司（以下简称“公司”或“东方财富”）为用户提供基于互联网的财经资讯、数据服务。数据安全及用户隐私保护是我们重点关注的议题，是公司信息治理的重中之重。公司特制定本声明，承诺严格落实数据安全及用户隐私保护，切实保障用户权益。

本声明适用于东方财富及控股子公司的所有业务条线。

一、建立健全管理体系

公司基于 ISO27001、ISO20000 及 ISO9001 认证建立并完善了信息安全管理体系、信息技术服务管理体系及质量管理体系，形成了组织架构人员及职能明确、制度清晰的管理体系，涵盖数据安全与用户隐私保护管理内容。

为全面贯彻落实数据安全与用户隐私保护相关要求，在公司董事会领导下，公司搭建网络信息与数据安全组织架构，由网络信息与数据安全领导小组、工作小组及执行小组组成。网络信息与数据安全领导小组由公司总经理任组长，负责对公司网络信息与数据安全工作相关的方针政策、重大事项进行决策；网络信息与数据安全工作小组负责监督安全开发工作进度、信息资产识别和数据分类分级工作进度等，并下设执行小组，将公司网络信息与数据安全工作充分落实到每一个职责岗位。

公司严格遵守国家相关法律法规，制定了《东方财富数据分类分级规范（试行）》《东方财富数据生命周期安全管理规范》《东方财富数据开放共享管理办法》《东方财富隐私保护指引》等指导性规范文件，适用于公司各部门及各分支机构，覆盖所有业务条线，各子公司结合自身监管要求参照制定并执行适用于自身的制度。

二、加强数据安全建设

公司积极落实公司数据安全及隐私保护管理规范，通过强化主动管理及提升被动应对，做好数据安全风险防范与应急管理工作，防范数据泄露等安全事件发生，减少突发事件造成的损失。此外，公司积极开展信息安全认证和审计工作，定期进行内部审计，同时委托外部专业机构进行外部审计，并持续开展全员数据安全培训，严格规范供应链数据安全管控措施，以切实加强数据安全建设。

（一）落实数据泄露风险管理

为加强数据泄露风险管理，公司采用主动管理、被动应对等措施防范数据泄露风险。公司成立至今，在数据安全及用户隐私保护方面未发生负面事件。

强化主动管理：

- 公司搭建内部数据管理平台，根据《东方财富数据分类分级规范（试行）》相关要求，对数据进行分类分级管理，对敏感数据进行加密管控，如对手机、身份证等信息采取落地加密的保护措施；
- 公司制定了《东方财富数据开放共享管理办法》，根据最小权限原则进行权限赋予和管控实施，所有授权均通过系统实现，并通过身份验证等方式加强系统访问控制；
- 公司全面贯彻落实《个人信息保护法》相关要求，依托安全管理部全盘总管用户隐私政策，制定了隐私政策，并根据提供服务及功能的变化适时对隐私政策进行更新，包括功能更新、权限调整等。隐私政策的更新及发布需经业务部门、法务部门、安全管理部共同审核；
- 公司积极响应国家号召，配合监管部门开展重点节日活动安全保障、数据安全风险评估、APP 个人隐私检查等工作；
- 公司通过定期和不定期的方式进行漏洞扫描和渗透测试，增强网络安全管理；
- 此外，子公司东方财富证券根据《证券期货经营机构信息系统备份能力标准》制定系统备份机制，确保数据安全性与可用性。

提升被动应对：

- 公司每年编制应急预案，内容涵盖信息系统故障、自然灾害等场景，并根据应急预案组织开展应急演练，总结演练结果并不断完善响应流程及机制，提升安全事件应对能力。

（二）开展信息安全认证和审计

基于完善的网络信息与数据安全管理架构以及管理制度，公司建立起健全的网络信息与数据安全管理体系，现管理体系已经通过国际信息安全标准 ISO27001、ISO20000 及 ISO9001 质量管理体系认证，纳入认证范围内的业务营业收入占公司合并范围内营业总收入 90%以上。

为加强隐私和数据安全控制，公司定期针对信息安全和隐私保护相关内容开展内外部审计。

开展信息安全外部审计：

- 根据国家等级保护要求，公司邀请外部机构定期对总部和下属子公司重要信息系统进行等级保护测评，三级系统每年一次，二级系统每两年一次。
- 依据 ISO 的审核规则，公司每年邀请外部机构对公司和主要子公司开展 ISO27001、ISO20000、ISO9001 的审计测评，评估相关管理体系的有效性。

开展信息安全内部审计：

- 公司每年进行内部审计，审计对象包括隐私保护指引及系统权限，以保障隐私和数据安全。每年至少一次评估当前隐私保护指引是否与实际情况一致，判断是否需进行修订，修订后的隐私保护指引均公开发布。每年对系统权限进行审计，评估系统权限赋予是否恰当，及时清理不必要权限。

（三）提升全员数据安全意识

公司通过组织数据安全意识培训、将数据安全与员工绩效考核挂钩、开展数据安全宣导活动等方式提升员工数据安全意识。

组织数据安全意识培训：公司通过线上线下培训的方式，每年组织开展覆盖全体员工的信息安全意识培训，培训内容涵盖用户信息安全保护、数据生命周期管理与保护等内容，培训方式包括针对公司全体员工的安全意识类培训（如信息安全意识宣讲、新员工培训等）及针对特定部门的专项培训（如针对人力资源部门、客服部门等与外部用户直接接触的部门培训、针对信息技术部门的培训等）。2022 年公司开展信息安全意识宣讲共计 15 场，要求全员参加，培训后考核合格率超 99%。

将数据安全与员工绩效考核挂钩：将员工信息安全意识培训列入公司员工绩效考核范畴，做好员工考核配套机制建设，建立信息安全违规事件处罚条例，将用户信息保护工作纳入条例范围，严格杜绝员工信息泄露行为。

开展数据安全宣导活动：公司每月通过安全宣传栏发布数据安全、用户隐私保护等相关内容宣导。公司组织开展了“反电信诈骗”百万赏金计划，旨在打击电信诈骗、保障用户信息和财产安全、净化信息网络环境。此外，公司积极响应国家网络安全宣传周要求，每年举办网络信息安全宣传周活动，制作并投放宣传物料，设计趣味游戏以提高员工参与度，提升员工安全意识。

（四）做好供应链数据安全管控

明确供应商数据安全管理要求：公司与全体供应商及合作伙伴签订合作协议，在协议中或通过补充协议的方式明确双方的权利及义务，要求全体供应商及合作伙伴遵守公司的数据保护政策或制定其自身的数据保护政策，确保数据安全。公司严禁供应商参与涉及重要及以上商业机密的数据管理。

追踪供应商数据安全管理落实情况：公司每年对供应商进行年度质量考核，评估项目执行情况及服务履行情况。公司要求供应商提交数据保障能力尽职材料，信息技术相关专人对上述材料进行存档管理。对于发现违规存储或使用公司经营和用户数据的供应商，责令其立即销毁并整改；若其拒绝配合整改，公司立即停止合作，并采取措施维护自身及用户的合法权益。

三、严格保护用户隐私

东方财富全面落实《个人信息保护法》相关要求，建立《东方财富隐私保护指引》，并通过保障用户数据管理权益、做好用户数据收集与保存、强化敏感

数据访问控制、规范第三方用户数据共享、将隐私保护融入产品开发环节等方式，切实做到严格保护用户数据安全。

（一）保障用户数据管理权益

公司非常重视用户的隐私保护，在用户使用东方财富服务时，公司通过《东方财富隐私保护指引》告知用户我们如何收集、使用、存储和共享个人信息，以及如何访问、更新、控制和保护个人信息，并说明用户享有的权利。指引适用于小程序、移动客户端（“APP”）、PC 端、WEB 端及软件著作权为东方财富信息股份有限公司的产品，如股吧、财经股票头条。此外，为全面贯彻落实《个人信息保护法》及证券监管相关要求，针对公司涉及的证券和期货业务，制定并公开披露《东方财富证券隐私保护指引》《东方财富期货隐私保护指引》。

访问权、修改权、删除权详见如下《东方财富隐私保护指引》“第六条 您如何访问和管理自己的个人信息”的规定：

“1.管理您的信息

您可通过以下方式查阅您的身份信息、账户信息，或修改您的个人资料，或进行相关的隐私、安全设置：

1)登录通行证账户，在“设置-账号设置”中；

2)登录证券账户后，在“交易-交易功能-个人信息”中；

出于安全性和身份识别的考虑或根据法律法规的强制规定，您可能无法修改注册时提供的初始注册信息。

…

3.注销账户

当您符合约定的账户注销条件并使用注销功能后，您该账户内的所有信息将被清空，我们将不会再收集、使用或对外提供与该账户相关的个人信息，但您在使用相关账户期间提供或产生的信息我们仍需按照监管要求的时间进行保存，且在该保存的时间内依法配合有权机关的查询。

1)通行证账户注销：通过“我-设置-其他-更多用户设置-账户注销”这样的流程完成账户注销，具体可根据操作界面上提示操作。

2)证券账户注销：通过“交易-更多-业务办理-在线销户”这样的流程完成账户注销，具体可根据操作界面上提示操作。

通行证账户与证券账户没有关联，当您注销其中任意一个账户都不会影响另一个账户的使用。”

（二）做好用户数据收集与保存

公司在《东方财富隐私保护指引》中明确告知用户东方财富如何收集、使用、存储和共享用户个人信息。

在数据收集环节，公司依据合法、正当、必要的原则，基于使用场景对个人信息进行必要性采集，确保最低限度收集；数据采集时明确告知用户收集的

信息类型与用途及保护措施，并以协议确认、具体场景下的文案确认、弹窗提示确认等形式获得用户同意。详见《东方财富隐私保护指引》“一、我们如何收集信息”。

在数据保存环节，除法律法规相关要求外，在交易目的已实现、停止提供产品或服务、用户数据超出保存期限后，公司会在法律法规监管要求的基础上根据用户要求删除用户个人信息或进行匿名化处理。详见《东方财富隐私保护指引》“三、我们如何存储和保护信息”。

（三）强化敏感数据访问控制

公司始终严格保护用户数据，致力于使用各种安全技术及配套的管理体系来尽量降低用户的信息被泄露、毁损、误用、非授权访问、非授权披露和更改的风险，主要通过应用最小访问权限原则、身份验证和授权、采用加密/去标识技术、部署敏感数据监控系统等方式进行用户数据、敏感数据管理。

应用最小访问权限原则：公司对可能接触到用户信息的员工按照最小权限原则授予权限，且权限赋予前均需经过相应的授权审批，并通过定期审阅以及审计机制对权限授予的合理性进行复核。

身份验证和授权：在数据访问过程中，采用密码、口令等方式进行有权限员工的身份验证；

采用加密、去标识技术：《东方财富隐私保护指引》中明确，公司涉及的个人敏感信息包括个人财产信息（银行账户、鉴别信息、交易和消费记录、流水记录等，积分、积分兑换等虚拟财产信息）、个人生物识别信息（声纹、面部识别特征）、个人身份信息（有效身份证件的种类、号码、签发机关和有效期限）、网站浏览记录、个人位置信息。对于必须使用敏感数据的流程需采取措施确保敏感数据安全，公司要求敏感数据脱敏后或去标识化后进行提取，并制定了数据提取流程进行规范。公司采用安全加密算法对敏感数据进行加密存储与加密传输。

部署敏感数据监控系统：公司对员工处理用户信息的行为进行系统监控；此外，公司在机房关键数据位置部署了敏感数据监控系统，对敏感数据的流向和使用方进行记录并定期审计。

（四）规范第三方用户数据共享

公司不会出于完成交易/服务以外的目的向第三方机构租用、销售或共享个人数据。若涉及必要的数据共享，公司会提前向用户明确并获得用户同意，并会进行个人信息安全影响评估，对第三方个人信息安全防护能力水平提出要求。

（五）将隐私保护嵌入产品开发

在产品开发及设计阶段，按照标准安全规范实施开发，并对产品设计方案进行安全评估，如系统涉及敏感数据的传输和存储，则相应提高数据加密及审计要求。其中，安全规范包括 Web 安全规范、安全配置参考手册、员工信息安全手册、信息安全违规事件处罚条例、信息安全奖惩管理实施细则等。

在信息系统变更或上线前，对方案开展安全评审在内的各方面评审，包括

漏洞扫描及渗透测试，判断是否存在数据泄露风险，并将测试结果留痕记录。如系统涉及敏感数据的传输、存储、使用，则会在加密、审计方面有严格要求；在产品和服务上线前，安全团队会评估产品和服务是否公司隐私保护指引相一致，若存在不一致的情况，将及时更新隐私保护指引并通知用户，或要求产品及服务进行相应调整。