**xxx银行**

系统日志管理办法

**第一章 总 则**

第一条 为保障xxx银行（以下简称“本行”）的日常生产经营活动正常进行，保障本行生产系统日志（以下简称“系统日志”）安全、高效管理，根据银监会《商业银行信息科技风险管理指引》的要求，制定本办法。

第二条 本办法所称系统日志是指各类信息系统生产环境运行过程的运行情况记录信息，主要分为三类：

（一）设备运行日志：各类服务器、网络设备、安全设备的运行情况记录等；

（二）基础软件运行日志：各类操作系统、数据库、中间件的运行情况记录等；

（三）应用系统运行日志：各类业务、应用、信息及监控管理软件的运行情况记录等。

第三条 总行信息科技部为本行系统日志日常管理的职能部门，具体负责系统日志的记录设置、保存、备份、恢复、使用、分析处理等工作。

**第二章 系统日志记录设置**

第四条 根据“谁主管，谁负责”的原则，由总行信息科技部专业维护人员依据生产维护的具体需求对各自负责的软硬件进行日志记录规则的设置。

第五条 系统日志存放要统筹考虑信息保存的必要性与存储空间的合理使用。有追溯价值的信息要重点保存，不能遗漏；重要程度不高的信息可不进行记录，减少对存储空间的浪费。

第六条 应用系统运行日志的记录设置应当紧贴应用的使用情况，在系统开发阶段予以充分考虑。

第七条 承载各类应用系统、基础软件环境的设备应正确设置时区与时间，与网络时间服务器进行同步配置，保证系统日志记录时间戳的准确性。

**第三章 系统日志保存**

第八条 系统日志应当严格按照监管要求，结合行内业务使用的具体要求及相关技术规范，合理设置系统日志保存的位置与方式，妥善保存便于备查。

第九条 重要信息系统的运行日志应当保存在专业存储设备上，保证数据不丢失。其它日志一般采取设备本地保存方式。

**第四章 系统日志备份与恢复**

第十条 重要信息系统运行日志实行定期与不定期相结合的备份方式，由指定人员检查运行情况，并登记在案。

第十一条 系统重大变更前，应当对系统日志进行必要的备份，必要时进行系统级备份。

第十二条 根据日志的重要级别，确定备份日志的保存期限，应根据备份介质使用寿命至少每年进行一次恢复性测试。

第十三条 备份介质的存放处必须符合防火、防水、防磁、防盗的安全要求。

第十四条 重要系统的运行日志要定期异地备份。

**第五章 系统日志使用**

第十五条 备份日志的使用与恢复，必须通过相关审批流程后操作，需要使用备份日志时，使用部门应填写《备份日志使用申请表》，交由需求部门及信息科技部负责人审批后方可使用。

第十六条 本行信息安全人员应定期对各类安全设备的系统日志进行检查，分析各类安全事件，保证系统安全运行。

**第六章 系统日志的分析处理**

第十七条 借助集中统一的日志管理平台，实现多种网络设备、安全设备、主机设备以及其他应用系统的日志集中搜集、分析与展现，实现对整个网络平台和面向应用的事前管理、事中监控和事后分析。

第十八条 各类专业维护人员应当定期对系统日志进行检查与分析，排查系统运行的隐患，调整优化系统日志的记录设置策略。

第十九条 信息科技部应制定相应的备份日志审核计划，计划中应将日志按等级分类，保证按照优先级对备份日志审核。需要备份日志审核时，需求部门应填写《备份日志审核表》，由需求部门及信息科技部负责人审批。

**第七章 附 则**

第二十条 本办法由xxx银行信息科技部负责解释和修订。

第二十一条 本办法自发文之日起施行。

附件：1.日志使用申请表

2.备份日志审核表

附表 1

日志使用申请表

***申请日期：***

|  |  |  |
| --- | --- | --- |
| ***申请使用部门*** | ***申请使用人*** |  |
|  |  |  |

***申请事由***

|  |  |  |
| --- | --- | --- |
| ***申请部门意见*** | ***科技部门意见*** |  |
|  |  |  |

***附表 2***

备份日志审核表

**审核日期：**

申请审核部门 日志级别

数据来源

审核数据内容

|  |  |  |
| --- | --- | --- |
| 需求部门意见 | 科技部门意见 |  |
|  |  |  |