延边州金融机构信息安全报告制度

一、总则

第一条　为加强延边州金融业信息安全管理，规范信息安全事件管理，增强信息安全风险防范的主动性，根据《中华人民共和国计算机信息系统安全保护条例》和《国务院办公厅关于印发中国人民银行主要职责内设机构和人员编制规定》以及《中国人民银行计算机系统信息安全报告制度》、《吉林省金融机构信息安全报告制度》特制定本制度。

第二条　本制度适用于在延边州内依法设立的银行业、证券业和保险业金融机构。

第三条　本制度报告范畴为网络与信息系统的信息安全，报告事项包括信息安全事件和信息安全风险两类。

第四条　本制度所称信息安全事件，是指被识别的、意外的一种或一系列系统、服务或网络状态的发生，表明由于自然或者人为以及软硬件故障等原因，造成可能的信息安全策略违规或某些安全防护措施失效，这些状态的发生极有可能危害业务系统正常运行和威胁数据安全，从而对国家、社会造成负面影响。

第五条　本制度所称信息安全风险，是指人为或自然的威胁利用网络与信息系统及其管理体系中存在的脆弱性，并由此导致信息安全事件的发生以及对组织造成损害的可能性。

二、事件报告

第六条　信息安全事件按照信息系统的重要性以及其影响范围、持续时间和数据泄漏、丢失、破坏等产生的影响等因素分级，根据中国人民银行总行的具体要求，信息安全事件分为特别重大信息安全事件（I 级事件）、重大信息安全事件（II 级事件）、较大信息安全事件（III 级事件）。当信息安全事件满足多个级别定级条件时，按最高级别确定事件等级，具体分级见附件 1。

第七条　各金融机构发生各类信息安全事件后，应依据事件影响范围和影响时间变化，按照上述定义进行事件级别的升级。

第八条　中国人民银行延边州中心支行作为延边辖区金融业各分支机构信息安全工作的协调与管理的主管部门，承担辖区内金融机构信息安全事件与风险的报告、接报、汇总和协调处置工作，部门下设办公室，办公室为中国人民银行延边州中心支行科技处。

第九条　各金融机构应按照附件 2 所示的信息安全报告流程，指定负责部门向上级主管部门和中国人民银行延边州中心支行报告信息安全事件，当负责部门发生变更时及时向中国人民银行延边州中心支行科技处报告。

第十条　信息安全事件应在事发、事中与事后三个阶段分别报告:

（一）事件发生时，事发单位应立即报告，报告方式包括电话、传真、短信、邮件等等。事发报告重在及时，事发报告要素

参见附件 3。

（二）事件处置过程中，事发单位及时报告事件处置进展情况，根据需要，应多次报告（报告频度视情况决定，报告方式以快捷、完整、准确为原则），事中报告单参见附件 4。

（三）事件处置结束后，事发单位要及时总结事件响应、处置工作，由相关金融机构办公室以正式文件的形式提交详细的事件总结报告，总结报告中应附事后报告单，事后报告单参见附件 5。

第十一条　对重大（II 级）及以上的信息安全事件，事发单位要在事件发生后 1 小时内向中国人民银行延边州中心支行科技处提交书面事中报告，每 2 小时上报一次信息安全事件处置情况，直至信息安全事件处置结束，在事件处置完毕后 5 个工作日内提交事后报告。

第十二条　对达到较大（III 级）级别的信息安全事件，事发单位要在事件发生后 2 小时内，向中国人民银行延边州中心支行科技处提交书面事中报告，根据实际情况，可多次报告，在事件处置完毕后 8 个工作日内提交事后报告。

第十三条　接到事发单位的重大（II 级）及以上信息安全事件报告后，中国人民银行延边州中心支行科技处应当立即报告人民银行上级信息安全主管部门。

第十四条　各金融机构应设立负责信息安全报告的固定值班电话，并将其报告至中国人民银行延边州中心支行科技处，当

值班电话号码发生变更时及时向中国人民银行延边州中心支行科技处报告。

第十五条　各金融机构应规范信息安全事件接收与响应流程，提高信息安全事件处置效率。

三、风险报告

第十六条　各金融机构应加强信息系统脆弱性及其面临威胁的监测、检测、评估与分析，及时研究对策、完善措施。

第十七条　各金融机构应将信息安全风险管理纳入考核，及时发现、预警、处置信息安全风险。

第十八条　各金融机构应向中国人民银行延边州中心支行科技处及时报告本机构的重大信息安全风险。重大信息安全风险报告格式见附件 6；完成风险整改后，应再次提交风险整改报告，整改报告内容应包括风险情况、采取的措施、整改后情况等。

四、附则

第十九条　信息安全事件与风险报告应及时，不得迟报、谎报、瞒报、漏报，报告格式应规范，内容应客观准确。

第二十条　信息安全报告实行责任追究制，对于本制度执行不力的，将在一定范围内提出通报批评，并作为对各金融机构进行工作评价的依据。若对执行本制度不力并造成严重后果的，将依据有关规定报相关执法部门追究责任部门领导和直接责任人的责任。

第二十一条 本制度由中国人民银行延边州中心支行负责解释。

第二十二条 本制度自印发之日起实施。

附件 1：信息安全事件分级

一、信息系统分类

根据国家等级保护定级原则，从信息系统数据信息和提供服务功能的重要性，按照安全事件发生后对国家安全、社会秩序、经济建设、公共利益以及金融机构主要业务造成影响程度的不同，进行信息系统的分类。

（一） A 类系统

信息系统数据或服务受到破坏后，凡符合下列条件之一的系统确认为 A 类系统:

1. 会对国家安全造成特别严重损害的系统。

2. 会对社会秩序、公共利益造成特别严重损害的系统。

3. 会对金融机构主要业务造成特别严重损害的系统。

（二） B 类系统

信息系统数据或服务受到破坏后，凡符合列条件之一的系统确认为 B 类系统:

1. 会对国家安全造成严重损害的系统。

2. 会对社会秩序、公共利益造成严重损害的系统。

3. 会对金融机构主要业务造成严重损害的系统。

（三） C 类系统

信息系统数据或服务受到破坏后，凡符合列条件之一的系统确认为 C 类系统:

1. 会对国家安全造成较大损害的系统。

2. 会对社会秩序、公共利益造成较大损害的系统。

3. 会对金融机构主要业务造成较大损害的系统。

二、信息安全事件分级定义

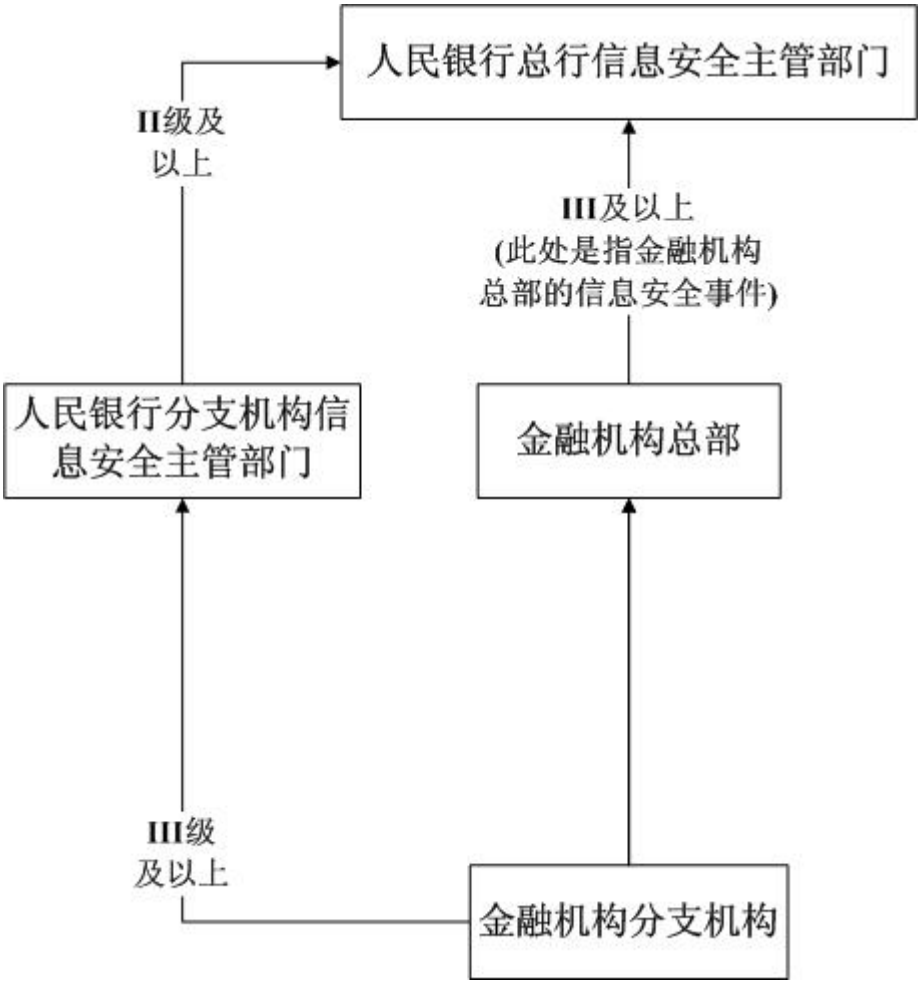
类型		特别重大信息安全事件（Ⅰ级）	重大信息安全事件（Ⅱ级）	较大信息安全事件（Ⅲ级）
系统运行安全类	A 类系统	金融机构延边辖区业务无法正常开展达 3 个小时（含）以上，或全国业务无法正常开展达 1 个小时（含）以上的信息安全事件。	金融机构延边辖区业务无法正常开展达 2 个小时（含）、3 个小时以内，或全国业务无法正常开展达 30 分钟（含）、1 个小时以内的信息安全事件。	金融机构延边辖区业务无法正常开展达 30 分钟（含）、2 个小时以内的信息安全事件。
	B 类系统	金融机构延边辖区业务无法正常开展达 6 个小时（含）以上，或全国业务无法正常开展达 3 个小时（含）以上的信息安全事件。	金融机构延边辖区业务无法正常开展达 3 个小时（含）、6 个小时以内，或全国业务无法正常开展达 40 分钟（含）、3 个小时以内的信息安全事件。	金融机构延边辖区业务无法正常开展达 40 分钟（含）、3 个小时以内的信息安全事件。
	C 类系统	金融机构延边辖区业务无法正常开展达 8 个小时（含）以上，或全国业务无法正常开展达 4 个小时（含）以上的信息安全事件。	金融机构延边辖区业务无法正常开展达 4 个小时（含）、8 个小时以内，或全国业务无法正常开展达 1 个小时（含）、4 个小时以内的信息安全事件。	金融机构延边辖区业务无法正常开展达 1 个小时（含）、4 个小时以内的信息安全事件。
数据安全类		数据丢失或被窃取、篡改、假冒对国家安全、社会秩序、经济建设和公众利益构成特别严重影响的网络与信息安全事件。	数据丢失或被窃取、篡改、假冒对国家安全、社会秩序、经济建设和公众利益构成严重影响的网络与信息安全事件。	数据丢失或被窃取、篡改、假冒对国家安全、社会秩序、经济建设和公众利益构成较大影响的网络与信息安全事件。
其他		其他对国家安全、社会秩序、经济建设和公众利益构成特别严重影响的网络与信息安全事件。	其他对国家安全、社会秩序、经济建设和公众利益构成严重影响的网络与信息安全事件。	其他对国家安全、社会秩序、经济建设和公众利益构成较大影响的网络与信息安全事件。

注：① 表中事件时间以一天内的时段累加计算；时断时续事件

时间按实际影响时间的 30%计算。

② 表中所称中断为异常中断，不包括计划内停机等情形。

附件 2：信息安全事件报告流程图



附件 3： 信息安全事件事发报告要素

事件名称	
事发单位	
事发部门	
报告时间	*年/月/日/时/分*
报告人姓名	
联系方式	
事件情况概述	*事件发现方式、发生事件、发生地点、现象及初步影响*
事件涉及的系统名称	
影响业务情况	*影响业务的名称和相关情况*
初步采取的措施及报告时的事件的状态	

附件 4：信息安全事件事中报告单

事件名称	
事发单位	
事发部门	
报告次数（多次报告时）	
报告时间	*年/月/日/时/分*
报告人姓名	
联系方式	
事件发现方式	*用户反映/巡检/监控报警/日志分析/检查/其他____（填写具体内容）*
事件发生时间	*年/月/日/时/分*
事件发生地点	*机房名*
事件涉及的系统名称	
事件现象	*用户无法登录/停止服务响应/服务响应变慢/设备停止工作/网络通信不畅/设备资源不足/数据库死锁/监控频繁报警/其他____（填写具体内容）*
影响业务情况	*影响业务的名称和具体情况*
影响范围	*所影响的外部/内部联网机构名称、影响的地区（省/市/县）名称和初步的损失估算*
事件原因分析	*按照系统脆弱点和外部威胁分别详尽描述，其中，外部威胁分类如下：有害程序/网络攻击/信息破坏/有害信息/硬件故障/软件故障/误操作/灾害性事故/其他___（填写具体内容）*
已采取的处置措施及事件的状态	
下一步拟采取的措施	
需人民银行协调处置的事项	

报告部门负责人签字：_____

注：

① 多次提交事中报告时，后续报告要素为事件名称、报告次数、报告时间、报告人姓名、联系方式、事件处置进展情况、事件处置措施详细描述、事件损失和影响的初步评估、下一步拟采取的措施。

② 事中报告原则上应加盖公章，如因条件限制无法加盖公章，报告部门负责人应签字。

附件 5：信息安全事件事后报告单

事件名称	
事发单位	
事发部门	
报告时间	*年/月/日/时/分*
报告人姓名	
联系方式	
事件系统架构	*主要业务功能/结构部署/关联系统名称*
事件系统硬件	*设备类别（网络/服务器/存储/外设）/设备品牌/设备型号/*
事件系统软件	*操作系统/数据库/存储/中间件/应用程序/名称（开发商）版本号、补丁号*
事件系统冗余	*HA/N+1/数据备份/应用备份*
直接影响业务	*业务名称详列*
间接影响业务	*业务名称详列*
事件区域	*外联区/接入区/交换区/工作区/生产区/安全管理区/测试区/互联网应用区/其他区*
事件部位	*网络通信服务/APP 服务/DB 服务/存储服务/备份服务/供配电/空调/机房/管理控制服务*
事件层次	*数据层（业务数据/用户数据/系统配置数据）/应用层（接口/WEB）/服务层（中间件/数据库/共享服务平台）/操作系统层（内存/磁盘/I/0 设备/外设/进程调度）硬件层（网络/服务器硬件及其固化程序）*
事件组件	*外部接入控制（网络接入/接口程序/接口设备）/用户访问控制（登录界面/I 与 O/用户管理/权限管理/用户视图/报表展现）/应用逻辑执行（例程/管理）/应用逻辑驱动（存取/显示）/数据库控制（查询/操作）/日志/审计/其他*
事件处置措施详细描述	*按照准备/排查与分析/限制、消除与恢复/事后措施等分阶段进行过程性描述* *若启用冗余备份手段恢复生产，说明条件准备/决策情况/具体处置措施/生产恢复效果/回切计划等*
事件源定位	*设计（架构/系统/组件）/实现（开发/集成/测试）/运维（业务变更/技术变更）/灾备（传输/复制）*
事件持续时间	*事件发生时间点至服务功能恢复或系统性能恢复时间点，（按分钟计算）*
事件处置队伍	*负责单位名称/协作单位名称/涉及单位名称及其处置效果描述*
损失和影响评估	*损失评估（经济损失/声誉损失）/影响（政治影响/社会影响）评估*
责任处置情况	*持续改进/责任处罚/其他*
类似事件预防措施建议	
处置经验与教训	
备注	

附件 6：重大信息安全风险报告单

风险描述	
报告时间	*年/月/日/时/分*
报告单位	
报告人姓名	
联系方式	
风险发现途径	*用户反映/巡检/监控报警/日志分析/检查/评估*
风险发现时间	*年/月/日/时/分*
风险发现地点	*机房名*
产生风险的系统名称	
产生风险的系统类别	*A/B/C*
风险系统硬件	*设备类别（网络/服务器/存储/外设）/设备品牌/设备型号*
风险系统软件	*操作系统/数据库/存储/中间件/应用程序/名称（开发商）版本号、补丁号*
风险层次	*数据层（业务数据/用户数据/系统配置数据）/应用层（接口/WEB）/服务层（中间件/数据库/共享服务平台）/操作系统层（内存/磁盘/I/0设备/外设/进程调度）硬件层（网络/服务器硬件及其固化程序）*
风险部位	*按照系统脆弱点和外部威胁分别详尽描述，其中，外部威胁分类如下：有害程序/网络攻击/信息破坏/有害信息/硬件故障/软件故障/误操作/灾害性事故/其他___（填写具体内容）*
风险产生原因	*设计缺陷（结构/程序）/实现缺陷（集成配置）/维护缺陷（业务与技术变更）/设备缺陷（设计/部件/补丁）/用户误操作*
风险危害分析	*风险可能危害的业务（包括关联业务）/机构/地域等名称、范围*
风险控制措施	*已采取措施及拟采取措施*
风险关联系统分析	
需人民银行协调处置事项	