某某单位
信息安全管理制度汇编

2019 年 1 月

信息化管理处

.

关于本文件

文件名称	吉林省某某单位信息安全管理制度汇编		
文件编号		控制级别	内部资料
文件类别	管理制度	文件页数	
编制		日期	年 月 日
审核		日期	年 月 日
签发		日期	年 月 日

分发控制[受控文件填写]

编号		份数	
用途			
审批人		日期	
经手人		日期	

.

目　录

.

.

.

.

.

.

第一章 安全策略总纲

.

1.1、信息安全策略总纲

1.1.1、 总则

第一条 为贯彻国家对信息安全的规定和要求，指导和规范吉林省某某单位信息系统建设、使用、维护和管理过程中，实现信息系统安全防护的基本目的，提高信息系统的安全性，防范和控制系统故障和风险，确保信息系统安全、可靠、稳定运行,维护社会秩序、公共利益和国家安全，特制定《吉林省某某单位信息安全策略总纲》（以下简称《总纲》）。

第二条 《总纲》根据国家信息安全相关政策法规而制定。

第三条 本制度适用于吉林省某某单位信息系统，适用于吉林省某某单位拟建、在建以及运行的非涉密信息系统。

1.1.2、 信息安全工作总体方针

第四条 吉林省某某单位信息系统的安全保护管理工作总体方针是“保持适度安全；管理与技术并重；全方位实施，全员参与；分权制衡，最小特权；尽量采用成熟的技术”。“预防为主”是吉林省某某单位信息安全保护管理工作的基本方针。

.

第五条 《总纲》规定了吉林省某某单位信息系统安全管理的体系、策略和具体制度，为信息化安全管理工作提供监督依据。

第六条 吉林省某某单位信息系统安全管理体系是由信息安全策略总纲、安全管理制度、安全技术标准以及安全工作流程和操作规程组成的。

(一)《总纲》是信息安全各个方面所应遵守的原则方法和指导性策略文件。

(二)《总纲》是制定吉林省某某单位信息安全管理制度和规定的依据。

(三)吉林省某某单位信息安全管理制度和规定了信息安全管理活动中各项管理内容。

(四)吉林省某某单位信息安全技术标准和规范是根据《总纲》中对信息安全方面相关的规定所引出的，其规定了信息安全中的各项技术要求。

第七条 吉林省某某单位信息安全工作流程和操作规程详细规定了主要应用和事件处理的流程、步骤以及相关注意事项，并且作为具体工作时的具体依照。

1.1.3、 信息安全总体策略

第八条 吉林省某某单位信息系统总体安全保护策略是：系统资源的价值大小、用户访问权限的大小和系统重要程度

.

的区别就是安全级别的客观体现。信息安全保护必须符合客观存在和发展规律，其分级、分区域、分类和分阶段是做好信息安全保护工作的前提。

第九条 吉林省某某单位信息系统的安全保护策略由吉林省某某单位网络安全与信息化工作领导小组负责制定与更新。

第十条 吉林省某某单位网络安全与信息化工作领导小组根据信息系统的安全保护等级、安全保护需求和安全目标，结合吉林省某某单位自身的实际情况，依据国家信息安全法规和标准，制定信息系统的安全保护实施细则和具体管理办法，并根据实际情况，及时调整和制定新的实施细则和具体管理办法。

第十一条 吉林省某某单位信息系统的安全保护工作应从技术体系和管理体系两个方面进行，技术体系包括物理环境安全、网络安全、主机安全、应用安全和数据安全等五个部分，管理体系包括安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等五个部分，由技术体系和管理体系共十个部分构成信息系统安全等级保护体系。

（一）物理环境安全包括：周边环境安全，门禁检查，防盗窃、防破坏、防火、防水、防潮、防雷击、防电磁泄露和干扰，电源备份和管理，设备的标识、使用、存放和管理等；

.

（二）网络安全包括：网络的拓扑结构，网络的布线和防护，网络设备的管理和报警，网络攻击的监察和处理，网络安全审计和检查及边界完整性检查；

（三）主机安全包括：主机的身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、监控和终端接入控制等；

（四）应用安全包括：应用系统的身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性和保密性、抗抵赖、软件容错和资源控制等；

（五）数据安全包括：数据传输的完整性和保密性、数据存储的完整性和保密性、数据的备份和恢复等；

（六）安全管理制度是信息系统安全策略、方针性文件，规定信息安全工作的总体目标、范围、原则和安全框架，是管理制度体系的灵魂和核心文件；

（七）通过构建和完善信息安全组织架构的措施，明确不同安全组织和不同安全角色的定位、职责以及相互关系，强化信息安全的专业化管理，实现对安全风险的有效控制；

（八）人员安全管理包括人员录用、人员管理、人员考核、保密协议、培训、离岗离职等多个方面；

（九）系统建设管理根据信息密级、系统重要性和安全策略将信息系统划分为不同的安全域，针对不同的安全域确定不同的信息安全保护等级，采取相应的保护。信息系统安全等级的定级决定了系统方案的设计、实施、安全措施、运

.

行维护等信息系统建设的各个环节。信息系统定级遵循“谁建设、谁定级”的原则；

（十）系统运维管理对信息系统进行综合监控管理，对支撑重要信息系统的资源进行监控保护，确保密码防护、病毒防护、系统变更等事件按照规定的信息安全管理策略实行，建立安全管理监控中心，实现对人、事件、流程、资产等方面的综合管理。

1.1.4、 安全管理

第十二条 吉林省某某单位信息系统定级备案管理完全按照国家相关信息安全标准的相关政策要求进行。要求所有接入吉林省某某单位的信息系统均按照等级保护定级备案要求进行定级，参考《信息系统安全保护等级定级指南GB/T22240-2008》,由各应用系统接入单位自主定级并填写定级报告，吉林省某某单位网络安全与信息化工作领导小组办公室填写定级备案表，经吉林省某某单位网络安全与信息化工作领导小组批准，由吉林省某某单位网络安全与信息化工作领导小组办公室统一负责向公安机关进行备案。所有吉林省某某单位信息系统必须确定其信息安全保护等级，并在吉林省某某单位网络安全与信息化工作领导小组办公室进行登记和备案。

第十三条 业务应用需求和设计单位，要充分考虑信息

.

系统的安全需求分析，统一按照业务系统归属进行安全域划分，确定定级备案情况；具体参考《信息安全等级保护管理办法》、《信息系统安全等级保护基本要求》，参照《信息系统安全等级保护实施指南》、《信息系统通用安全技术要求》、《信息系统安全工程管理要求》、《信息系统等级保护安全设计技术要求》等标准规范要求，结合行业特点进行安全需求分析。

（一）信息安全需求分析，至少包括以下信息安全方面的内容：

1. 安全威胁分析；
2. 系统脆弱性分析；
3. 影响性分析；
4. 风险分析；
5. 系统安全需求。

（二）可行性分析中须包括以下信息安全方面的内容：

1. 明确项目的总体信息安全目标，并依据信息安全需求分析的结论提出相应的安全对策,每个信息安全需求都至少对应一个信息安全对策,信息安全对策的强度根据相应资产/系统的重要性来选择；
2. 描述如何从技术和管理两个方面来实现所有的信息安全对策，并形成信息安全方案；
3. 增加项目建设中的信息安全管理模式、信息安全组

.

织结构、人员的安全职责、建设实施中的安全操作程序和相应安全管理要求；

4. 对安全方案进行成本-效益分析；

5. 需求分析阶段必须明确地定义和商定新系统的需求和准则，并形成文件，便于后期验收。相关信息安全需求的要求和准则应包括：用户管理、权限管理、日志管理和数据管理等。

第十四条 业务应用的安全设计应按照国家信息安全标准进行，并依照信息安全需求分析评估得出的结论，通过相关专家评审会后，综合多方意见，进行安全设计。

具体要求如下：

(一) 物理安全-设计中要充分考虑到物理访问控制、防盗窃和防破坏、防雷击、防火、防水、防潮、电力、物理位置、防静电和电磁防护，做到增强控制，对人员和设备的出入进行监控；

(二) 网络安全-设计中要充分考虑到结构安全、访问控制、设备防护、安全审计、边界完整性检查、入侵防范、恶意代码防范，确保重要主机的优先级，做到应用层过滤，对入网设备的接入进行非法外联的定位和阻断，对形成的记录进行分析、形成报表，对审计系统进行两种以上鉴别技术，保证特权用户分离；

(三) 主机安全-设计中充分考虑主机系统(操作系统)的

.

身份鉴别、访问控制、入侵防范、恶意代码防范、安全审计、资源控制、剩余信息保护，要求必须监控服务器相关服务，保证最小授权原则，对形成的记录进行分析并形成报表；

(四) 数据安全-设计中充分考虑数据完整性、数据备份和恢复、数据保密性；

(五) 应用安全-设计中充分考虑应用系统的身份鉴别、访问控制、通信完整性和保密性、软件容错、安全审计、资源控制、剩余信息保护、抵赖性。

在信息系统安全规划设计时，应该考虑系统的容量和资源的可用性，以减少系统过载的风险，并采取相应的保密措施，控制涉及核心数据软件设计的相关资料的使用，并应遵循以下原则：

(一) 充分考虑应用安全实现的可控性，以便尽可能地降低安全系统与应用系统结合过程中的风险；

(二) 保持安全系统与应用系统的相互独立性，避免功能实现上的交叉或跨越；

(三) 建立完善的信息安全控制机制，包括：用户标识与认证、逻辑访问控制、公共访问控制、审计与跟踪等。

第十五条 信息系统安全建设管理需要按照国家信息安全标准的相关要求，并在安全管理组织的领导下，结合应用的实际情况，进行信息安全建设。

.

在建设中应充分考虑系统定级管理、安全方案设计管理、产品采购和使用管理、自行以及外包软件开发管理、工程实施管理、测试验收管理、系统交付管理、安全服务商选择管理、系统备案管理、等级测评管理等因素对信息系统安全的影响程度。

信息系统安全建设管理要求将系统建设过程有效程序化，明确指定项目实施监理负责人，确保系统设计文档和相关代码的安全，对销毁过程要进行安全控制，自行开发时应当严格控制对程序资源库的访问。

第十六条 信息系统安全验收管理按照国家相关信息安全标准的要求，结合吉林省某某单位信息系统的实际情况进行安全验收管理规范化。项目验收需得到各业务单位、吉林省某某单位网络安全与信息化工作领导小组办公室共同确认签字验收。项目应达到项目任务书中制定的总体安全目标和安全指标，实现全部安全功能。验收报告中应包括项目总体安全目标及主要内容。验收报告中应包括项目采用的关键安全技术内容。系统验收并移交后，必须立即修改系统中的默认口令。应用系统项目验收应审查如下内容：

(一) 功能检查包括对软件功能完整性、正确性进行审查和评价；

(二) 项目管理审查包括对项目计划、采用标准、需求方案及其执行情况进行审查和评价；

.

(三) 测试结果审查包括对项目测试报告、监理单位出具的监理报告等进行审查;

(四) 技术文档检查包括对项目开发单位交付的文档资料（纸质文档和电子文档）进行审查。

(五) 系统交付时,应根据合同要求制定系统交付的清单;

(六) 系统运行所需要的全部设备;

(七) 系统运行所需要的全部软件;

(八) 系统文档，包括系统建设过程中的文档，详细的系统使用和维护文档;

(九) 系统应急方案;

(十) 系统使用培训教材。

系统建设项目有下列情况之一，不能通过安全验收:

(一) 验收文件、资料、数据不真实;

(二) 未达到安全设计要求;

(三) 设计不符合国家信息安全建设相关标准要求;

(四) 擅自修改设计目标和建设内容;

(五) 系统建设过程中出现重大问题，未能解决和做出说明，或存在纠纷。

项目验收完毕后，系统建设部门应对负责系统使用和维护的人员进行相应培训，并履行服务承诺。

第十七条 安全测评管理是按照国家信息安全标准测评的相关要求，结合吉林省某某单位的实际情况进行安全测

.

评。项目验收时应按照信息安全法律法规和标准情况，进行自评估或委托具有国家相关技术资质和安全资质的第三方测评机构进行测评，并出具测评报告，测评报告将作为项目验收的参考依据。信息系统的安全性测试验收应独立进行，测试程序应包括以下内容：

(一) 测试验收前根据设计方案或合同要求等制订测试验收方案，测试验收方案应对参与测试部门、人员、现场操作过程等进行要求,并确保测试和接收标准被清晰定义并文档化；

(二) 测试方案应通过吉林省某某单位网络安全与信息化工作领导小组办公室的论证和审定；

(三) 严格依据测试方案进行测试，测试验收过程中详细记录测试结果；

(四) 至少应审查主机端口开放情况是否符合系统说明、使用网络侦听工具查通讯数据包是否符合系统说明和使用恶意代码软件检测软件包中可能存在的恶意代码等。

(五) 拟定测试验收报告，并由相关负责人签字确认。

第十八条 安全运维管理按照国家信息安全标准的要求，项目验收完毕后，结合吉林省某某单位的实际情况进行运行维护管理工作。信息安全管理部门接管后，负责物理安全、网络安全、主机安全、数据安全等管理工作，并定期和

.

不定期的进行信息安全检查，确保信息系统安全运行。各业务系统的维护人员负责维护和监控责任范围内的应用系统，不得越权进行访问。信息安全运行维护项目应包括但不限于以下内容：

(一) 对物理安全的机房环境、温湿度等检查；

(二) 对网络的连通性、时延、丢包率，检查网络的状况、故障及攻击事件等；

(三) 对设备运行状态检查；

(四) 对出口链路或关键链路流量进行检查，设备配置进行备份工作等。

(五) 对新购置的设备和软件在上线之前进行安全性检查、策略合理性测试。

(六) 对设备和软件的日志进行定期和不定期的审计。

(七) 对设备和软件进行版本升级和相关库升级。

(八) 建立监控平台，对设备安全漏洞、安全事件、系统日志等信息进行监控，制定各项计划性的安全维护工作。

(九) 建立单位作业计划应包括以下内容安全设备维护、安全监控、操作日志、日志审核、故障管理、测试等工作，明确执行期限，落实到人。安全维护作业计划在编制和确定后，各业务单位应根据其内容严格执行。定期对维护计划执行情况进行总结分析。

.

（十）定期出具安全运行维护报告，报告涉及方面包括但不限于以下内容：安全设备维护内容、安全监控内容、操作日志、系统日志、故障处理内容等。

1.1.5、 制度的制定与发布

第十九条 吉林省某某单位信息化管理处负责制订信息系统安全管理制度，并以文档形式表述，经吉林省某某单位网络安全与信息化工作领导小组办公室讨论通过，由吉林省某某单位网络安全与信息化工作领导小组办公室负责人审批发布。

第二十条 吉林省某某单位信息化管理处负责组织制度编制、论证、监督检查和修订等工作。

第二十一条 吉林省某某单位信息化管理处负责根据信息系统安全管理制度，结合系统的特点进行细化和制定实施细则，报吉林省某某单位网络安全与信息化工作领导小组办公室审批，以正式形式发布。

第二十二条 吉林省某某单位信息系统安全管理制度编写格式统一，并进行版本控制。

第二十三条 信息安全管理制度由吉林省某某单位网络安全与信息化工作领导小组办公室负责审核，以正式文件形式发布，同时注明发布范围并有收发文登记。

.

1.1.6、 制度的评审和修订

第二十四条 由吉林省某某单位网络安全与信息化工作领导小组办公室负责文档的评审,对安全策略和制度的有效性进行程序化、周期性评审,并保留必要的评审记录和依据。

第二十五条 吉林省某某单位信息化管理处负责定期组织对安全管理制度的执行情况进行检查,并结合国家信息安全主管部门每年定期对信息安全进行检查中发现的问题,对安全管理制度进行有针对性的修订与完善。

第二十六条 当发生重大安全事故、出现新的安全漏洞以及技术基础结构发生变更时,吉林省某某单位信息化管理处要对安全管理制度的细则进行修订,修订后报吉林省某某单位网络安全与信息化工作领导小组办公室进行审批。

第二十七条 每个策略和制度文档有相应的负责人或负责部门,负责对明确需要修订的文档进行维护,并制定信息安全管理制度对应负责人或负责部门的清单。

.

附件 1-1-1 网络安全管理制度论证审定记录（模板）

网络安全管理制度论证审定记录表

<table>
<tr><td>组织部门</td><td colspan="5"></td></tr>
<tr><td>评审内容</td><td colspan="5"></td></tr>
<tr><td>评审原因</td><td colspan="5"></td></tr>
<tr><td>评审时间</td><td colspan="5"></td></tr>
<tr><td rowspan="7">参与人员</td><td>姓名</td><td>部门</td><td>岗位职责</td><td>联系方式</td><td>签到</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>评审意见</td><td colspan="5"></td></tr>
<tr><td>评审结论</td><td colspan="5"></td></tr>
<tr><td rowspan="2">签字</td><td>组织人</td><td colspan="4"></td></tr>
<tr><td>负责人</td><td colspan="4"></td></tr>
</table>

.

	记录人	

.

附件 1-1-2 网络安全管理制度收发文记录（模板）

网络安全管理制度收发文记录表

发文信息	文件名称			
	发文部门			
	文件编号			
	发文号			
	发文日期			
	发文方式			
签收信息	签收部门	签收人	签收时间	备注

.

第二章 安全管理机构

.

2.1、信息安全组织及岗位职责管理规定

2.1.1、 总则

第一条 为了加强吉林省某某单位对信息安全工作的管理，全面提高信息安全管理能力，规范信息安全管理组织体系，建立健全信息安全机构职责，特制定本规定。

第二条 本规定依据《国家信息化领导小组关于加强信息安全保障工作的意见》、《GB/T20269-2006 信息安全技术信息系统安全管理要求》等政策标准制定。

第三条 本规定依照“信息安全管理的主要领导负责、全员参与、依法管理、分权和授权和体系化管理”原则编制，具体原则如下：

（一）主要领导负责原则：吉林省某某单位应确保主要领导参与并确立组织统一的信息安全保障宗旨和政策，组织有效的安全保障队伍，调动并优化配置必要的资源，协调安全管理工作与各部门工作的关系，并确保其落实、有效；

（二）全员参与原则：信息系统所有相关人员普遍参与信息系统的安全管理，并与相关方面协同、协调，共同保障信息系统安全；

（三）依法管理原则：信息安全管理工作应保证管理主

体合法、管理行为合法、管理内容合法、管理程序合法；

（四）分权和授权原则：对特定职能或责任领域的管理功能实施分离、独立审计等实行分权，避免权力过分集中所带来的隐患，以减小未授权的修改或滥用系统资源的机会。任何实体（如用户、管理员、进程、应用或系统）仅享有该实体需要完成其任务所必须的权限，不应享有任何多余权限。

（五）体系化管理原则：吉林省某某单位整体应符合信息系统等级保护三级的体系化管理目标和要求。

第四条 本规定适用于吉林省某某单位。

2.1.2、 信息安全组织机构

第五条 吉林省某某单位应建立由吉林省某某单位网络安全与信息化工作领导小组和吉林省某某单位网络安全与信息化工作领导小组办公室共同构建的安全管理机构。

第六条 由吉林省某某单位主管领导或主管领导授权的主管机构领导担任吉林省某某单位网络安全与信息化工作领导小组组长，小组成员包括：

（一）吉林省某某单位信息化主管领导；

（二）吉林省某某单位各业务单位的主管领导；

（三）吉林省某某单位信息化管理处主管领导。

第七条 吉林省某某单位网络安全与信息化工作领导小

.

组办公室是吉林省某某单位的信息化管理处，是信息安全工作的执行机构，负责执行吉林省某某单位网络安全与信息化工作领导小组交办的各项工作，由吉林省某某单位信息化主管领导主管领导担任负责人，成员为各业务单位的主管领导，信息安全执行层包括：

（一）吉林省某某单位的网络管理员、系统管理员、安全管理员、安全审计员、安全策略/规划员、数据库管理员、应用管理员和机房管理员；

（二）吉林省某某单位各业务单位的安全员。

第八条 信息化管理处应设立信息安全管理岗位，分别为安全管理员、安全审计员、网络管理员、系统管理员、数据库管理员、应用管理员和机房管理员，负责执行网络、系统、数据库、应用和机房的安全管理和运维工作。

第九条 其他信息化相关部门应指派安全员，负责协调本部门信息安全工作的落实和具体执行情况。

2.1.3、 信息安全组织职责

第十条 吉林省某某单位网络安全与信息化工作领导小组办公室负责领导吉林省某某单位的信息系统安全工作，组织职责如下：

（一）根据国家和行业有关信息安全的政策、法律和法规，确定信息安全工作的总体方向、总体原则和安全工作方

.

法；

（二）根据国家和行业有关信息安全的政策、法律和法规，批准吉林省某某单位信息系统的安全策略和发展规划；

（三）确定各有关部门在信息系统安全工作中的职责，领导安全工作的实施；

（四）监督安全措施的执行，并对重要安全事件的处理进行决策；

（五）指导和检查信息化管理处的各项工作；

（六）建设和完善信息系统安全组织体系和管理机制。

第十一条 吉林省某某单位网络安全与信息化工作领导小组办公室负责贯彻、落实和执行吉林省某某单位网络安全与信息化工作领导小组下达的各项工作，组织职责如下：

（一）贯彻、落实和解释国家和行业有关信息安全的政策、法律、法规和信息安全工作要求，起草吉林省某某单位信息系统的安全策略和发展规划；

（二）落实和执行吉林省某某单位信息安全工作的日常事务，对具体落实情况进行总结和汇报；

（三）负责安全措施的实施或组织实施，组织并参加信息安全重要事件的处理；

（四）负责内、外部组织和机构的信息安全沟通、协调和合作工作；

（五）组织编制和落实信息安全规划、方案、实施、测

.

试和验收等工作；

（六）指导和检查相关单位信息系统安全工作落实情况；

（七）监控信息系统安全总体状况，提出安全分析报告；

（八）指导和检查相关单位和下级单位信息系统安全人员及要害岗位人员的信息安全工作；

（九）协同有关部门共同组成应急处理小组，组织处理信息安全应急响应工作；

（十）负责组织信息系统安全知识的培训和宣传工作。

2.1.4、 信息安全岗位职责

第十二条 吉林省某某单位信息安全组织中应建立信息安全岗位，明确信息安全岗位职责。

第十三条 信息安全工作主管(信息化管理处主任)的岗位职责如下：

（一）组织、协调落实各项信息安全工作；

（二）组织评审信息安全总体策略、规划方案、管理制度和技术规范；

（三）组织评审信息安全产品技术规格和相关产品安全规格；

（四）组织监督、检查信息安全工作的落实情况。

第十四条 安全管理员(专职)的岗位职责如下：

.

（一）起草和编制吉林省某某单位信息安全方针、信息安全保障体系框架和信息安全策略、制度和技术规范；

（二）起草和编制吉林省某某单位信息安全总体规划，收集信息系统安全需求；

（三）推动吉林省某某单位信息安全方针、信息安全策略、信息安全管理制度及信息安全技术规范的实施落实。

（四）定期组织信息系统漏洞扫描和信息安全风险评估工作，形成信息系统和整体安全现状报告，并向吉林省某某单位网络安全与信息化工作领导小组办公室进行汇报；

（五）负责制定总体网络访问控制策略和规则，并对其进行监控和审计工作，定期发布策略执行情况；

（六）负责制定全员的安全培训计划，组织开展安全培训工作；

（七）对网络、系统、应用、数据库管理员进行安全指导；

（八）定期收集信息安全漏洞和公告信息，并告知相关部门的信息安全运维管理人员及安全员；

（九）协调信息安全应急响应组织和技术支撑单位。

第十五条 安全审计员的岗位职责如下：

（一）定期审计信息安全策略执行情况，收集信息系统日志和审计记录，并提供审计报告；

（二）对安全、网络、系统、应用、数据库、机房管理

.

员的操作行为进行监督，安全职责落实情况进行检查；

（三）组织检查相关单位和下级单位信息系统安全人员及要害岗位人员的信息安全工作。

第十六条 系统管理员的安全职责如下：

（一）根据吉林省某某单位安全策略定期对系统进行自评估；

（二）依照安全策略对系统进行安全配置和漏洞修补；

（三）对系统进行日常安全运维管理，定期更改系统账号，并定期提交安全运行维护记录或报告；

（四）在发生系统异常和安全事件时对系统进行应急处置。

第十七条 网络管理员的安全职责如下：

（一）根据吉林省某某单位安全策略定期对网络设备、网络架构进行自评估；

（二）依照安全策略对网络设备进行安全配置；

（三）对网络设备、安全设备进行日常安全运维管理，并定期提交安全运行维护记录或报告；

（四）在发生系统异常和安全事件时，对网络设备、安全设备进行应急处置。

第十八条 数据库管理员的安全职责如下：

（一）根据吉林省某某单位安全策略定期对数据库安全进行自评估；

.

（二）依照安全策略对数据库进行安全配置和漏洞修补；

（三）对数据库进行日常安全运维管理，定期检查数据库用户，并提交安全运行维护记录或报告；

（四）在发生数据库异常和安全事件时，对数据库以及备份数据进行应急处置和恢复。

第十九条 应用管理员的安全职责如下：

（一）根据吉林省某某单位安全策略定期对应用进行自评估；

（二）依照安全策略对应用进行安全配置和漏洞修补；

（三）对应用进行日常安全运维管理，并提交安全运行维护记录或报告；

（四）在发生应用异常和安全事件时，对应用进行应急处置和恢复。

第二十条 机房管理员的安全职责如下：

（一）负责机房的物资管理和日常维护工作；

（二）根据信息化管理处的要求，严格遵守工作流程，确保日常工作的正常进行；

（三）完成信息化管理处交办的其他工作。

第二十一条 重要业务系统操作人员的安全职责如下：

（一）根据吉林省某某单位安全策略对业务系统进行安全操作；

.

（二）负责定期对业务系统操作进行自评估，如发现非法或违反安全策略的操作应及时报告安全审计员。

第二十二条 相关部门安全员的岗位职责如下：

（一）负责本部门信息安全工作的开展，并配合信息化管理处的信息安全工作；

（二）遵照吉林省某某单位的信息安全策略协调本部门的信息安全技术落实；

（三）指导并参与信息安全相关项目的建设；

（四）协调本部门的信息安全工作，并接受数据信息化管理处定期和不定期的检查。

2.1.5、 信息安全岗位要求

第二十三条 吉林省某某单位应设立专职的信息安全管理岗位，并由专人负责，根据信息安全管理的实际工作情况，人员编制为 3-6 人。

第二十四条 吉林省某某单位设立专职的安全管理员。

第二十五条 关键岗位应配备多人共同管理，定期轮岗，关键岗位人员配备坚持“权限分散、不得交叉覆盖”的原则，安全管理员和安全审计员不能由一人身兼。

第二十六条 信息化管理处应根据岗位职责，确定岗位所需要的安全技能，并对所有信息安全岗位人员进行相应的安全技能培训。

.

第二十七条 吉林省某某单位信息系统的安全技术岗位可由其他相关管理员兼任，其中网络安全管理、系统安全管理、数据库安全管理以及应用安全管理工作可分别由网络管理员、系统管理员、数据库管理员以及应用管理员执行。

第二十八条 重要业务系统操作人员应在日常工作中认真执行吉林省某某单位安全策略和技术安全规范中的各项要求。

第二十九条 各个业务单位的安全员应紧密配合部信息安全工作，协调本单位信息安全策略的落实和信息安全工作的具体执行。

2.1.6、 附则

第三十条 本规定的解释权归吉林省某某单位。

第三十一条 本规定自发布之日起生效。

.

附件 2-1-1 网络安全工作授权审批单（模板）

网络安全工作授权审批单

授权审批事件信息			
审批事项			
事项类型	☐受控资料使用　☐外部网络连接　☐内部网络接入 ☐特殊权限申请 ☐其他_____		
申请人		**所在部门**	
担任职位		**申请时间**	
详细说明			
授权审批流程及签字			
审批人员	**人员签字**	**审批意见**	**审批时间**
申请人			
部门领导			
主管领导			
其他相关人员			

.

附件 2-1-2 网络安全工作会议记录表（模板）

网络安全工作会议记录表

会议信息			
会议名称			
会议日期		会议时间	
会议地点			
参会单位	☐内部会议 ☐主管机构 ☐监督机构 ☐外联单位 ☐服务厂商		
主持人		记录人	
人员信息			
参会人员	单位/部门	联系方式	签到时间
会议记录			
会议内容			

.

附件 2-1-3 外联单位工作联系表（模板）

外联单位工作联系表

序号	姓名	联系电话	邮箱	单位	负责事项	备注
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						

.

24						

.

2.2、信息安全检查与审计管理制度

2.2.1、 总则

第一条 为了加强吉林省某某单位信息安全检查与审计工作管理，确保信息安全管理符合国家有关要求，特制订本制度。

第二条 本规定适用于吉林省某某单位。

2.2.2、 安全检查

第三条 信息安全检查包括各业务部门自查和信息安全处定期执行的安全检查。

第四条 各业务部门的自查内容应包括业务系统日常运行、系统漏洞和数据备份等情况，自查工作应保留自查结果。自查应至少一个季度组织一次。

第五条 信息化管理处执行的安全检查内容应包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况和业务处室自查结果抽查等。安全检查应至少半年组织一次。

第六条 自查和安全检查均应在检查之前形成检查表，自查检查表应经过业务部门领导审核通过，安全检查表应经过信息安全工作小组审核通过。

.

第七条 应严格按照检查表实施检查，检查完毕，记录下所有检查结果，检查记录需经各业务部门领导签字认可。

第八条 应对检查记录进行归档，只有授权人员可以访问阅读。

第九条 应对检查结果进行汇总分析，形成安全检查报告，检查报告应对问题进行分析，提出解决建议。

第十条 应制定措施防止安全检查结果的非授权散布，只对经过授权的人员通报安全检查结果。

第十一条 各业务部门应阅读并理解安全检查报告，在信息化管理处的指导下对出现的问题进行整改。信息化管理处应对整改过程进行监督，并将整改结果报送信息安全工作小组。

2.2.3、 安全审计

第十二条 安全审计作为整体审计工作的一个部份，依据审计工作相关管理办法开展安全审计工作。

第十三条 安全审计人员的配备应根据实际情况，采用如下方法的一种，原则上应以审计部门培养自身独立的安全审计人员为主，其他手段为辅。

1、 由审计部门独立完成，使用审计部门具备相应技能的人员完成审计工作；

2、 由审计部门和信息化管理处共同完成，信息化管理

处指派熟悉技术的人员配合审计部门完成审计工作，本情形需注意审计独立的原则，进行交叉审计；

3、 聘请外部专业审计单位完成审计工作

第十四条 安全审计的内容主要包括：

1、 相关法律法规的符合情况；

2、 管理部门的相关管理要求的符合情况；

3、 现有安全技术措施的有效性；

4、 安全配置与安全策略的一致性；

5、 安全管理制度的执行情况；

6、 安全检查和自查的检查结果及检查报告；

7、 日志信息是否完整记录；

8、 各类重要记录是否免受损失、破坏或伪造篡改；

9、 检查系统是否存在漏洞；

10、检查数据是否具备安全保障措施。

第十五条 安全审计工作应具有独立性，避免有舞弊的情况发生。

第十六条 安全审计的方式分为：

1、 全面审计：即审计内容覆盖安全管理范围内的所有部门，以及所有信息安全控制措施要求的检查。

2、 专项审计：即审计内容只涉及部分部门，或部分信息安全控制措施要求的检查。

第十七条 无论是采用全面审计还是专项审计方式，安全

.

审计应每一年对所有的部门，以及所有的信息安全控制措施要求至少进行过一次审计。

第十八条 被审计方应积极配合信息安全审计工作，应对审计结果进行确认。

第十九条 安全审计工作中发现的不符合事项应按照审计管理相关制度要求进行改进。审计部门应将改进过程和结果通告给信息安全工作小组。

2.2.4、 附则

第二十条 本制度的解释权归吉林省某某单位。

第二十一条 本制度自发布之日起生效。

.

附件 2-2-1 年度网络安全检查记录（模板）

年度网络安全检查记录

单位基本情况						
单位名称						
单位地址	_____省（区、市）_____地（区、市、州、盟） _____县（区、市、旗）					
邮政编码						
单位网络安全分管领导	姓　　名		职务/职称			
网络安全责任部门						
责任部门负责人	姓　　名		职务/职称			
	办公电话		移动电话			
责任部门联系人	姓　　名		职务/职称			
	办公电话		移动电话			
单位类型						
信息系统总数（总部和分支机构）		第四级系统数		第三级系统数		
		第二级系统数		第一级系统数		
		未定级系统数				
本单位信息系统总数（已在公安部门报备）		第四级系统数		第三级系统数		
		第二级系统数		未定级系统数		
本单位信息系统测评数量		第四级系统数		第三级系统数		
		第二级系统数		未定级系统数		
本单位信息系统测评合格数量		第四级系统数		第三级系统数		
		第二级系统数		未定级系统数		
一、网络安全工作的基本情况						
1.网络安全工作组织（协调）领导机构情况						
（说明网络安全组织（协调）领导机构建立、组成、分工以及网络安全工作议事或例会制度等具						

.

体情况）
2.网络安全责任制落实情况
（说明本单位网络安全工作责任制的具体内容：包括每个信息系统是否有明确的安全责任人，专职信息安全员的数量情况，是否逐级签订网络安全责任书，是否建立了责任追究制度，是否明确了专门的监督管理人员负责责任追究制度落实等情况）
3.网络安全规划和策略
（说明是否制定了本单位网络安全规划和策略，规划和策略的核心内容，是否落实了网络安全与信息化建设同步立项、同步设计、同步建设、同步验收等情况）
4.网络安全工作考核和经费保障情况
（说明本单位网络安全工作是否纳入到年度考核指标，是否定期召开会议或印发文件部署网络安全工作，本年度的网络安全工作经费预算情况，上年度的网络安全经费预算和执行情况）
5.网络安全教育培训情况
（说明本单位网络安全教育培训计划具体制定情况，信息技术人员及系统使用人员定期进行安全培训的具体情况）
6.网络安全人员安全管理制度
（说明本单位信息安全人员安全管理制度的制定情况：包括人员录用、离岗、考核、安全保密、教育培训管理制度。）
7.机房安全管理制度
（说明本单位机房安全管理制度的具体内容：包括制定和下发人员进出机房管理制度，机房进出人员登记记录情况，机房的日常安全保卫和防火、防盗、防水的各项工作措施落实情况，及机房日常监控情况）
8.系统建设管理制度

.

（说明本单位系统建设管理制度的执行情况：包括按照制度要求在产品采购、服务外包过程中签订安全保密责任书，及信息系统投入使用前进行安全性测试，请查阅相关记录）

目前系统建设并未在产品采购、服务外包过程中签订安全保密责任书，但在合同中有对保密责任的约束，信息系统投入使用前未进行严格的安全性测试，现已意识到网络安全的重要性，会逐步完善系统建设管理制度，并要求系统建设严格按照管理制度有序进行。

9．资产管理制度

（说明本单位是否指定专人进行网络与信息系统资产管理，是否建立信息系统软硬件统一登记表，是否及时对信息系统中的老旧设备进行维护和更换等）

10.日常网络安全监测和预警情况

（说明日常网络安全监测预警制度的制定和执行情况，单位自身开展网络安全监测预警情况以及聘请有关技术支撑单位对互联网站和网上信息系统开展技术渗透情况）

11.安全事件应急处置和灾备建设情况

（说明本单位安全时间应急处置的具体内容：包括应急预案的制定，下发和学习，定期开展应急演练的情况，是否根据演练情况修订或完善应急处置预案，是否与公安、通信、电力以及其他运行支撑部门开展联合应急演练情况，是否建立了应急处置工作机制，是否开展了异地灾备中心建设等情况）

12.网络安全事件（事故）情况

（说明本年度是否发生网络安全事件（事故），具体原因是什么，如何进行处置，造成的后果和影响是什么）

二、信息安全等级保护具体工作情况

1.信息系统定级备案情况

（说明本单位的信息系统的定级及备案情况，包括资料的编制及填写，主管部门、监管部门及公安部门的报备情况）

2.等级测评工作情况

.

（说明本单位的等级测评经费预算情况，对选择的等级测评机构资质情况及已定级的信息系统进行等级测评的数量，第三级以上信息系统按要求定期开展测评工作的情况，及等级测评报告提交受理备案的公安机关的相关工作情况）
3.安全建设整改情况
（说明本单位安全建设整改情况的具体内容：包括对发现安全问题的信息系统进行安全建设整改的工作情况，及在完成整改前，采取有效的风险控制措施的执行情况）
4.安全自查工作情况
（说明本单位开展安全检查工作的计划、内容及执行情况；本单位通过自查发现安全隐患的数量情况，对安全隐患的整改情况）
5.信息安全整改工作落实情况
（说明本单位信息安全整改工作落实情况，包括信息安全整改短期计划及长期计划制定情况，整改工作落实情况，资金落实情况等）
三、信息系统安全保护管理措施和关键技术措施建设情况
1.网络安全情况
（说明本单位网络安全情况：包括网络设备运行状况、网络流量、用户行为等的记录分析情况；网络边界处监视端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫等攻击情况，及当对网络设备进行远程管理时；采取措施防止鉴别信息在网络传输过程中被窃听情况）
2.主机安全情况
（说明本单位的主机安全情况：包括操作系统和数据库系统管理用户身份标识、口令有效性和定期更换情况；采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别情况，及防恶意代码软件安装、更新情况）
3.应用安全情况

.

（说明本单位应用安全情况：包括登录控制模块对登录用户进行身份标识和鉴别情况，及依据安全策略控制用户对文件、数据库表等客体的访问情况）
4.数据安全及备份恢复情况
（说明本单位重要信息系统数据在传输、存储、保密等方面采取的安全保护措施情况；对重要业务应用和重要数据的备份情况）
四、信息系统使用信息技术产品和服务情况
1.系统和应用软件使用情况
（列表说明本单位系统和应用软件中，国内和国外操作系统、数据库、办公软件、业务应用软件、中间件、防木马病毒软件等的品牌、使用数量以及与国产的比例情况 ）
2.系统硬件产品使用情况
（列表说明本单位系统硬件产品中，国内和国外小型机、服务器、交换机、路由器等信息技术产品以及防火墙、入侵检测设备等信息安全产品的硬件品牌、产品使用数量以及与国产的比例情况）
3.系统使用密码产品情况
（列表说明本单位密码产品中，国内和国外密码算法和密码产品的等品牌、使用数量以及与国产的比例情况）
4.系统服务使用情况
（说明本单位系统服务中，国内和国外信息安全服务的使用情况和比例）

填表人		**时间**	
网络安全负责人		**时间**	

.

第三章 人员安全管理

.

3.1、内部人员信息安全管理规定

3.1.1、 总则

第一条 为保障吉林省某某单位人员信息安全管理的规范性，制定本规定。

第二条 人员信息安全管理包括与信息化工作有关的人员录用、岗位人选、人员转岗和离岗、人员考核、人员惩戒、人员教育和培训等的信息安全管理。

第三条 本规定适用于吉林省某某单位。

3.1.2、 人员录用

第四条 信息安全人员录用规则遵照人事部门的人员录用管理规定执行。

第五条 录用过程中应注意以下涉及信息安全方面的要求：

（一）录用部门应明确被录用人员的信息安全技能要求，在录用过程中依据技能要求进行考察，并对技能考核结果进行记录；

（二）对于可接触较多机密或更高级别信息资产或特殊工种的人员，需要签订保密协议；

.

（三）应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议，明确应尽的信息安全保护义务，保证其在岗工作期间和离岗后一定时期内，均不得违反岗位安全协议。

3.1.3、 岗位人选

第六条 明确所有信息安全岗位人员在信息系统安全保护中的职责和权限，其工作、活动范围应当被限制在完成其任务的最小范围内。

第七条 安全管理员、安全审计员、网络管理员、系统管理员、数据库管理员、机房管理员等和信息安全有关的岗位人员，必须经过严格的审查并考核其业务能力。

3.1.4、 人员转岗和离岗

第八条 人员的转岗和离岗由所在部门及时通知人事部门，只有具备经过人事部门签字的保密承诺文档后才能办理转岗和离岗手续。

第九条 人员转岗和离岗时，需及时终止离岗人员的所有访问权限，及时变更转岗人员的访问权限。

第十条 对转岗和离岗人员，要对设备上保留的数据进行安全处理，包括备份需要留存的数据以及删除不必要的数据。

.

第十一条 对关键岗位的转岗和离岗人员需重申调离后的保密义务，要求调离人员在保密承诺文档上签字，承诺相关保密义务后方可离开。

3.1.5、 人员考核

第十二条 信息化管理处每年对所有岗位人员进行信息安全考察，内容如下：

（一）对所有人员进行信息安全意识考核；

（二）对涉及信息安全管理、检查和执行的岗位人员，将定期进行信息安全技能的考核，包括信息安全管理知识的掌握程度、所管理业务系统中安全产品的操作技能、所管理业务系统中使用的操作系统和应用软件的安全使用等；

（三）每年发生的信息安全事故、信息安全检查结果和信息安全审计结果将纳入考察内容。

第十三条 信息安全考察结果将进行存档，以便查询，及与上次考核进行对比分析。

第十四条 对于考核中发现有违反信息安全法规行为的人员或发现不适于承担信息安全关键岗位的人员要依据有关规定处理。

第十五条 信息化管理处每年还将对信息安全三大员（系统管理员、安全管理员、安全审计员）的人员进行一次工作督察，督察的内容参照《安全组织人员岗位职责》中有

关的要求执行。

3.1.6、 人员惩戒

第十六条 人员违反信息安全策略和规定时，依照信息化管理处相关规定进行处理。

第十七条 如该信息安全违规行为涉及法律层面，则将移交司法机关处理。

3.1.7、 人员教育和培训

第十八条 由信息化管理处制定培训计划，实施信息安全教育和培训工作，培训计划分层次、分阶段，循序渐进地进行。分层次培训是指对不同层次和不同岗位的人员，如对管理层（包括决策层）、安全管理员、系统管理员和所有信息安全相关人员开展有针对性和不同侧重点的培训。分阶段培训是指在信息安全管理体系的建立、实施和保持的不同阶段，实施不同的培训内容。

第十九条 新员工在正式上岗前，需进行信息安全方面的培训，明确岗位所要求遵守的信息安全管理制度、技术规范以及操作流程。

第二十条 对信息系统的维护人员和管理人员需定期开展信息安全技术教育培训（每年至少一次），明确如何安全使用有关系统，包括各业务系统、主机操作系统、电子邮

.

件系统以及计算机硬件设备等。

第二十一条 定期开展由供应商或厂家提供的专业安全技术培训，帮助相关信息安全管理人员和技术人员了解掌握正确、安全地安装、配置和维护系统。

第二十二条 在信息安全教育和培训后实行书面的考核，确认教育和培训的效果，对安全教育和培训的情况和结果记录并归档保存。

第二十三条 日常的信息安全教育和培训以内部培训为主，对于暂时没有条件实施内部培训的，可根据需要，邀请厂商、合作伙伴或者专业的培训机构实施培训。

3.1.8、 附则

第二十四条 本规定的解释权归吉林省某某单位。

第二十五条 本规定自发布之日起生效。

.

附件 3-1-1 人员录用审查考核结果记录（模板）

人员录用审查考核结果记录

基本情况					
姓名		性别		出生日期	
身高		体重		籍贯	
民族		政治面貌		婚姻状况	
身份证号		拟定部门		拟定岗位	
联系电话		家庭住址			

教育经历				
时间	毕业院校或培训机构	专业	学历	证明人

工作经历				
时间	单位	部门	岗位	证明人

家庭成员				
姓名	关系	职业	工作单位地址或现住址	联系电话

.

考核结果	
基本技能考核结果	
专业技能考核结果	
其他相关考核结果	
其他审查	
资料真实情况确认	
违纪违法情况审查	
其他相关情况审查	
审查意见	
用人部门意见及签字	
人事部门意见及签字	
主管领导意见及签字	

.

附件 3-1-2 信息系统关键岗位安全协议（模板）

（一）协议范围

本协议适用于信息化管理处从事业务、管理和技术关键岗位的人员。

（二）协议有效期限

关键岗位的任职期内。

（三）保密要求

作为关键岗位人员，我严格遵守以下保密要求：

1、 严守党和国家的秘密，认真执行《中华人民共和国保守国家秘密法》和本单位的各种保密规定。

2、 严格遵守保密人员工作守则：不该说的秘密不说；不该看的秘密不看；不该知道的秘密不问。

3、 不把党和国家的秘密透漏给家属、亲友和其他不应知道秘密的人。

- 不在私人通信和通话中涉及秘密信息；不在办公室以外的地方存放密件；个人使用的写有涉密信息的保密本要妥善保管，非保密本不记载秘密信息。
- 不在不利于保密的场合谈论有关保密设备的相关事宜。
- 未经允许，不私自与外国机关、团体、人员进行往来；与在台湾、香港、澳门及国外的亲友往来、通信，需经主管领导同意。

4、 不利用保密设备从事私人活动。

5、 外出执行任务或转移驻地时，密件亲自携带，不交于他人携带或保管。

6、 未经允许不进入安全控制区域（保密要害部门、部位），如涉密机房、领导办公室、档案室等；获准进入时，不自行翻阅文件、电报等。

7、 不在涉密机房内拍照、录音、录像。

8、 认真学习保密规定，增强保密意识，加强自觉管理。

（四）违约责任

如未遵守保密要求，我接受本单位的相关规章制度的惩罚。

.

关键岗位聘任人签字：　　日期：

关键岗位所在部门领导签字：　　日期：

.

附件 3-1-3 信息安全岗位培训计划制定要求（模板）

信息安全岗位培训计划制定要求

信息安全培训要体现层次性，对不同岗位的人员进行侧重不同的培训：

- 主管信息安全工作的高层负责人或各级管理人员的培训，其重点是掌握和了解本单位信息安全的整体策略及目标、信息安全体系的构成、安全管理机构建立和管理制度的制订。
- 负责信息安全运行管理及维护的技术人员的培训，重点是充分理解信息安全管理策略，掌握安全评估的基本方法，对安全操作和维护技术的合理运用。
- 信息系统用户的培训，其重点是学习各种安全操作规程，了解和掌握与其相关的安全策略，包括自身应该承担的安全职责。

对于特定的管理人员，提供特定的安全培训，比如负责密钥管理的人员，就应该特别注重密钥管理方面的技能培训，而对于网络服务的提供者，着重强调网络服务安全注意事项

本单位关于信息安全岗位培训工作组织实施的事宜说明如下：

1、由信息化管理处统一领导和布置工作，各部门视自己的需要和实际情况组织落实，各单位根据各自的培训内容和培训对象制定相应的岗位培训计划，培训计划需经数据管理中心审核后执行。各部门向信息化管理处报送本部门的培训计划和培训记录。

2、由信息化管理处落实面向本单位全体人员的培训工作，由各部门落实面向本部门人员的培训工作。

3、培训结束后，由信息化管理处组织考核和记录工作。

4、信息安全岗位培训计划的内容如下，请各部门视实际情况修改：

.

信息安全岗位培训计划

培训目的：通过持续、有效、层次分明、专业领先的安全培训来提升本单位工作人员的整体安全意识和技能，使工作人员养成良好的安全习惯，保证本单位信息及系统的有效使用和稳定运行，为本单位的各项工作的顺利进行起到应有的促进作用。

培训方式：培训方式主要有集中培训和指导自学两种。

培训对象（岗位）：本单位全体工作人员（包括信息安全技术岗位、管理岗位、使用岗位的人员）

培训内容：包括信息安全基础知识、本单位信息安全策略、本单位安全管理制度、岗位操作规程等

培训时间和地点：各部门自行安排

.

附件 3-1-4 人员离岗安全处理记录（模板）

人员离岗安全处理记录

基本信息			
姓名		联系方式	
部门		入职时间	
担任职位		是否关键岗位	
离岗原因		离岗时间	
交接情况			
工作交接人		交接时间	
办公物品交还情况	监督人：		
密码用品交接情况	监督人：		
账号口令更改情况	监督人：		
其他物品交还情况	监督人：		
离岗保密承诺			

.

本人了解有关保密法规制度，知悉应当承担的保密义务和法律责任。在此庄重承诺：

一、认真遵守国家保密法律法规和中电投集团保密规章制度，履行保密义务。

二、不以任何方式泄露所接触、知悉的国家秘密和商业秘密。

三、已全部清退不应由个人持有的各类国家秘密及商业秘密载体。

四、未经原单位审查批准，不擅自发表涉及原单位未公开工作内容的文章、著述。

五、自愿接受脱密期管理，自_____年___月___日至_____年____月___日服从有关部门的保密监管。

违反上述承诺，自愿承担党纪、政纪责任和法律后果。

承诺人签名：　　_____年___月___日

审批意见	
部门领导意见及签字	
人事部门意见及签字	
主管领导意见及签字	

.

附件 3-1-5 人员培训考核记录（模板）

人员培训考核记录

培训情况记录					
培训内容					
培训类型	☐基础技术 ☐安全意识 ☐防病毒 ☐应急预案 ☐系统运维				
培训日期			培训时间		
培训地点			培训人		
组织部门			考核方式		
培训记录					
效果评价					
考核结果记录					
序号	姓名	岗位	培训情况	考核结果	备注
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

.

附件 3-1-6 人员奖惩及违纪记录（模板）

人员奖惩记录

姓名	部门	奖惩事项描述	奖励				惩处			
			表扬	奖金	记功	其他	警告	罚款	记过	其他

员工违纪处理记录表

人员信息			
姓名		入职时间	
所在部门		担任岗位	
主要违纪事实			
处理意见			
所在部门处理意见	部门领导签字：　　年　月　日		
人事部门意见	部门领导签字：　　年　月　日		
相关领导意见	部门领导签字：　　年　月　日		

.

3.2、外部人员访问信息安全管理规定

3.2.1、 总则

第一条 为有效防范外部人员访问带来的信息安全风险，加强和规范外来人员的信息安全管理，保证信息资源的安全，制定本规定。

第二条 本规定适用于吉林省某某单位。

3.2.2、 定义

第三条 本规定所述的外部人员包括软件开发商、产品供应商、系统集成商、设备维护商、服务提供商以及外单位借调人员和挂职人员等外来人员(写到内部人员管理制度中去)，外部人员分为临时外部人员和非临时外部人员。

第四条 临时外部人员指因业务洽谈、技术交流、提供短期和不频繁的技术支持服务而临时来访的外部人员。

第五条 非临时外部人员指因从事合作开发、参与项目工程、提供技术支持、顾问服务及外单位借调人员和挂职人员等外来人员，是必须在吉林省某某单位长期办公的外部人员。

.

3.2.3、 外部人员访问信息安全管理

第六条 外部人员的访问方式包括现场访问和远程网络访问。

第七条 接待人是指吉林省某某单位受访部门派出的，负责接待外部人员的接口人。

第八条 临时外部人员访问重要信息资源所在物理区域（如机房、重要服务器或设备等），需获准后方可进入。

第九条 接待人必须全程陪同临时外部人员，告知有关安全管理规定，不应透露与外部工作无关的信息，不得任其自行走动和未经允许使用吉林省某某单位的计算机设备。

第十条 非临时外部人员，由接待部门提出申请，信息化管理处出具意见，向保卫部门提出申请，信息化管理处依照保卫部门审批结果办理工作手续。

第十一条 原则上禁止外部人员携带的电脑接入吉林省某某单位网络，如因工作需要（如软件开发测试）接入吉林省某某单位网络，必须向信息化管理处申请，并使用信息化管理处的设备或经过信息化管理处检查认可的设备。

第十二条 第三方人员如有需要访问信息时，需要依照如下几个阶段进行：

1、 访问申请阶段，接待人根据第三方人员实际需要提出某时间段内访问网络、主机等相关信息的申请；

2、 审批申请阶段，接待人所属部门管理者审批申请。

.

审批后备案；

3、 注销访问阶段，第三方人员访问结束，接待人终止访问申请，并备案；

第十三条 不允许外部人员进行远程网络访问。如确因维护需要远程访问，必须上报审批后方可进行。

第十四条 外部人员开发测试环境只能连接开发网，且必需采用防火墙进行有效隔离，严禁接入生产网。确需在线测试的项目，应上报分管领导批准，采取必要的防护措施，选择适当的时间进行。

第十五条 外部人员在机房内的所有操作，都必需说明该操作可能引起的安全风险，并由接待人确认后才能操作。接待人必须对外部人员的操作进行全程监控，记录外部人员的操作内容并存档备案。

第十六条 必须定期评估外部人员带来的安全风险，至少每年评估一次。必须防范外部人员带来的以下安全风险：

1、 外部人员的物理访问带来的设备、资料盗窃；

2、 外部人员的误操作导致各种软硬件故障；

3、 外部人员的资料、信息外传导致泄密；

4、 外部人员对计算机系统的滥用和越权访问；

5、 外部人员给计算机系统、软件留下后门；

6、 外部人员对计算机系统的恶意攻击。

.

3.2.4、 第三方安全要求

第十七条 非临时外部人员必须签署安全保密协议（加一个附件）后才能进场工作。禁止外部人员试图了解和查阅与工作无关的吉林省某某单位资料以及访问与工作无关的信息系统，外部人员如因业务需要查阅吉林省某某单位资料或访问吉林省某某单位信息系统，必须获得相关负责人批准并详细登记，并确认已与信息化管理处签署有效的保密协议。

第十八条 未经批准，禁止外部人员携带移动存储介质进入吉林省某某单位，移动存储介质必须在接待人的监控下使用。

第十九条 未经相关负责人特别许可，外部人员不得在办公区域和机房内摄影、拍照。

3.2.5、 附则

第二十条 本规定的解释权归吉林省某某单位。

第二十一条 本规定自发布之日起生效。

.

第四章 系统建设管理

.

4.1、定级备案管理规定

4.1.1、 总则

第一条 为规范吉林省吉林省某某单位信息系统定级备案管理，制定本规定。

第二条 本规定适用于吉林省吉林省某某单位，适用于吉林省吉林省某某单位拟建、在建以及运行的非涉密重要信息系统。

4.1.2、 定义

第三条 信息系统的安全保护等级分为以下五级

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

.

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

第四条 名词定义

业务部门:信息系统的使用部门。

业务信息安全：从业务信息安全角度反映的信息系统安全。

系统服务安全：从系统服务安全角度反映的信息系统安全。

受侵害客体：等级保护对象受到破坏时所侵害的客体包括以下三个方面：

a)公民、法人和其他组织的合法权益；

b)社会秩序、公共利益；

c)国家安全。

对客体的侵害程度：等级保护对象受到破坏后对客体造成侵害的程度有造成一般损害、造成严重损害和造成特别严重损害。

一般损害：工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题，较低的财产损失，有限的社会不良影响，对其他组织和个人造成较低损害。

严重损害：工作职能受到严重影响，业务能力显著下降且严重影响主要功能执行，出现较严重的法律问题，较高的

财产损失，较大范围的社会不良影响，对其他组织和个人造成较严重损害。

特别严重损害：工作职能受到特别严重影响或丧失行使能力，业务能力严重下降且或功能无法执行，出现极其严重的法律问题，极高的财产损失，大范围的社会不良影响，对其他组织和个人造成非常严重损害。

第五条 角色定义

应用系统负责人：由业务部门为每个信息系统指定的定级备案工作负责人；

系统定级管理负责人：由信息化管理处指定的定级备案负责人。

4.1.3、 岗位及职责

第六条 业务部门：应对待定级系统指定应用系统负责人，对待建、在建和已建信息系统根据等级保护相关要求进行定级，并完成定级报告。

第七条 信息化管理处：吉林省吉林省某某单位网络安全与信息化工作领导小组办公室指定系统定级管理负责人，完成定级备案表，并报吉林省吉林省某某单位网络安全与信息化工作领导小组审核，审核通过后报公安机关备案。

.

4.1.4、 系统定级方法

第八条 信息系统定级方法如图所示：

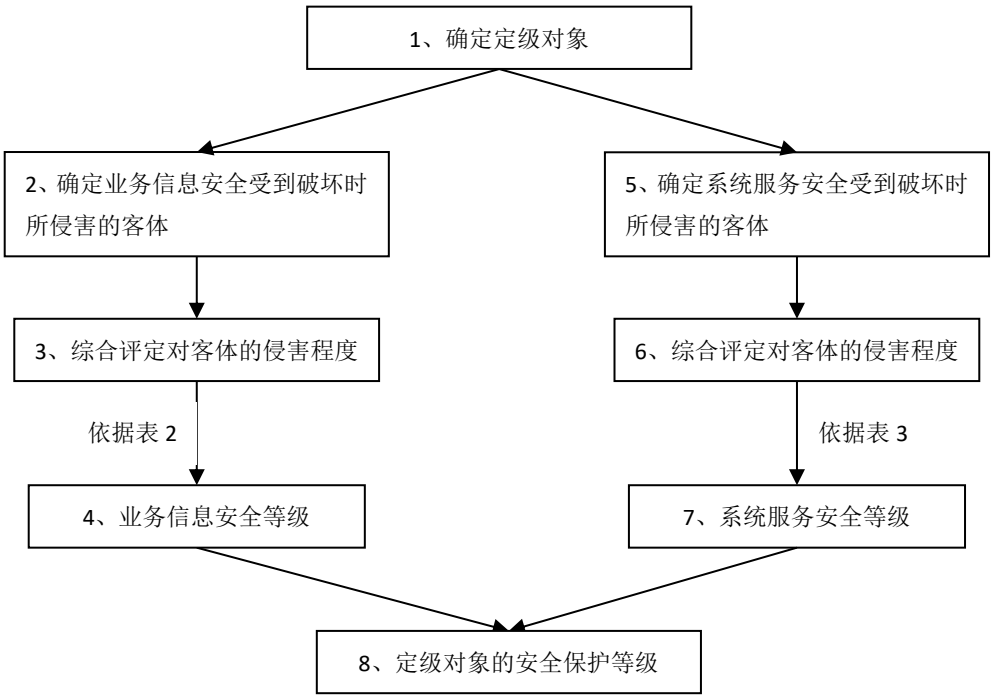

图 1 信息系统定级方法图

第九条 信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度，定级要素与信息系统安全保护等级的关系如表 1 所示：

表1 业务信息安全保护等级矩阵表

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

第十条 信息系统安全包括业务信息安全和系统服务安全，与之相关的受侵害客体和对客体的侵害程度可能不同，

.

因此，信息系统定级应由业务信息安全和系统服务安全两方面确定。

第十一条 根据业务信息安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据表 2 业务信息安全保护等级矩阵表，即可得到业务信息安全保护等级。

表2 业务信息安全保护等级矩阵表

业务信息安全被破坏时所受侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

第十二条 根据系统服务安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据表 3 系统服务安全保护等级矩阵表，即可得到系统服务安全保护等级。

表3 系统服务安全保护等级矩阵表

系统服务安全被破坏时所受侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

4.1.5、 系统定级备案管理

第十三条 吉林省吉林省某某单位应按《信息安全等级保护管理办法》(公通字【2007】43 号)和《GB/T 22240—2008 信息安全技术信息系统安全等级保护定级指南》的要求进行

.

信息系统的定级、设计、建设、测评、备案和变更管理，具体的定级备案工作由信息化管理处和业务需求单位共同负责。

第十四条 吉林省吉林省某某单位信息系统定级遵循“自主定级”的原则，由业务部门进行自主定级，吉林省吉林省某某单位信息系统安全保护等级一般为第二级或第三级，如因特殊情况需定级为第四级或以上，需由信息化管理处确认。

第十五条 信息系统定级流程如下：

(一) 应用系统负责人应参照相关标准填写《信息系统安全等级保护定级报告》，完成自主定级，报告应中明确信息系统安全保护等级，详细说明定级的方法和理由，定级方法详见第 4.1.4 节内容。

(二) 业务部门完成自主定级后，将《信息系统安全等级保护定级报告》提交信息化管理处进行存档，并将定级结果报信息安全领导小组审核。

(三) 由信息化管理处协助业务部门组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定，并对专家论证文档进行保存，记录专家对定级结果的论证意见。

(四) 如安全技术专家对信息系统定级结果的合理性和正确性存在异议，则由业务部门、信息化管理处和技术专家组

.

共同讨论确认信息系统的安全保护等级，并由业务部门根据最终的论证意见重新填写《信息系统安全等级保护定级报告》。

(五) 如安全技术专家对信息系统定级结果的合理性和正确性无异议，则由吉林省吉林省某某单位网络安全与信息化工作领导小组办公室，指定的定级管理负责人根据《信息系统安全等级保护备案表》中填表说明填写《备案表》，并进行备案工作。

第十六条 信息系统备案流程如下：

(一) 定级管理负责人进行信息系统备案时应当提交公安机关公共信息网络安全监察部门《备案表》（一式两份）及其电子文档。第二级及以上信息系统备案时需提交《备案表》中的表一、二、三；第三级及以上信息系统还应当在系统整改、测评完成后 30 日内提交《备案表》表四以及其相关材料；

(二) 备案资料经公安机关公共信息网络安全监察部门审核通过后，定级管理负责人会收到由公安机关公共信息网络安全监察部门出具的《信息系统安全等级保护备案材料接收回执》；

(三) 公安机关公共信息网络安全监察部门审核后认定备案资料不齐全的，会在当场或者在五日内一次性告知定级管理负责人其补正内容，定级管理负责人应根据公安机关公共

.

信息网络安全监察部门告知的补正内容补齐相关资料，并提交公安机关公共信息网络安全监察部门；

（四）备案材料经公安机关公共信息网络安全监察部门审核通过后，定级管理负责人会在递交材料的十个工作日内收到加盖公安机关印章（或等级保护专用章）的《备案表》一份；

（五）备案材料经公安机关公共信息网络安全监察部门审核未通过，认为其不符合等级保护要求的，公安机关公共信息网络安全监察部门会在十个工作日内通知定级管理负责人进行相应整改，并向定级管理负责人出具《信息系统安全等级保护备案审核结果通知》。

（六）定级管理负责人收到公安机关公共信息网络安全监察部门出具的由公安部统一监制《信息系统安全等级保护备案证明》后，信息系统备案工作结束。

第十七条 每个信息系统相应的应用系统负责人都应在信息化管理处进行登记，如应用系统负责人发生变更，业务部门应及时通知信息化管理处对人员信息进行变更。

第十八条 应用系统负责人有义务配合信息化管理处以及公安部进行信息安全等级保护检查工作。

第十九条 拟建以及在建的重要信息系统在投入使用前应按本规定进行信息系统定级，并且在信息系统投入使用后，应当按要求和程序进行该信息系统安全等级备案工作。

.

第二十条 信息系统发生重大变更导致系统安全保护等级变化时，信息化管理处和业务部门应重新确定信息系统的安全保护等级，按相应程序报备，并按新的等级要求调整保护措施。

.

附件 4-1-1 系统定级结果评审及审批意见（模板）

系统定级结果评审及审批意见

信息系统基本信息					
序号	系统名称	系统级别	资料准备		
			定级报告	备案表	其他附件
1					
2					
3					
4					
5					

评审记录			
评审专家	所在单位	联系方式	评审意见

审批意见	
信息安全负责人审批意见	负责人签字：　　_____年___月___日
网络安全与信息化工作领导小组审批意见	负责人签字：　　_____年___月___日
主管部门审批意见	

.

	负责人签字：　　年　月　日

.

4.2、信息安全方案设计管理规定

4.2.1、 总则

第一条 为规范吉林省某某单位信息系统安全方案的设计管理，制定本规定。

第二条 吉林省某某单位信息系统安全方案应参考国家信息安全相关标准的要求进行设计。

第三条 本规定适用于吉林省某某单位。

4.2.2、 安全建设总体规划责任部门

第四条 吉林省某某单位网络安全与信息化工作领导小组负责对吉林省某某单位信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划。

4.2.3、 安全方案的设计和评审

第五条 吉林省某某单位信息化管理处应根据信息系统的安全保护等级选择相应的基本安全措施，并依据风险分析的结果补充和调整安全措施。

第六条 信息系统的安全保护等级确定后，信息化管理处应选择具有相应资质的单位，依照国家信息安全等级保护管理规范和技术标准进行安全方案设计。

.

第七条 信息安全方案应包括安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案等相关配套文件。

第八条 信息安全方案设计完成后，信息化管理处应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，记录专家论证意见。

第九条 信息安全方案经过信息吉林省某某单位网络安全与信息化工作领导小组批准后，才能正式实施。

4.2.4、 安全方案的调整和修订

第十条 由信息化管理处根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

第十一条 信息化管理处应维护信息安全方案相关配套文件的历史版本和修订版本，并有维护记录。

4.2.5、 附则

第十二条 本规定的解释权归吉林省某某单位。

第十三条 本规定自发布之日起生效。

.

附件 4-2-1 安全方案评审及审批意见（模板）

安全方案评审及审批意见

安全方案基本信息			
方案名称			
编制单位		编制人员	
编制时间		评审类型	□新建 □修订 □变更
所属项目			
内容简介			
相关附件			

评审记录			
评审专家	所在单位	联系方式	评审意见

审批意见	
信息安全负责人审批意见	负责人签字： _____年___月___日
网络安全与信息化工作领导小组审批意见	负责人签字： _____年___月___日

.

主管部门审批意见	负责人签字：　　_____年___月___日

.

4.3、产品采购和使用信息安全管理规定

4.3.1、 总则

第一条 为规范吉林省某某单位在信息系统产品采购和使用中信息安全有关的事项，制定本规定。

第二条 吉林省某某单位按国家信息安全相关政策法规和标准的规定进行信息系统产品的采购和使用。

第三条 本规定适用于吉林省某某单位。

4.3.2、 产品采购和使用

第四条 吉林省某某单位的信息技术产品的采购由数据管理中心统一负责。

第五条 吉林省某某单位的信息化产品采购活动需要符合国家信息安全政策要求，特别是信息安全产品必须要有资质证明。

第六条 吉林省某某单位应按照《中华人民共和国招标投标法》和《中华人民共和国政府采购法》的有关规定，优先选择国产自主可控的信息安全设备、核心网络设备、基础软件、系统软件和业务应用软件等关键产品，以确保信息系统的安全可控。因特殊原因必须选用国外信息技术产品的，应请国家有关部门进行安全审查，并报吉林省某某单位网络

.

安全与信息化工作领导小组批准。

第七条 采购信息安全产品时，吉林省某某单位将要求产品研制、生产单位提供相关材料，包括：营业执照、产品的版权或专利证书、提供的声明和通过国家认定的信息安全产品检测实验室的检测证明以及计算机信息系统安全专用产品销售许可证等材料。

第八条 信息系统安全等级为三级（以上）信息系统在选择信息安全产品时，除遵守以上规定外，还应当符合以下条件：

（一）产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格；

（二）产品的核心技术、关键部件具有我国自主知识产权；

（三）产品研制、生产单位及其主要业务、技术人员无犯罪记录；

（四）产品研制、生产单位声明其产品没有故意留有或者设置漏洞、后门、木马等程序；

（五）对已列入信息安全产品认证目录的，应当取得国家信息安全产品认证机构颁发的认证证书。

第九条 产品采购到货后，信息化管理处组织验收小组对供货方的货物进行技术方面的验收，验收时候需要查验产品

.

的各种文档、证书、报告及证明文件，确认符合前述各条款规定。

4.3.3、 产品采购清单的维护

第十条 信息化管理处预先对产品进行选型测试，确定产品候选范围，并定期审定和更新候选产品名单。

第十一条 信息化管理处根据产品的更新换代情况每年对产品采购候选清单进行审定和更新。

4.3.4、 附则

第十二条 本规定的解释权归吉林省某某单位。

第十三条 本规定自发布之日起生效。

.

附件 4-3-1 安全产品采购记录（模板）

安全产品采购记录

产品基本信息			
产品名称		**产品编号**	
生产厂家		**供货单位**	
品牌名称		**规格型号**	
项目归属		**质量保证期**	
采购部门		**采购人**	
采购数量		**采购时间**	
采购单价		**采购总价**	
产品类型	☐安全产品　☐密码产品　☐存储介质　☐其他产品		
详细参数			

检验测试记录			
序号	**检验项目**	**检验测试结果**	**备注**
1	产品数量		
2	规格型号		
3	产品外观		
4	产品质量		
5	合格证（材质单）		
6	前期选型测试		
7	备用产品信息		

人员签字			
检验人员		**检验时间**	

.

负责人签字		**审批时间**	

.

附件 4-3-2 候选产品清单（模板）

候选产品清单

序号	产品类型	候选产品名称	品牌	型号	测试情况
1	核心交换机	1）			
		2）			
2	接入交换机	1）			
		2）			
3	路由器	1）			
		2）			
4	防火墙	1）			
		2）			
5	入侵检测	1）			
		2）			
6	防毒墙	1）			
		2）			
7	日志审计	1）			
		2）			
8	数据库审计	1）			
		2）			
9	防病毒软件	1）			
		2）			
10	堡垒机	1）			
		2）			
11	漏洞扫描	1）			
		2）			
12	安全准入	1）			
		2）			
13	VPN	1）			
		2）			
14	上网行为管理	1）			
		2）			
15	身份认证系统	1）			
		2）			
16	网闸	1）			
		2）			
候选产品清单审定情况					
审定人			审定时间		

.

4.4、信息系统自行软件开发管理规定

4.4.1、 总则

第一条 为规范吉林省某某单位自行软件开发管理，制定本规定。

第二条 本规定适用于吉林省某某单位。

4.4.2、 自行软件开发管理

第三条 确保开发、测试与运行设备的分离。

第四条 信息化管理处对项目参与人员进行信息安全意识培训。

第五条 软件需求分析阶段，必须明确地定义和商定新系统的要求和准则，并形成文件，便于后期验收。相关安全需求的要求和准则应包括：

(一) 用户管理；

(二) 权限管理；

(三) 日志管理和数据管理（存储、传输）。

第六条 在系统设计时，应该考虑系统的容量和资源的可用性，以减少系统过载的风险，如数据库容量、并发连接数、带宽、内存、CPU、硬盘大小以及其他可能因素，并应采取相应的保密措施，控制涉及核心数据软件设计相关资料的使

.

用范围。

第七条 对系统层面上的和模块层面上的安全设计进行审查。

第八条 确认各模块的设计，以及模块间的接口设计能满足系统层面的安全要求。

第九条 软件编码阶段对源代码安全控制如下：

(一) 减少源代码被破坏和非授权访问的可能，对源代码的访问权限应进行严格控制；

(二) 为了保障源代码的安全，要求开发设备与测试设备和运行设备进行分离，运行设备上只有执行代码；

(三) 应注释代码中无用的代码；

(四) 旧源程序版本应被保存，并对代码进行版本控制，确保代码的可用；

(五) 对代码的访问权限进行严格的权限控制；

(六) 所有运行代码库的修改、更新都要有操作日志记录。

第十条 软件编码阶段对数据安全控制如下：

(一) 原则上不允许使用真实数据进行测试，特殊情况需要使用真实测试数据时，需要对系统测试数据进行安全保护；

(二) 测试环境与生产环境分离；

(三) 将测试数据和生产数据相分离；

(四) 测试过程中，应对测试数据进行安全保护；

.

（五）测试完成之后，应立即将测试数据从测试系统中删除。

第十一条 为了降低开发过程中变更的风险，应考虑以下有关内容：

（一）确保由授权用户提交变更申请；

（二）保留变更的授权级别记录；

（三）审查变更控制措施和流程的完整性，确保未被修改和破坏；

（四）及时发布操作系统的变更通知；

（五）在实施之前，详细的变更方案必须获得正式审批、批准；

（六）在实施之前，确保授权用户接受变更；

（七）选择恰当的变更时间，确保在具体实施过程中最大限度地减少业务影响；

（八）确保系统文档在每次修改后得到及时更新，并确保旧文档被正确归档和处置；

（九）保留所有变更的审计跟踪记录；

（十）确保及时更新业务连续性计划。

第十二条 确保系统应用程序的输入数据安全，通过数据输入检测下列有关错误：

（一）超范围的数值；

（二）数据域中的无效字符；

.

(三) 遗漏的或者不完整的数据；

(四) 超出数据容量的上下限；

(五) 未经授权或者不一致的控制数据；

(六) 对合法性输入错误应有相关提示。

第十三条 要确保系统应用的数据完整性安全，防止信息在处理过程中被篡改。

第十四条 要确保系统应用的输出数据准确，检查输出数据，保证正确处理储存信息：

(一) 模糊性检查测试输出数据是否合理；

(二) 测试、验证、核实输出的相关结果提示。

第十五条 软件开发的整个过程的各阶段都应有开发文档的输出，内容包括：

(一) 开发各阶段输出的文档应有相应的安全性方面的内容；

(二) 需求说明书中应明确描述用户的安全需求；

(三) 设计中应有针对安全性需求的设计，并需要经过评审；

(四) 在测试大纲或者测试方案中应有安全性测试方案，并以此进行安全性测试；

(五) 文档应设定密级及传阅范围，以限定其访问范围；

(六) 文档的访问控制应有相应的授权审批机制；

(七) 文档作为软件开发中的配置项，应遵循软件配置管

理要求。

第十六条 软件开发之前，应对参与开发的所有人员进行保密教育，并签署保密协议，以规范开发人员的行为。

第十七条 软件开发过程中，应将开发人员与测试人员分离。

第十八条 项目验收到须得到各业务部门、吉林省某某单位网络安全与信息化工作领导小组办公室共同确认签字验收。

第十九条 项目应达到项目任务书中制定的总体安全目标和安全指标，实现全部安全功能。

第二十条 验收报告中应包括项目设计总体安全目标及主要内容。

第二十一条 验收报告中应包括项目采用的关键安全技术内容。

第二十二条 系统验收并移交后，必须立即修改系统中相关的口令。

4.4.3、 附则

第二十三条 本规定的解释权归吉林省某某单位。

第二十四条 本规定自发布之日起生效。

.

4.5、信息系统外包软件开发管理规定

4.5.1、 总则

第一条 为规范吉林省某某单位外包软件开发管理，制定本规定。

第二条 本规定适用于吉林省某某单位。

4.5.2、 外包软件开发管理

第三条 由各业务部门提出信息系统软件开发需求，信息化管理处按照规定程序确定外包开发单位，并在信息化管理处内部指定专人负责软件开发过程中与业务部门、开发单位的沟通及软件交付后的维护工作。

第四条 通过规定程序取得信息系统开发资格的单位，应依照国家信息安全政策法规和技术标准中关于应用安全的要求，设计、建设符合相应安全保护等级要求的应用系统。

第五条 信息系统的开发必须符合软件工程规范，并在软件开发的各阶段按照安全管理目标进行管理和实施。计算机信息系统的开发人员或参加开发的协作单位应经过严格资格审查，并签订保密协议书，承诺其负有的安全保密责任和义务。

.

第六条 开发单位完成建设任务后，需向建设使用单位移交完整的信息系统开发过程文档资料，包括需求分析说明书、软件设计说明书、软件程序源代码、系统安装光盘、系统安装手册、系统管理手册和软件操作手册（包括：纸质和光盘介质）等。

第七条 外包开发的软件在交付前，由信息化管理处组织验收小组依据开发要求的技术指标对软件功能和性能进行验收测试。

第八条 测试环境必须使用信息化管理处认可的硬件设备环境，在建设使用单位认可的测试场地进行。禁止使用实际数据作为测试数据。

第九条 外包开发的软件在安装之前，由信息化管理处组织技术力量采用第三方的商业检测工具检测软件中的恶意代码，并根据开发单位提供的源代码对软件中可能存在的后门进行审查，记录审查结果。

第十条 应用系统开发完成后应经过至少一个月的试运行，经立项主管部门领导审批后才能投入正式使用。

第十一条 应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要。

第十二条 应要求外包服务商每年至少开展一次信息安全风险评估并提交评估报告，应要求外包服务商聘请外部机

.

构定期对其进行安全审计并提交审计报告，督促其及时整改发现的问题；

第十三条 应制定外包服务商应急计划，以应对外包服务商破产、不可抗力或其它潜在问题导致服务中断或服务水平下降的情形，保障信息系统连续、可靠运行。

4.5.3、 附则

第十四条 本规定的解释权归吉林省某某单位。

第十五条 本规定自发布之日起生效。

.

4.6、信息系统工程实施安全管理制度

4.6.1、 总则

第一条 为规范吉林省某某单位信息系统工程（以下本文件所涉及的“工程”均指吉林省某某单位信息系统工程）实施管理，制定本制度。

第二条 吉林省某某单位应按国家相关信息安全相关政策法规和标准的规定进行信息系统工程实施管理。

第三条 本制度适用于吉林省某某单位。

4.6.2、 工程实施管理

第四条 由信息化管理处负责信息系统工程实施过程的管理工作。

第五条 工程实施单位应提供其能够安全实施信息系统建设的资质证明和能力保证。

第六条 在工程实施之前，由工程实施单位制定详细的工程实施方案，实施方案需要经信息安全领导小组批准认可后方可实施。

第七条 工程实施方案应包括工程时间限制、进度控制和质量控制等方面内容。

.

第八条 工程实施单位在实际工程实施中应按照工程实施方案内容对工程实施过程进行进度和质量控制，并定期向信息化管理处提交阶段性工程报告等文档。

第九条 由工程实施单位和监理单位共同制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则，管理制度需要得到信息化管理处的批准。

4.6.3、 实施过程控制方法

第十条 在工程实施过程中，使用主动控制的方法：

(一) 预测和估计潜在的风险，在问题发生之前采取有效的防范措施；

(二) 评价项目的现状和进展趋势，分析其影响并提出建设性意见；

(三) 对项目状态持续不断的跟踪、监测，有效而经济地预防意外事故。

第十一条 在确定项目总目标和阶段目标并开始按计划实施后，进入项目控制期。项目经理要始终不断明确以下关键问题：

(一) 项目目前处于什么阶段；

(二) 项目的最终和本阶段目标是什么；

(三) 怎样做才能实现项目目标；

(四) 现在采取的措施是否都是正确的。

.

第十二条 项目进度控制措施如下：

(一) 组织措施

1. 明确项目控制人员的具体职责；
2. 进行项目工作结构的分解，创建项目工作控制基线及项目控制时间；
3. 确定项目进度工作制度和工作计划，如项目每周例行会议。

(二) 经济措施：确保项目资金的提供；

(三) 信息管理：

1. 对影响项目进度的干扰和风险因素进行分析；
2. 进行计划进度和实际进度的比较；
3. 定期制作各种进度情况报告。

第十三条 质量控制的关键：

(一) 加强质量意识：提高所有实施人员特别是负责人的质量意识，认识到质量是项目成功与否的关键。

(二) 明确质量责任：项目经理及有关部门负责人和项目组成员都要明确自己在保证项目质量工作中的责任。

(三) 提高人员素质：选择满足实施需求且高质量的人员组建项目组。

(四) 制定质量标准：建立一套完整的质量标准化体系，根据项目计划工作内容由责任人逐一制定。

第十四条 项目质量的保证措施：

.

(一) 项目总体目标明确、清晰、量化。如果项目实施过程发生变化，要重新考虑项目目标。

(二) 将项目总体目标分解为阶段目标，并将工作任务分解为最小单位。

(三) 根据工作任务，在计划中设定检查控制点

(四) 对每项工作任务进行评价,并对各种问题进行总结。

(五) 评价整个项目。评价总结工作在项目结束后进行，目的是系统地分析项目工作成果是否达到了项目目标的要求。

第十五条 项目风险控制和管理：

(一) 风险识别：确定各阶段工作的风险种类、对项目的影响；

(二) 风险量化：对风险及风险产生的影响进行评估；

(三) 应对计划：制定风险管理计划，采取措施增大制约风险的机会；

(四) 风险控制：不断对风险管理计划进行更新，并对风险因素采取预防和纠正措施。

第十六条 项目执行过程中为了保障项目在预期的目标（进度、质量/范围、成本）范围内完成，必须严格执行项目计划，尽量避免项目需求变更和人员变更。如果出现不可预知的因素导致项目变更，必须及时调整项目目标、项目计划，并通知工程管理人员，由其签字确认。

.

第十七条 项目经理应根据项目计划的关键路线图，在项目执行过程中关注关键路线的执行情况。针对项目中出现的变更采用补救、更新计划等方式进行处理。

4.6.4、 实施人员行为准则

第十八条 工程开通和维护要严格按照工程规范的要求进行。

第十九条 规范施工、文明施工，严禁马虎作业。

第二十条 进入机房施工须征得机房管理员同意，按照外来人员访问管理规定执行。

第二十一条 在机房和办公场所工作时，要严格遵守吉林省某某单位的各项规章制度。

第二十二条 对设备进行维护操作时，须经部相关部门主管人员认可，并在部相关人员陪同下进行。

第二十三条 对设备硬件进行操作注意要有防静电措施。

第二十四条 在部内网计算机上不允许使用未经授权的存储介质（U 盘、光盘、硬盘等）。

第二十五条 携带物品进入机房须征求机房值班人员和信息化管理处主管的同意，并放置在指定位置，不可随意乱放。

第二十六条 实施人员每天工作结束后,要清理工作现

.

场,保持机房整洁。

第二十七条 严禁擅自使用办公电话，如确实需要，须经相应部门人员同意后方可使用。

第二十八条 严禁在机房或办公场所内吸烟、玩游戏和乱动其它厂家设备。

4.6.5、 附则

第二十九条 本制度的解释权归吉林省某某单位。

第三十条 本制度自发布之日起生效。

.

附件 4-6-1 工程测试验收评审及审批意见（模板）

工程测试验收评审及审批意见

工程项目基本信息			
项目名称			
承建单位		**单位地址**	
项目负责人		**联系电话**	
实施时间		**项目类型**	□工程 □网络 □软件
所属项目			
评审内容			
相关附件	1）施工方案： 2）验收报告： 3）其他资料：		

评审记录			
评审人员	**单位/部门**	**联系方式**	**评审意见**

审批意见	
信息安全负责人审批意见	负责人签字：　　年　月　日
网络安全与信息化工作领导小组审批意见	负责人签字：　　年　月　日
主管部门审批意见	

.

	负责人签字：　　年　月　日

.

4.7、信息系统测试验收安全管理规定

4.7.1、 总则

第一条 为规范吉林省某某单位信息系统测试验收管理，制定本规定。

第二条 吉林省某某单位应按国家信息安全相关政策法规和标准的规定进行信息系统测试验收管理工作。

第三条 本规定适用于吉林省某某单位。

4.7.2、 测试验收管理

第四条 由信息化管理处组织验收小组负责信息系统测试验收，并按照本管理规定的要求完成系统测试验收工作。

第五条 由吉林省某某单位委托具备国家相关技术资质和安全资质的第三方测试机构对系统进行安全性测试，并出具安全性测试报告。

第六条 在测试验收前由第三方测试机构根据设计方案或合同要求等制订测试验收方案，《测试验收方案》的内容包括：

（一） 测试策略：描述测试策略；

（二） 测试描述：包括测试环境、测试人员安排、测试

.

方法和测试时间安排等；

（三） 测试规定：包括环境准备、数据准备、测试人员行为准则和测试用例准备等；

（四） 可交付件：测试完成后，提交测试日志、缺陷报告和测试报告等。

第七条 吉林省某某单位网络安全与信息化工作领导小组对第三方测试机构提交的《测试验收方案》进行审定，审定通过后按《测试验收方案》开展测试活动。在测试验收过程中应详细记录测试验收结果，并形成测试验收报告。

第八条 测试验收报告中需要给出测试是否通过的结论，如果报告中提出了存在的问题，则同时还需要提供针对这些问题的改进报告。测试报告和改进报告都需要有第三方测试机构的签字或盖章。

第九条 由信息化管理处组织验收小组对系统测试验收报告进行审定，并签字确认。

第十条 信息系统验收完成后，信息化管理处应明确负责信息系统的运行维护工作的责任人，明确岗位安全责任。

第十一条 信息化管理处认真做好信息系统建设项目的档案建设工作，建设完成后及时移交相关部门。

4.7.3、 测试验收控制方法

第十二条 由测试负责人组织测试人员准备测试环境，

.

并进行系统测试。

第十三条 由测试人员根据《测试验收方案》中的测试用例对系统进行测试。

第十四条 测试人员在测试过程中填写《测试用例表》，并将发现的问题及时交给实施单位，并令其在一定期限内修改完毕。

第十五条 根据实际情况可以对系统进行初步测试验收【初验】和最终测试验收【终验】。测试验收全部完成后由测试人员根据测试情况编制《测试验收报告》，《测试验收报告》由验收小组负责审核批准。

第十六条 软件产品需要通过单元测试、集成测试和系统测试。

4.7.4、 测试人员行为准则

第十七条 测试人员严格按照《测试验收方案》中规定的时间进场开展测试。

第十八条 测试人员严格按照测试规范执行各项测试活动。

4.7.5、 附则

第十九条 本规定的解释权归吉林省某某单位。

第二十条 本规定自发布之日起生效。

.

4.8、信息系统交付安全管理规定

4.8.1、 总则

第一条 为规范吉林省某某单位信息系统的交付管理，制定本规定。

第二条 吉林省某某单位应按国家信息安全相关政策法规和标准的规定进行信息系统交付管理工作。

第三条 本规定适用于吉林省某某单位。

4.8.2、 交付管理

第四条 由信息化管理处负责系统交付的管理工作，并按照本管理规定的要求完成系统交付工作。

第五条 工程验收完成后，由信息化管理处督促工程实施单位提供详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点，确保工程实施单位提供系统建设过程中的文档和指导用户进行系统运行维护的文档。

第六条 工程实施单位应对信息化管理处负责系统运行维护的技术人员进行相应的技能培训，并对培训情况进行记录，包括培训内容、培训时间和参与人员等。

.

4.8.3、 系统交付的控制方法

第七条 系统试运行完成后，工程实施单位项目经理参照项目合同及项目实施计划，判断项目现状是否达到需方要求以及项目是否可进入验收阶段。

第八条 若验收条件满足，由工程实施单位项目经理出面与信息化管理处共同拟定《系统验收计划》，同时，工程实施单位项目经理填写《项目验收申请表》、《系统交付清单》，提交信息化管理处审批。

第九条 信息化管理处确认《系统验收计划》和《系统交付清单》后，工程实施单位派出代表和验收小组、监理单位一起进行项目验收工作。

第十条 项目验收过程中，工程实施单位项目经理应详细记录问题。对于验收过程中出现的问题，实施单位项目经理应安排实施人员对项目进行修改和完善，并取得验收小组认可。

第十一条 项目验收完毕后，验收小组在《项目验收报告》上签字确认。

第十二条 项目验收完毕，工程实施单位应组织项目组执行系统交付工作，按《系统交付清单》提交交付物，并为信息化管理处负责系统运行维护的技术人员提供相应的技能培训。

.

4.8.4、 参与人员行为准则

第十三条 参与系统交付的工程实施单位人员应严格按照《系统交付清单》准备交接的设备、软件和文档等。

第十四条 参与系统交付的信息化管理处人员根据《系统交付清单》对交付物进行逐项清点，发现问题及时与工程实施单位人员沟通。

4.8.5、 附则

第十五条 本规定的解释权归吉林省某某单位。

第十六条 本规定自发布之日起生效。

.

4.9、信息系统等级测评管理规定

4.9.1、 总则

第一条 为规范吉林省某某单位信息系统等级测评管理工作，特制定本规定。

第二条 本规定适用于吉林省某某单位。

第三条 吉林省某某单位按国家信息安全相关政策法规和标准的规定进行信息系统等级测评管理工作。

4.9.2、 等级测评管理

第四条 由信息化管理处负责吉林省某某单位信息系统等级测评管理工作。

第五条 选择具有国家相关技术资质和安全资质的测评单位进行等级测评。

第六条 安全等级为第三级（含）以上的信息系统应当选择符合下列条件的等级保护测评机构进行测评,第二级信息系统系统可以参照第三级系统要求，自主选择测评机构。

（一） 在中华人民共和国境内注册成立（港澳台地区除外）;

（二） 由中国公民投资、中国法人投资或者国家投资的

.

企事业单位（港澳台地区除外）；

（三） 从事相关检测评估工作两年以上，无违法记录；

（四） 工作人员仅限于中国公民；

（五） 法人及主要业务、技术人员无犯罪记录；

（六） 使用的技术装备、设施应当符合本办法对信息安全产品的要求；

（七） 具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度。

第七条 在信息系统运行过程中，第三级信息系统应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的应及时整改；第二级信息系统自主决定测评频率。

第八条 在系统发生变更时及时对系统进行信息系统等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改。

4.9.3、 附则

第九条 本规定的解释权归吉林省某某单位。

第十条 本规定自发布之日起生效。

.

4.10、 信息系统安全服务商选择管理办法

4.10.1、 总则

第一条 为规范吉林省某某单位信息系统的安全服务商选择管理，特制定本办法。

第二条 吉林省某某单位按国家信息安全相关政策法规和标准的规定进行信息系统安全服务商的选择工作。

第三条 本办法适用于吉林省某某单位。

4.10.2、 安全服务商选择

第四条 信息系统建设过程中，应选择具有相关服务资质并且信誉较好的厂商，要求其已获得国家主管部门的资质认证并取得许可证书，能有效实施安全工程过程，并且有成功的实施案例。

第五条 对重要的信息系统工程建设项目，需在主管部门指定或在特定范围内选择具有服务资质的信誉较好的厂商，并经实践证明是安全可靠的厂商。

第六条 在确定好安全服务商后，与安全服务商签订安全责任合同书或保密协议，规定保密范围、安全责任、违约

.

责任、协议的有效期限等。

第七条 在确定好安全服务商后，与其签订服务合同，确保其提供技术培训和服务承诺。

4.10.3、 附则

第八条 本办法的解释权归吉林省某某单位。

第九条 本办法自发布之日起生效。

.

附件 4-10-1 个人工作保密承诺书（模板）

个人工作保密承诺书

甲方：吉林省某某单位

乙方：_____

乙方所属单位：_____

乙方身份证号码：_____

鉴于乙方在甲方工作期间,可直接或间接接触、知悉、了解或掌握甲方（或其子公司、关联公司）保密信息,并且乙方愿意为保护甲方（或其子公司、关联公司）的保密信息而承担保密义务,甲乙双方经平等协商,就乙方在履职期间及离职以后保守甲方（或其子公司、关联公司）的保密信息的有关事项,根据甲方有关管理规定制订下列条款共同遵守:

第一条　保密信息

本承诺书所称的保密信息是指,乙方因在甲方履职而获得、接触或以其他方式知悉的任何信息,不论此种信息以口头、书面、电子或者通过其他介质形式存在,亦不论是在本承诺书签署之前、当时或之后知悉。保密信息的内容包括但不限于:

（一）依据国家相关法律法规,甲方承担保密义务的国家秘密信息;

（二）与甲方（或其子公司、关联公司）的经营、业务、交易、产品、客户有关的任何信息;

（三）依据承诺书规定,甲方负有保密义务的任何信息;

（四）任何甲方的技术方案及措施、软件、数据库、技术秘密等。

第二条　保密义务

乙方应履行如下义务:

.

（一）只为甲方利益而不为任何其他目的将保密信息用于在甲方的履职行为;

（二）未经甲方书面同意,不以任何方式向任何第三方泄漏保密信息;

（三）除为在甲方履职需要之目的，不得复制保密信息;

（四）未经甲方同意，乙方不得将其以任何方式获得的保密信息带出甲方为其提供的工作场所，包括不得带回其住处;

（五）如发现保密信息已经或可能被泄漏,应当立即采取为甲方利益的一切合理措施并立即报告甲方;

（六）遵守甲方制定的保密制度,并本着谨慎、诚实的态度,采取一切必要、合理的措施,维护甲方保密信息的机密性;

（七）乙方不得利用其在甲方获悉的保密信息为除甲方以外的第三方服务。

第三条　保密期限

本承诺书的保密期限为自乙方首次获得、接触或者知悉保密信息之日起，至该保密信息被甲方书面宣布解密之日止。

第四条　保密信息的返还

乙方在甲方工作结束前 1 个月内,应无条件地将其持有的保密信息移交给甲方或其授权的人。

如果保存保密信息的载体（包括但不限于硬盘、移动硬盘、软盘、光盘、优盘、磁带、存储卡）属于乙方所有,则乙方应当将甲方的保密信息从载体上永久删除。

第五条　其他约定

（一）如乙方违反本承诺书的任何条款,乙方应协助甲方采取一切合理的补救措施，并赔偿甲方由此受到的损失;

（二）甲方有权根据乙方的行为严重性决定是否解除与乙方的工作关系;

（三）任何对本承诺书内容的修改或变更均须书面认可;

（四）本承诺书一式两份,甲乙双方各执一份。

乙方单位名称（公章）：_____

乙方（签字）：_____

.

_____年____月____日

.

附件 4-10-2 服务项目保密协议书（模板）

服务项目保密协议书

委托方 吉林省某某单位（以下简称“甲方”）与_____（简称“乙方”）在签订《_____服务合同》的前提下，为保证双方的合法权利，经协商双方达成如下保密协议：

1、乙方不得向第三方透露在安全服务期间获得和知晓的甲方（包括其分支机构）的商业秘密和其他有关的保密信息。商业秘密包括技术秘密和经营秘密，技术秘密主要指甲方委托分析的信息系统的秘密，其保密内容包括但不限于：软件产品代码、软件可执行程序、等级测评报告、等级测评结果、操作手册、技术文档、用户手册等。经营秘密包括但不限于双方洽谈的情况、签署的任何文件，包括合同、协议、备忘录等文件中所包含的一切信息、定价政策、设备资源、人力资源信息等。

2、甲方不得向第三方透露在安全服务期间获得和知晓的乙方（包括其分支机构）的商业秘密和其他有关的保密信息。商业秘密包括技术秘密和经营秘密，其中技术秘密包括计算机软件、数据库、技术报告、实验数据、操作手册、技术文档、相关的函电等。经营秘密包括但不限于双方洽谈的情况、签署的任何文件，包括合同、协议、备忘录等文件中所包含的一切信息、定价政策、设备资源、人力资源信息等。

3、未经对方书面同意，任何一方不得在双方合作目的之外使用或向第三方透露对方的任何商业秘密，不管这些商业秘密是口头的或是书面的，还是以磁盘、胶片或电子邮件等形式存在的。

4、在现场测评工作时，应尊重甲方有关保密的管理规定，听从接待人员的安排和引导。未经允许不得进入对方中心机房、办公室内受控的工作环境，与对方技术人员进行的交流，仅限于合作项目有关的内容。

5、如果一方违反上述条款，另一方有权根据违反的程度以及造成的损害采取以下措施：

.

（1）终止双方的合作；

（2）要求赔偿因失密造成的损失。

在采取上述措施之前，一方将给予违约的另一方合理的在先通知。

6、与本协议有关的任何争议，双方应通过友好协商解决。如协商不成，任何一方可将此争议提交当地仲裁委员会进行仲裁。仲裁裁决对双方均有约束力。

7、本协议作为委托测试协议的附件，一式两份，甲方一份，乙方一份，与协议具有同等法律效力。

本协议自双方授权代表签字盖章之日起生效，但有效期不限于协议有效期。

甲方（公章）：吉林省某某单位　　乙方（公章）：_____

_____　　_____

甲方法人或授权人（签字）：_____　　乙方法人或授权人（签字）：_____

日期：_____年___月___日　　日期：_____年___月___日

.

第五章 系统运维管理

.

5.1、环境安全管理规定

5.1.1、 总则

第一条 为保证吉林省某某单位办公区和机房内设备处于最佳状态，使其运行服务质量能够满足业务使用的需求，并保证信息资产不被非法物理访问，特制订此规定。

第二条 本规定适用于吉林省某某单位。

5.1.2、 机房安全管理

第三条 设备的维护必须有专人负责，他人不可随意操作。设备需要停机检查时，应经运维工作小组批准后，方可进行。关闭设备时，应经运维工作小组领导同意。

第四条 明确各设备的安全管理责任人。

第五条 机房内严禁从事与工作无关的各项工作。

第六条 机房内设备必须按照设计及相关规定布置，机房内预留位置不能随意占用。

第七条 设备安放合理，布线整齐，强电与通信电缆走线分离，避免交叉，禁止随意改动布线。

第八条 操作维护终端应具备 UPS 不间断电源或逆变

.

器，应该有明确的防病毒措施，定期进行检查。维护终端设备严禁上网，严禁装载游戏软件等。

第九条 无人职守机房必须有配套的环境监控设备，如出现环境监控告警应及时解决。

第十条 机房空调应指定专人负责，使机房温、湿度应符合机房维护技术指标要求，机房正常温度应保持在20℃—25℃，相对湿度保持在40%—60%。

第十一条 机房应有良好的防静电措施，机房内配置防静电手环，地面铺设防静电地板。

第十二条 机房照明设备安全可靠，应配备应急灯，各种照明设备应有专人负责，定期检修。

第十三条 机房门窗要密闭，环境保持卫生清洁，机房内设备摆放整齐。

第十四条 交换机、路由器应建立防尘缓冲带，备有工作服和工作鞋。

第十五条 维护人员要切实遵守安全制度，认真执行用电、防火的规定，做好防火、防盗、防爆、防雷、防冻、防潮等工作，确保人身和设备的安全。

第十六条 机房配置灭火设备，各种灭火设备要定位摆放，定期对防火设备进行检查。一旦发生火情，值班人员应按机房灭火流程图及应急措施进行处理，并立即逐级上报。

第十七条 在维护、测试、装载、故障处理、日常操作

.

及工程施工等工作中，应采取预防措施，防止造成工伤和通信事故。

第十八条 机房内非特殊需要，严禁使用明火。

第十九条 机房应配置电子门禁系统，外来人员不得擅自进入机房。因公原因进入机房，应经相关领导批准后，进行物理登记和电子记录双重备案，方可进入。

第二十条 定期对无人职守机房进行巡查，在洪水、冰凌、台风、雷雨、严寒等情况下，应加大巡视强度，以确保机房室内外环境的良好与安全，保证机房设备正常运行。

第二十一条 机房内严禁吸烟、饮食、睡觉、闲谈。各种与工作无关的书刊、报纸和其它物品不准带入机房。

第二十二条 值班不做与工作无关的事，严禁在终端设备上操作与工作无关的程序。值班人员不得撤离工作岗位。

第二十三条 按时、按质、按量完成各种维护测试，发现问题及时分析处理，认真完成各项质量指标。

第二十四条 按时、按质、按量完成各项作业计划，要符合作业计划的周期要求。

第二十五条 各项维护记录齐全、准确。

5.1.3、 办公区信息安全管理

第二十六条 任何员工进入办公区域时，必须佩带工卡，工卡必须戴在外部可见的地方。员工如果忘记或丢失工

.

卡，由门卫登记并向员工提供临时出入卡。

第二十七条 员工在办公区发现没有在明显位置佩带工卡/临时卡的人员必须主动询问对方的身份并要求出示相关证件。

第二十八条 不允许转借自己的工卡或使用其他员工的工卡。

第二十九条 未经许可，员工不得企图进入严格限制的办公区域，如机要室、存储介质室等。

第三十条 当携带计算机存储介质离开办公区时必须具备通行证，所有此类物品的出门都必须在门卫处记录。

第三十一条 在员工离职时，所有的访问权必须立即收回（工卡、办公室钥匙等）。

第三十二条 对所有需要进入办公区域的供应商、顾问、拜访者等非内部人员，必须有员工陪同，在门卫处进行登记，并发放临时卡后方可进入。

第三十三条 接待人不得引领和允许供应商、合作商进入未经批准的机房、办公区或其它机要区域，员工有权拒绝或制止供应商、合作商进入未经批准的办公区域。、

第三十四条 接待部门原则上应为供应商、合作商安排专门的办公场所。业务洽谈应当在接待室或对外会议室内进行，重大项目的会谈应当在专门的会议室进行，不得在办公室进行。

.

第三十五条 员工下班后桌面上不能有敏感信息的纸件文档，敏感信息的文档应放在抽屉或保密柜内，存放敏感信息文件的保密柜必须设置密码。

第三十六条 员工离开座位超过30分钟，必须对计算机进行锁屏，桌面上不能有敏感信息的纸件文档。

第三十七条 所有有单独房间的员工,在离开办公室时必须锁门。当办公室无人时，离开必须锁门。

第三十八条 妥善保管好个人的贵重物品和仪器,下班后必须把贵重物品和仪器存放在保密柜内。

第三十九条 员工调离部门或更换办公室时,必须立即交还原办公室钥匙。

5.1.4、 附则

第四十条 本规定的解释权归吉林省某某单位。

第四十一条 本规定自发布之日起生效。

.

附件 5-1-1 机房来访人员登记表（模板）

机房来访人员登记表

来访人员填写						陪同/审批人员填写	
日期	姓名	单位	进入时间	事由	离开时间	陪同人员	备注

.

.

5.2、资产安全管理制度

5.2.1、 总则

第四十二条 为加强和规范吉林省某某单位信息系统资产（包括设备和介质等）的安全管理，对信息系统资产使用、传输、存储及维护等方面的管理做出规定，规范信息系统资产管理和使用的行为，特制定本制度。

第四十三条 本制度适用于吉林省某某单位信息系统资产的管理和使用。

第四十四条 信息系统资产包括以下内容：

（一）信息资产：包括应用数据、系统数据、安全数据等数据库和数据文档、系统文件、用户手册、培训资料、操作和支持程序、备用系统安排、存档信息等；

（二）软件资产：包括应用软件、系统软件、开发工具和实用程序等；

（三）有形资产：包括计算机设备(处理器、监视器等)、通信设备(路由器、传真机等)、磁介质(磁带、移动存储介质、光盘等)、其他技术装备(电源，空调设备)、家具和机房等；

（四）应用业务相关资产：包括由信息系统控制的或与

.

信息系统密切相关的应用业务的各类资产，由于信息系统或信息的泄露或破坏，这些资产会受到相应的损坏；

（五）服务：包括计算和通信服务，通用设备如供暖、照明、供电和空调等。

5.2.2、 信息系统资产使用

第四十五条 信息系统资产采购后交付使用部门的资产管理员，资产管理员对资产按照规则命名和标识，使用人要在本部门《资产清单》上进行领用登记，然后由资产管理员交付资产给使用人。

第四十六条 信息系统资产的使用人、责任人是其资产的第一责任人，要按照产品手册、操作规程、管理制度等要求正确的使用设备或介质资产，防止其被盗、遗失、被未授权修改以及信息的非法泄漏。

第四十七条 信息系统资产的传输、存储、维护或销毁参照介质管理中相关内容执行。

第四十八条 信息系统资产基本信息发生变化时，使用人/责任人需要到本部门资产管理员处进行相关的信息变更。

5.2.3、 信息系统资产传输

第四十九条 含有敏感工作信息的信息系统资产在传

.

输过程中必须亲自交给接受方。

第五十条 通过外部运输人员传输的信息系统资产需要接受者签字等措施，以保证传送安全到达。

第五十一条 需要有日志记录含有敏感工作信息的信息系统资产的传输过程（多少、在哪里、接收者姓名、地址等）。

第五十二条 含有敏感工作信息的信息系统资产不能在旅游时携带，除非经过管理部门审批同意。

5.2.4、 信息系统资产存储

第五十三条 信息资产领取使用后，按照信息资产明细账和信息资产登记卡片，明确信息资产的使用人员和存放地点，使用人员是信息资产保管的责任人，负责固定资产在使用过程中的安全和完整。

第五十四条 贵重的、精密程度较高的信息系统资产应指定专人保管。

5.2.5、 信息系统资产维护

第五十五条 信息系统资产日常维护包括巡检与监控、备份与恢复、停机检修。

第五十六条 巡检与监控人员对应用系统、网络系统和机房的运行状况进行监控，定期检查系统日志，填写机房巡

.

检日志，及时报告、处理发生的异常事件，并定期汇总上报数据管理中心。

第五十七条 备份与恢复人员按方案进行系统备份，并在系统环境发生重大变化时对系统和数据及时进行恢复。

第五十八条 资产维护人员制定详细停机检修方案，报信息化管理处审批后，在网上发布停机公告，电话通知重点用户，确认对用户无重大影响后，按方案停机检修，尽量安排在节假日期间。

第五十九条 信息系统资产需外出维修的，必须由使用人员提出申请，部门负责人签字确认，经信息化管理处审核方可，如设备未出保修期，由资产管理部门向信息化管理处提供产品保修证书，所有产品保修证书统一由资产管理部门编号保管。

第六十条 各部门人员均不得擅自拆装信息系统资产设备，如有故障，不得私自拆修，须及时通知信息化管理处，由技术人员进行检查维修。

第六十一条 所有信息系统资产使用人员应爱护资产设备，自觉进行日常清理保洁及相关简单的维护。

5.2.6、 信息系统资产报废

第六十二条 信息资产正常报废时，填报《信息系统资产报废申请表》（0），办理相关手续。

.

（一）信息资产报废单位填写《信息系统资产报废申报表》一式三份，由本单位负责人批准。

（二）单位批准后，经办人员携带报废申请表及信息系统资产实物到信息化管理处进行核实鉴定。

（三）经核实后，信息资产管理部门将报废信息资产回收（自收自支事业单位除外），并在《信息系统资产报废申报表》上级资产管理部门意见处签字。

（四）信息化管理处签字后，报主管领导审批，办理报废审批。

（六）《信息系统资产报废申请表》经主管领导审批后，一份作为单位固定资产管理部门核销固定资产台账依据，一份作为单位财务部门核销固定资产账和固定资产卡片依据，一份作为信息化管理处回收依据。

第六十三条 吉林省某某单位在信息系统资产损毁或丢失时，分清责任后进行处理，并办理相关手续。

（一）使用部门或个人发生信息系统资产损毁或丢失时，应及时报本部门信息系统资产专管人员，由专管人员确认后，查明原因，报单位领导审批。

（二）经领导批准后，单位填写《信息系统资产报废申请表》一式三份，按信息系统资产报废的手续办理。

（三）单位查清责任原因后，责任人写出检查并按信息系统资产实际价值的10%做出赔偿，另有规定的从其规定。

.

第六十四条 吉林省某某单位报废信息系统资产由信息化管理处进行统一处置。

（一）各单位将报废的信息系统资产交回信息化管理处（自收自支单位除外），不得自行处置，及时办理交接手续，统一由信息化管理处进行处置。

（二）信息化管理处将处置的信息系统资产残值收回后，统一由信息化管理处挂账，集中安排使用。

第六十五条 为了确保信息资料安全，吉林省某某单位在信息系统资产处置前，涉及到网络、软件系统及计算机类设备时，通知数据管理中心专管人员进行检查、清理计算机硬盘资料后，再行处置。

5.2.7、 附则

第六十六条 本制度的解释权归吉林省某某单位。

第六十七条 本制度自发布之日起生效。

.

附件 5-2-1 资产清单（模板）

资产清单

资产名称	资产型号	资产统一命名	重要程度	采购人	采购部门	交付使用时间	使用人/责任人	责任部门	所处位置	资产状态	资产核对记录	资产核对时间	核对人	备注

说明：

1、 建议用专用的表格工具制作清单，如 office excel,便于筛选和统计，条目可参考上面的表格。

2、 “资产统一命名”指：按照本单位命名规则对资产统一命名和标识。

3、 “重要程度”指：资产发生故障后对信息系统的影响程度。

4、 “采购人”和“采购部门”便于在资产使用发生问题时，联系售后服务。

5、 “交付使用时间”指：使用部门使用人在本部门资产情况维护人处进行领用登记的时间。

6、 如果设备是个人使用，则领用人为“使用人”；如果设备是网络或服务器等基础设施，则领用人为“责任人”。

7、 “责任部门”指：资产“使用人”或“责任人”所属的部门，如果“使用人”或“责任人”转移到其他部门，“责任部门”一栏也要发生变更。

8、 “所处位置”指：资产的物理存放位置。

9、 “资产状态”指：“使用”或是“弃置”，“弃置”资产的管理办法遵照本单位财物部门相关制度。

10、 “资产核对记录”指：“正确”或“有误”，由资产清单维护人定期对本部门的信息

.

系统资产进行清查、核对、登记，主要核对设备和介质是否保存完好，有无变更，有无遗失等。

.

附件 5-2-2 信息系统资产报废申请表（模板）

信息系统资产报废申请表

申报单位：　　年　月　日

报废理由：

信息系统资产品名	规格型号	数量	单位	购置时间	金额

单位意见：

签字盖章：　　年　月　日

上级资产管理部门意见：

签字盖章：　　年　月　日

上级财务部门意见：

签字盖章：　　年　月　日

上级主管领导意见：

签字盖章：　　年　月　日

备注：

.

.

5.3、介质安全管理制度

5.3.1、 总则

第一条 为加强吉林省某某单位介质安全管理，即对存储介质的使用、存储、携带、记录、清单等活动提供明确的安全管理标准，特制订此制度。

第二条 本制度适用于吉林省某某单位。

5.3.2、 介质管理标准

第三条 保管人控制下的存储介质和用来备份或是用做灾难恢复的，需存放在一定安全级别的区域，当无人看管时，要将这些介质存放在办公室或保密柜中。

第四条 用做一般系统备份的存储介质可以与用户控制下的存储介质分开放置，必须被慎重管理以保证在需要恢复的情况下能够得到，同时必须记录在管理员的目录清单里。

第五条 必须建立存储介质的原始存储目录清单，并定期对备用目录清单进行盘点，以备将来使用，当所有权发生变化时，必须进行存储库盘点。

第六条 存储介质库中介质的转移和支配应该是可记录的。

.

第七条 必须对所有存储介质的出库和入库及其保持记录进行控制。

第八条 存储介质被运离或送出时，要被放在一个被锁住的箱子里，用防篡改的封条封住。

第九条 安装和使用存储介质时必须防止非授权的访问。

第十条 任何的存储介质盘点与检查出现差异必须报告给运维工作小组，并且介质库中的所有介质，包括打开过的空白带和格式化过的、擦除过的、媒体操作装置中的介质都必须有清单列表。责任人必须对所有的清单文档签字。

第十一条 含有敏感工作信息的存储介质在邮递或内部传输时候必须被放在标记的密封套子或是包装盒中，被邮递或传输到外部时，内盒需要明确标记为敏感信息，外盒或封套不要标记敏感信息字样。

第十二条 制定硬盘加密，硬盘口令等具体措施。

第十三条 含有敏感工作信息的存储介质不再使用时，应与安全管理工作人员联系，销毁这些敏感信息存储介质。

第十四条 存储介质要全面考虑数据分类标签的需求，如磁带、磁盘及其它存储介质等有不同的分类标签。

第十五条 含有敏感信息的存储介质的复制要有跟踪、出处、输送记录，对拷贝的人需要了解具体情况。

第十六条 在复制或输出敏感信息到存储介质时，需要

.

有人监控（不能让敏感信息自行输出到远程存储介质，特别是远程可移动存储介质）。

第十七条 存储介质的存放，需要用不同的标签或介质类型来表示是原件还是拷贝件。

第十八条 含有敏感信息的存储介质在传递过程中必须亲自交给接受方。

第十九条 通过外部运输人员传递的存储介质需要接受者签字等措施，以保证安全到达。

第二十条 需要有日志来记录含有敏感信息的存储介质的传递过程（多少、在哪里、接收者姓名、地址等）。

第二十一条 除非经过管理部门特别同意，旅游时不能携带含有敏感信息的存储介质。

第二十二条 除非存储介质内的敏感信息已经被加密，否则存储介质不许在无人看管的可移动设备上使用。

第二十三条 可移动存储介质必须放在随身携带的手提箱中，而不能放在其他的货物托管地方。

第二十四条 所有含有内部信息的存储介质对外部人员都是保密的，严禁员工、顾问和合作方带走。

第二十五条 任何计算机存储介质不再用于存储保密信息之前，必须要进行格式化。

第二十六条 不允许将含有敏感信息的存储介质和非敏感信息的存储介质混放在一起。

.

第二十七条 存储介质删除敏感信息后，必须执行重复写操作防止数据恢复。

第二十八条 含有硬拷贝形式的敏感信息存储介质的报废处理方式是切碎或者烧毁。

第二十九条 如果将存储介质给第三方使用，需要信息化管理处确认敏感信息已经删除。

第三十条 当携带存储介质离开时必须出示通行证，所有此类物品必须在门卫处记录。

第三十一条 访问磁带、磁盘和文档库需要提出申请，由信息化管理处审批同意放可进行，并登记备案。

5.3.3、 附则

第三十二条 本制度的解释权归吉林省某某单位。

第三十三条 本制度自发布之日起生效。

.

附件 5-3-1 存储介质操作记录表（模板）

存储介质操作记录表

介质名称	编号	操作类型	操作时间	结束时间	经手人	审批人	备注

.

说明：操作类型包括：使用、送修、带出、销毁、盘点等行为。

.

5.4、设备安全管理制度

5.4.1、总则

第一条 为加强吉林省某某单位设备安全管理，明确维护人员责任，保障系统的安全稳定运行，特制订本制度。

第二条 本制度适用于吉林省某某单位。

5.4.2、设备安全管理

第三条 信息化管理处负责对吉林省某某单位信息系统相关的各种设备（包括备份和冗余设备）、线路等定期进行维护管理。

第四条 信息系统的各种软硬件设备的选型、采购、发放和领用参照《系统建设管理-信息系统产品采购和使用管理规定》执行。

第五条 信息处理设备的带离需由带离人员填写设备出门条（见 0），经由设备所属部门领导签字后方可带离单位。

第六条 设备出现故障、须开机箱维修的，应由信息化管理处派工程师到现场进行维修或送信息化管理处维修，严禁各部门私自开机箱维修。现场维修时，应由相关人员全程陪同。

.

第七条 在处理设备故障、进行维修过程中，故障维修申请人应及时提供该机相关资料、文档，确保维修工作得以顺利进行。

第八条 计算机维修人员在维修过程中，对于需要更换的零部件，在价格和型号等方面要及时与申请人沟通，取得认同后再更换。

第九条 维修人员应当认真填写《设备维修记录表》(见0)。

第十条 在接到用户提出需外部门维修人员对计算机、数字复印机等设备进行现场维修申请时，信息化管理处计算机维修人员需全程陪同，严禁外部门维修人员擅自读取和拷贝计算机、数字复印机中存储的信息。

第十一条 禁止在系统外对设备进行远程维护和远程监控，并严格控制系统内的设备远程维护和远程监控。

第十二条 设备的维修流程如下：

（一）由设备管理人员填写《设备维修记录表》(见0)；

（二）报信息化管理处；

（三）由信息化管理处派工程师到现场进行维修或送信息化管理处维修；

（四）维修人员填写《设备维修记录表》(见0)。

第十三条 设备超过使用年限或发生故障无法维修且无相应配件更换时，可予以报废，必须办理相应报废手续。

.

设备报废参照《系统运维管理-资产安全管理制度》中关于信息系统资产报废的规定执行。

5.4.3、 配套设施、软硬件维护管理

第十四条 由信息化管理处负责信息系统配套设施、软硬件的维护管理工作，制定相应的巡检表格和操作规程，规范运行维护活动。

第十五条 运行维护工作由系统运维负责人指定相关资产责任人按照操作规程进行，资产责任人承担某一资产的维护和管理。

第十六条 对配套设施、软硬件设备和线路的常规运行维护操作按照操作规程进行，操作规程由资产责任人负责更新和维护。

第十七条 对供电和通信设施进行巡检，发现问题及时处理。

第十八条 重要线路线缆埋放地点应有明显警示装置，防止因施工等原导致意外破坏，并将系统内所有线路线缆的布置图进行整理汇编，以备查看。

第十九条 每半年对软硬件系统（包括备份和冗余设备）进行巡检，发现问题及时处理。系统运维小组按照实际需要制定巡检要求，并按照规定巡检。

第二十条 巡检对照巡检表格逐项巡检，巡检表保存一

.

年。

第二十一条 巡检工作由运维单位组织,具体检查工作每天进行、每周回顾、每月总结。

第二十二条 巡检包括网络巡检、主机以及数据库巡检、应用系统巡检、机房相关设备巡检。

第二十三条 网络巡检主要内容:

网络设备外观、接电情况、指示灯、cpu 利用率、内存负载(byte)、广域网接口状态、局域网接口状态、模块状态,《网络作业计划巡检表》参见附件 3;

第二十四条 主机巡检主要内容:

CPU 使用率、内存使用率/pagingspace、文件 系统空间、磁盘、IO、网络状况、系统错误日志/mail、硬件报警灯、增减用户、应用纪录、TOP5 应用进程、参数调整纪录、故障/异常纪录、维护总结,《主机作业计划巡检表》参见附件 4;

第二十五条 数据库巡检主要内容:

数据库 CPU 使用率、内存使用率/pagingspace、文件系统空间、磁盘 IO、网络状况、系统错误日志、oracle 进程数、alert.log 纪录信息、表空间使用率、TOP5 数据库进程、用户表空间权限变更、故障/异常纪录、维护总结,《数据库作业计划巡检表》参见附件 5;

第二十六条 应用服务状况巡检主要内容:

.

应用服务器 CPU 使用率、内存使用率、文件系统空间、磁盘 IO、网络状况、系统错误日志、oracle 进程数、alert.log 纪录信息、表空间使用率、TOP5 数据库进程、用户表空间权限变更、故障/异常纪录、维护总结，《应用服务作业计划巡检表》参见附件 6；

第二十七条 机房相关设备巡检主要内容：

门禁系统、机房温度、机房湿度、门窗状况、机房清洁状况、UPS 状况、UPS 电池状态、空调机器状况，《机房相关设备作业计划巡检表》参见附件 7。

第二十八条 巡检工作的开展

（一）网络巡检由运维单位指定的网络设备维护人员进行巡查和操作；主机巡检由运维单位指定的主机设备维护人员进行巡查和操作系统巡检，必须按信息化管理处规定的时间和项目巡视检查管辖下的设备；应用服务巡检由应用开发商指定、信息化管理处认可的应用系统维护人员进行巡查和操作，每个工作日巡视检查管辖下的设备和系统；数据库巡检由运维单位指定的数据库维护人员进行巡查；

（二）巡检人员应根据当班设备的具体运行情况，对运行的设备进行巡检和监控；

（三）巡检人员发现设备有缺陷，发现设备运行状态指示灯有损坏，发现安全保护有变化，均应即时通知系统管理员调整或更换，保证设备的监控元件在完好状态下运行；

.

（四）巡检人员发现设备和系统有不正常的噪音、压力、内存泄露等又不能迅速排除的，必须立即报告信息化管理处，并采取适当的防护措施，防止事故的发生或扩大；

（五）每次巡检均须在相应的巡检记录上依顺序做好巡查情况和结果记录；

（六）信息化管理处系统管理员每周一次对巡查情况和结果进行抽查，发现问题追查原因，如属人为应追究当事人责任。

第二十九条 信息化管理处及相关的系统管理员、网络管理员、应用系统开发商等应给予巡检人员配合，提交相关的管理记录文档、系统资源信息，信息提供人对信息的真实性承担负责。

5.4.4、 设备使用管理

第三十条 服务器安全操作规程

（一）服务器只能由系统管理员或授权的人员操作；

（二）服务器应使用独立的 UPS 后备电源并不得随意断电、重启，一旦发生故障，应当及时通知系统管理员处理；

（三）系统管理员应妥善设置系统密码，不得泄漏，并定期更改；

（四）系统管理员应当定期升级程序补丁，在升级补丁之前应做好相应测试，并备有应急恢复机制；

.

（五）每天上班首先检查服务器是否正常工作，发现问题及时处理。

第三十一条 计算机终端使用安全要求

（一）用户终端必须按照要求统一部署防病毒软件及终端安全管理及补丁分发系统，并确保其能够接受来自服务器的自动更新，对接入系统的存储设备要经过计算机病毒与恶意代码的检查处理；

（二）对于本人在系统中的身份标识符，采用英文字母、数字和特殊字符中两者以上组合的8位长度口令。要对使用本人身份标识符产生的操作行为负责；

（三）用户在退出系统时，要注销帐号；

（四）用户在暂时离开显示器时，要锁屏；

（五）所有用户均有责任报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点。用户发现安全弱点和可疑事件时，应立即向运维单位报告。

第三十二条 网络设备安全使用要求

（一）网络设备必须放置并固定在专用机柜中。放置机柜的房间要求通风良好、消防设施齐备，并由专人管理；

（二）网络设备必须提供不间断电源以防止突然断电对设备造成损害及数据丢失；

（三）核心网络设备必须提供冗余供电，提高整体运行可靠性；

.

（四）网络设备需要定期更换管理口令；

（五）网络管理员定期检查各网络设备运行情况；

（六）法定节假日指定专人对网络设备的运行状态进行监控；

（七）只允许经过专业培训，并授权的信息安全保护关键岗位人员才能对网络设备进行调整或对硬件设施进行维护；

（八）对网络设备的配置进行操作变更时应做好记录，保存与备份更新后的配置。

5.4.5、 附则

第三十三条 本制度的解释权归吉林省某某单位。

第三十四条 本制度自发布之日起生效。

.

附件 5-4-1 设备出门条（模板）

设备出门条

出门条				出门条		
存根	年　月　日			携物证	年　月　日	
携物者	单位			携物者	单位	
	姓名		字		姓名	
物品名称		数量	第	物品名称		数量
			号			
领导签字				领导签字		

附件 5-4-2 设备维修记录表（模板）

设备维修记录表

基本信息	
单位	
日期	
设备编号	
设备名称及用途	
设备位置	
负责人	
设备型号配置	
故障现象	
单位审批	
签字： 日期：	
数据管理中心意见	
签字： 日期：	
维修记录（需说明是内部维修、外部维修地点，并注明是否包含存储介质）：	
维修人： 日期：	

.

附件 5-4-3 网络运维巡检表（模板）

网络运维巡检表

序号	巡检关键指标	巡检人员	巡检时间	本次结果或故障内容	上次结果或故障内容	结论或处理意见
1	主机名					
2	机器清洁状况			□不需要清洁 □需要清洁		
3	路由器/交换机型号及版本					
4	路由器/交换机地址					
5	设备位置					
6	设备故障灯是否有亮			□无报警 □有报警		
7	cpu 利用率					
8	内存负载（byte）					
9	广域网接口状态、					
10	局域网接口状态					
11	模块状态					

.

附件 5-4-4 主机运维巡检表（模板）

主机运维巡检表

序号	巡检关键指标	巡检人员	巡检时间	本次结果或故障内容	上次结果或故障内容	结论或处理意见
1	主机名					
2	机器清洁状况			□不需要清洁 □需要清洁		
3	主机型号及版本					
4	主机地址					
5	设备位置					
6	设备故障灯是否有亮			□无报警 □有报警		
7	CPU 使用率					
8	内存使用率 /pagingspace					
9	文件系统空间					
10	磁盘 IO					
11	网络状况					
12	系统错误日志/mail					
13	增减用户					
14	应用纪录					
15	TOP5 应用进程					
16	参数调整纪录					
17	故障/异常纪录					

.

附件 5-4-5 数据库运维巡检表（模板）

数据库运维巡检表

序号	巡检关键指标	巡检人员	巡检时间	本次结果或故障内容	上次结果或故障内容	结论或处理意见
1	主机名					
2	主机型号及版本					
3	数据库版本					
4	主机地址					
7	CPU 使用率					
8	内存使用率/pagingspace					
9	文件系统空间					
10	磁盘 IO					
11	网络状况					
12	系统错误日志					
13	oracle 进程数					
14	alert.log 纪录					
15	表空间使用率					
16	TOP5 数据库进程					
17	用户表空间权限变更					
18	故障/异常纪录					
19	维护总结					

.

附件 5-4-6 应用服务运维巡检表（模板）

应用服务运维巡检表

序号	巡检关键指标	巡检人员	巡检时间	本次结果或故障内容	上次结果或故障内容	结论或处理意见
1	主机名					
2	主机型号及版本					
3	应用服务器版本					
4	主机地址					
5	应用系统 CPU 使用率					
6	内存使用率/pagingspace					
7	队列情况					
8	应用服务端口情况					
9	应用日志情况					
10	参数调整纪录					
11	故障/异常纪录					
12	当前维护小结					

.

附件 5-4-7 机房相关设备运维巡检表（模板）

序号	巡检关键指标	巡检人员	巡检时间	本次结果或故障内容	上次结果或故障内容	结论或处理意见
1	门禁系统					
2	机房温度					
3	机房湿度					
4	门窗状况					
5	机房清洁状况					
6	UPS 状况					
7	UPS 电池状态					
8	空调机器状况					
9	防盗报警装置					
10	监控系统					
11	自动消防系统					
12	动力环境监控系统					
13	供电系统					
14	备用发电机					
15	当前维护小结					

.

5.5、运行维护和监控管理规定

5.5.1、 总则

第一条 为保障吉林省某某单位网络与信息系统安全、稳定运行，加强网络与信息系统运行维护和监控管理，特制订此规定。

第二条 本规定适用于吉林省某某单位。

5.5.2、 运行维护和监控工作

第三条 由信息化管理处负责吉林省某某单位信息系统的安全运行维护和监控工作，保证各项业务的正常运行。

第四条 建立安全管理中心，对通信线路、主机、网络设备和应用软件的运行状况，对设备状态、恶意代码、网络流量、补丁升级、安全审计等安全相关事项进行集中管理；并形成监测记录文档，指定专人对监测记录进行整理并保管。

第五条 监测记录应包括监测对象、监控内容、监控的异常现象处理等方面。

第六条 组织人员定期对监测记录进行分析、评审，发现可疑行为时采取必要的措施；形成分析报告，分析报告应

包括监测到的异常现象和处理措施等。

第七条 维护项目应包括但不限于以下内容：

（一） 机房环境、温湿度检查；

（二） 网络链路的实时监控；

（三） 网络的连通性（内网、外网）、时延、丢包率检查；

（四） 设备运行状态检查：CPU 负荷、连通性等；

（五） 出口链路或关键链路流量检查；

（六） 设备备份工作等。

第八条 定期和不定期对安全设备的策略进行检查，确保安全策略符合系统现状的要求。

第九条 对新购置的设备和软件在上线之前进行安全性检查、策略合理性测试。

第十条 对设备和软件的日志定期和不定期进行审计，了解整个网络的状况、设备的运行状况和网络故障及攻击事件。

第十一条 设备和软件分为版本升级和相关库（如病毒库、IDS 策略库）两部分。在业务不能满足或者出现一个很严重的漏洞的情况下，要进行相关升级和逐级上报。

第十二条 各系统运维人员负责维护和监控责任范围内的设备，不得越权进行访问。

.

5.5.3、 安全运行维护和监控作业计划

第十三条 系统运维人员根据维护和监控工作内容制定各项计划性的安全维护工作。

第十四条 作业计划应包括以下内容：安全设备维护、安全监控、操作日志、日志审核、故障管理、测试等工作。

第十五条 编制安全维护作业计划时，应充分考虑可能发生的各种情况，明确执行期限，落实到人。

第十六条 编制安全维护作业计划时，应明确各项作业的执行完成标志，提供可操作的核查手段。

第十七条 系统运维人员应定期提交下年安全维护作业计划，由信息化管理处核准后实施。

第十八条 安全维护作业计划核准下达后，要保质、保量、按时完成，不得任意更改，如系统环境变化或遇特殊情况需要临时变动时，须经信息化管理处核准后及时更新。

第十九条 安全维护作业计划在编制和确定后，应根据其内容严格执行。

第二十条 系统运维人员应及时填写维护报告并和相应的维护作业计划归档。

第二十一条 系统运维人员应定期对维护计划执行情况进行总结分析。

第二十二条 对于未及时完成或完成情况欠佳的安全维护作业计划，应及时认真地作好总结工作，分析原因，避

.

免下次出现同样的问题。

第二十三条 安全维护作业计划确定严格执行，并由信息化管理处进行定期检查。

第二十四条 安全运行维护报告是安全维护工作小组工作的重要成果之一，对以后的安全运行维护工作有着指导性的意义，是以后运行维护计划制定的可行性依据之一。

第二十五条 安全运行维护报告的内容，应根据作业计划执行情况的对应信息作为参考，结合实际情况来编写。

第二十六条 安全运行维护报告涉及方面包括但不限于以下内容：安全设备维护、安全监控、操作日志、日志审核、故障管理和测试等工作。

5.5.4、 附则

第二十七条 本规定的解释权归吉林省某某单位。

第二十八条 本规定自发布之日起生效。

.

附件 5-5-1 监控记录分析评审表

监控记录分析评审表

基本信息	
监控系统名称	
监控位置	
监控设备型号	
摄像机数量	
分析评审日期	
分析评审时间	
分析评审人员	
分析操作位置	
监控配合人员	
评审信息	
硬件设备运行状态是否完好	
有效画面数量是否缺失	
监控画面是否清晰连续完整	
时钟是否已经与标准时间同步	
各监控画面是否有遮挡物	
监控记录保存时长是否符合要求	
是否发现违规行为	
违规行为处理方法	
其他问题	
审批信息	
分析人员签字	
监控人员签字	
主管领导签字	

.

5.6、网络安全管理制度

5.6.1、 总则

第一条 为审视吉林省某某单位网络系统的安全性，降低网络系统存在的安全风险，确保网络系统安全可靠地运行，特制订此制度。

第二条 本制度适用于吉林省某某单位。

5.6.2、 网络设备管理

第三条 信息化管理处网络管理员对网络设备进行维护监控等工作。

第四条 网络设备的登录口令必须足够强壮难以被破译。

第五条 网络设备的当前配置文件必须在主机上有备份文件。

第六条 网络设备的拓扑结构、IP 地址等信息在一定范围内保密。

第七条 网络整体的拓扑结构需进行严格的规划、设计和管理，一经确定，不能轻易更改。

第八条 定期检查网络设备的日志，及时发现攻击行为。

第九条 网络设备的软件版本应该统一升级到较新版

.

本。

第十条 网络设备的安装、配置、变更、撤销等操作必须严格按照相关流程进行。

第十一条 网络管理员应每季度对网络进行漏洞扫描，并与系统管理员、安全管理员一起进行扫描结果的分析。如发现重大安全隐患，应立即上报。

第十二条 网络管理员进行漏洞扫描前需提出申请，详细描述扫描的技术、范围、时间及可能的影响，在获得数据管理中心领导审批后，方可执行。

第十三条 对重要网段要进行重点保护，要使用防火墙等安全设备以及 VLAN 或其他访问控制方式与技术将重要网段与其它网段隔离开。

第十四条 网络结构要按照分层网络设计的原则来进行规划，合理清晰的层次划分和设计，可以保证网络系统骨干稳定可靠、接入安全、便于扩充和管理、易于故障隔离和排除。

第十五条 网络管理员定期对网络的性能分析，以充分了解系统资源的运行情况及通信效率情况，提出网络优化方案。

第十六条 按照最小服务原则为每台基础网络设备进行安全配置。

第十七条 网络连接管理过程中，需明确网络的外联种

.

类，包括互联网、合作伙伴企业网、上级部门网络和管理部门网络等，根据外联种类确定授权与批准程序，保证所有与外部系统的连接均得到授权和批准，并具备连接策略及对应的控制措施。

第十八条 除网络管理员特别授权外，员工内严禁拨号上网。经授权的拨号上网，必须首先与内部网络断开。

第十九条 网络互连原则：

（一）与互联网的连接中，在互连点上的防火墙上应该进行 IP 地址转换；

（二）任何部门不得自行建立新的信息平台，如确有需求，需经由相关部门认证批准后实施；

（三）互联网接入必须有防火墙等安全防范设备。未经许可，任何部门或个人不得私自在网络内新增与互联网的连接。

第二十条 办公网络中不同业务的网络之间互连原则：

（一）互连点上必须实施安全措施，如网络访问控制列表、安装防火墙等；

（二）网络之间互连点采取集中原则，并考虑安全冗余；

（三）网络互连点及安全设备必须纳入到网管体系的监控。

.

5.6.3、 用户和口令管理

第二十一条 要求对网络设备的登录帐号的设置权限级别，授权要遵循最小授权原则。

第二十二条 保证用户身份标志的唯一性,即不同的个人用户必须采用不同的用户名和口令登录，并且拥有不同的权限级别。不同用户的登录操作在设备日志文件上均有记录，便于追查问题。

第二十三条 网络设备的直接责任人拥有超级用户权限，其他网络管理员按照工作需求拥有相应的用户权限．网络管理员不得私开用户权限给其它人员。

第二十四条 用户的口令尤其是超级用户的口令必须足够强壮难以被破译，这是保证设备安全性的基本条件。口令的设置应该满足规定的标准。

5.6.4、 配置文件管理

第二十五条 配置文件存储着网络设备的所有配置信息。网络设备中的运行配置文件和启动配置文件应该随时保持一致。

第二十六条 所有的网络配置文件有文档记录,网络设备的配置文件需要定期备份。

第二十七条 通过 TFTP 或 FTP 的方式可以将设备的配置文件下载到本地主机上作备份文件以防不测，在设备配置

.

文件损坏时可再通过 TFTP 或 FTP 的方式从本地主机上载到设备的 FLASH 中恢复备份的配置文件。

第二十八条 网络设备的拓扑结构、IP 地址等信息文档属于机密信息，应该在一定范围内予以保密。

第二十九条 网络配置信息的修改要获得各业务处室安全管理员的批准方可进行。

第三十条 各业务处室定期对网络配置信息是否符合当前网络状况进行检查和分析，并做详细记录。

5.6.5、 日志管理

第三十一条 网络设备通常可以设置日志功能，日志可以直接登录到设备上查看，也可以设置将日志发送到某台指定的 UNIX 主机上查看。日志中具体包含的内容可以在命令行配置方式下设定。

第三十二条 在日志文件中可以查看到曾经登录过该设备的用户名、时间和所作的命令操作等详细信息，为发现潜在攻击者的不良行为提供有力依据。

第三十三条 网络管理员必须定期查看所管设备的日志文件，发现异常情况要及时处理和报告上级主管，尽早消除网络安全隐患。

第三十四条 网络管理员要定期对日志文件进行备份。日志文件保存时间应在 3 个月以上。

.

第三十五条 对日志文件的访问要获得各业务处室安全管理员的批准。

5.6.6、 设备软件管理

第三十六条 网络设备的软件版本（IOS 或 VRP 等）较低可能会带来安全性和稳定性方面的隐患，因此要求在设备的 FLASH 容量许可的情况下统一升级到较新的版本。必要情况下可升级设备的 FLASH 容量。

5.6.7、 设备登录管理

第三十七条 网络设备一般都具有允许远程登录的功能，远程登录给网络管理员带来很多方便，但同时也带来一定的网络安全隐患，远程管理时需采用加密方式管理。

第三十八条 通常在网络设备上可以设置相应的 ACL 限定可远程登录的主机在指定网段范围内，拒绝部分潜在的攻击者，保证网络安全。

5.6.8、 附则

第三十九条 本制度的解释权归吉林省某某单位。

第四十条 本制度自发布之日起生效。

.

附件 5-6-1 网络运维记录表（模板）

网络运维记录表

运维时间	运维人员	工作内容	处理方法	处理结果	备注

说明：工作内容至少包括：漏洞扫描、恶意代码查杀、补丁\病毒库升级、数据备份、数据

.

恢复、系统变更、操作回退、操作演练、恢复演练、应急演练等操作。

.

附件 5-6-2 违规外联及接入行为检查记录表（模板）

违规外联及接入行为检查记录表

检查时间	检查人员	违规人员	违规行为	处理方法	备注

.

5.7、系统安全管理制度

5.7.1、总则

第一条 为加强吉林省某某单位系统安全管理，明确岗位职责，规范操作流程，维护系统正常运行，确保计算机信息系统的安全，特制订本制度。

第二条 本制度适用于吉林省某某单位。

5.7.2、系统安全策略

第三条 由系统管理员根据业务需求和系统安全分析制定系统的访问控制策略，控制分配信息系统、文件及服务的访问权限。

第四条 对系统管理员用户进行分类，明确各个角色的权限、责任和风险，权限设定遵循最小授权原则。

第五条 由系统管理员定期对系统安装安全补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并采取磁盘或磁带对重要文件进行备份后，方可实施系统补丁程序的安装。

第六条 由安全管理员每月对系统进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补；形成漏洞扫描报告，内容包含系统存在的漏洞、严重级别和结果处理等方面。

.

第七条 各终端工作计算机未进行安全配置、未装防火墙或杀毒软件的，不得入网。各计算机终端用户应定期对计算机系统、杀毒软件等进行升级和更新，并定期进行病毒清查，不允许下载和使用未经测试和来历不明的软件、不要打开来历不明的电子邮件、以及不要随意使用带毒U盘等介质。

第八条 禁止未授权用户接入吉林省某某单位网络及访问网络中的资源，禁止未授权用户使用BT、电驴等占用大量带宽的下载工具。

第九条 任何员工不得制造或者故意输入、传播计算机病毒和其他有害数据，不得利用非法手段复制、截收、篡改计算机信息系统中的数据。

第十条 禁止利用扫描、监听、伪装等工具对网络和服务器进行恶意攻击，禁止非法侵入他人网络和服务器系统，禁止利用计算机和网络干扰他人正常工作的行为。

第十一条 计算机各终端用户应保管好自己的用户帐号和密码。严禁随意向他人泄露、借用自己的帐号和密码；严禁不以真实身份登录系统。计算机使用者更应定期更改密码、使用复杂密码。

第十二条 IP地址为计算机网络的重要资源，计算机各终端用户应在系统管理员的规划下使用这些资源，不得擅自更改。另外，某些系统服务对网络产生影响，计算机各终端用户应在系统管理员的指导下使用，禁止随意开启计算机中

.

的系统服务，保证计算机网络畅通运行。

第十三条 网络参数配置文档、重要计算机信息系统详细开发资料及其源程序等核心技术文档，由信息化管理处严格管理。

第十四条 系统核心技术文档资料的外借应有审批手续和记录，借阅人不得转借给他人，不得复制、泄露和引用具体技术内容。

5.7.3、 安全配置

第十五条 系统安全配置由系统管理员、安全管理员负责，其余任何人不得随意更改配置。

第十六条 安全配置的更改应有记录，由安全审计员负责审计。

5.7.4、 日志管理

第十七条 由系统运维人员依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作。

第十八条 由安全审计员定期对运行日志和审计结果进行分析，形成分析报告，报告内容包括帐户的连续多次登录失败、非工作时间的登录、访问受限系统或文件的失败尝试、系统错误等非正常事件。

.

5.7.5、 日常操作流程

第十九条 各应用系统的操作流程由各应用系统开发厂商提供，经业务部门进行确认，信息化管理处各业务部门工作人员在日常工作中按照操作流程执行。

5.7.6、 附则

第二十条 本制度的解释权归吉林省某某单位。

第二十一条 本制度自发布之日起生效。

.

附件 5-7-1 补丁测试记录（模板）

补丁测试记录

测试时间	测试设备/系统	升级前版本	测试记录	升级后版本	备注
			1）测试人员： 2）测试结果： 3）操作影响：		
			1）测试人员： 2）测试结果： 3）操作影响：		
			1）测试人员： 2）测试结果： 3）操作影响：		
			1）测试人员： 2）测试结果： 3）操作影响：		
			1）测试人员： 2）测试结果： 3）操作影响：		
			1）测试人员： 2）测试结果： 3）操作影响：		
			1）测试人员： 2）测试结果： 3）操作影响：		
			1）测试人员： 2）测试结果： 3）操作影响：		
			1）测试人员： 2）测试结果： 3）操作影响：		
			1）测试人员： 2）测试结果： 3）操作影响：		
			1）测试人员： 2）测试结果： 3）操作影响：		
			1）测试人员： 2）测试结果： 3）操作影响：		

.

附件 5-7-2 日志审计分析记录（模板）

日志审计分析记录

基本信息	
日志审计活动名称	
日志名称	
日志来源	
审计分析日期	
审计分析时间	
审计分析人员	
审计分析方法	□人工审计　□工具审计（工具名称：_____）
日志获取方式	
日志处理方式	
审计信息	
日志数据访问权限是否有效控制	
日志数据存储时间是否大于半年	
日志数据是否单独存储	
日志数据是否加密存储	
日志内容、元素、事件是否完整	
日志时间是否与标准时间同步	
通过审计发现源设备的安全隐患	
安全隐患处理方法	
其他问题	
审批信息	
审计人员签字	
主管领导签字	

.

5.8、恶意代码防范管理规定

5.8.1、 总则

第一条 为加强吉林省某某单位网络与信息系统安全保护，避免遭受恶意代码攻击和病毒感染，特制订此规定。

第二条 本规定适用于吉林省某某单位。

5.8.2、 恶意代码防范工作原则

第三条 禁止任何业务部门或员工以任何名义制造、传播、复制、收集恶意代码。

第四条 员工在使用计算机的任何时间内必须运行防病毒软件，进行定期得病毒检测和清除。未经许可，不得随意下载标准规定之外的防病毒软件或病毒监控程序。

第五条 在发布最新版本杀毒软件后，必须在规定期限内，将个人计算机的杀毒软件升级。

第六条 新购置的、借入的或维修返回的计算机，在使用前应当对硬盘认真进行恶意代码检查，确保无恶意代码之后才能投入正式使用。

第七条 软盘、光盘以及其它移动存储介质在使用前应进行病毒检测，严禁使用任何未经防病毒软件检测过的存储介质。

.

第八条 计算机软件以及从其它渠道获得的电脑文件，在安装或使用前应进行病毒检测，禁止安装或使用未经检测过的软件或带毒软件。

5.8.3、 职责

第九条 运维工作小组应制定防恶意代码和病毒管理办法并对执行情况进行检查。

第十条 各业务部门安全管理员的职责：

（一）对于已经实施安全域管理的系统，要定期进行从相关技术支撑单位获得相关升级支持，根据策略强制所有用户进行病毒代码更新；

（二）对于尚未进行安全域管理的系统，要定期进行从相关技术支撑单位获得相关升级支持。要在第一时间以邮件方式、书面、短信等方式通知所有负责用户进行升级，收到通知的用户在登陆局域网的当天要按照要求进行病毒代码升级，完成后以邮件方式、书面、短信方式回复安全管理员。安全管理员根据实际情况进行抽查；

（三）及时跟踪解决对用户反映的病毒问题；

（四）及时跟踪防病毒软件的升级情况，并及时将升级的版本及相关措施公布；

（五）对用户上报的病毒追踪其根源，查找病毒传播者；

（六）对于不能立即解决得病毒问题，应及时组织协同

.

相关的技术和业务人员进行跟踪解决，在问题解决前尽快采取相应措施阻止事件进一步扩大；

（七）对病毒的发作时间、发作现象、清除等信息进行维护、备案、并制作案例；

（八）日常病毒信息的公告和发布；

（九）对本部门员工进行病毒防治的教育和培训；

（十）相关工作日志（发送和接受）的保存和归档。

5.8.4、 工作要求

第十一条 各业务部门向外发布文件或软件时，应该用规定的防病毒软件检查这些该文件或软件，有病毒应及时清除，之后才能向外发布。

第十二条 对邮件中的附件在使用之前应该进行病毒检测，收到来历不明的邮件不要打开并及时通知安全管理员处理。

第十三条 如果发现本机感染了病毒，不管病毒从何处传播而来，都应该向安全管理员进行汇报，如果确认从别的机器传播而来的，还应该及时通知该机器的使用者，以便采取相应的防治措施。

第十四条 任何个人不得私自发布计算机病毒疫情。如果发现防病毒软件不能清除的病毒，在问题处理之前，还应禁止使用感染该病毒的文件，同时断开网络连接。

.

第十五条 应指定专人对网络和主机进行恶意代码检测并保存检测记录。

第十六条 用户有义务接受有关部门组织的恶意代码防范、防治的教育和培训。

5.8.5、 附则

第十七条 本规定的解释权归吉林省某某单位。

第十八条 本规定自发布之日起生效。

.

附件 5-8-1 恶意代码检查结果分析记录（模板）

恶意代码检查结果分析记录

基本信息	
恶意代码检查结果分析活动名称	
恶意代码检查结果报告名称	
恶意代码检查范围	
恶意代码检查操作人员	
恶意代码检查操作事件	
审计分析日期	
审计分析时间	
审计分析人员	
审计分析方法	□人工审计　□工具审计（工具名称：_____）
审计信息	
系统内是否感染恶意代码	
恶意代码感染设备名称	
恶意代码类型	□病毒　□木马　□恶意程序　□其他_____
恶意代码是否得到有效清除	
是否造成不良后果	
恶意代码感染原因	□互联网感染　□网络攻击　□内网感染 □误操作　□移动介质　□未知　□其他_____
恶意代码感染情况发展趋势	□增多　□减少　□爆发式感染　□常见病毒 □流行病毒
恶意代码感染通报情况	
其他问题	
审批信息	
审计人员签字	

.

主管领导签字	

.

5.9、密码使用管理制度

5.9.1、 总则

第一条 为规范吉林省某某单位信息系统帐号口令管理，保障各系统安全运行，特制订此制度。

第二条 本制度适用于吉林省某某单位。

5.9.2、 密码使用管理

第三条 员工应了解进行有效访问控制的责任，特别是密码使用和员工设备安全的责任。

第四条 员工应保证密码安全，不得向其他任何人泄漏。对于泄漏密码向造成的损失，由员工本人负责。

第五条 不要共享个人密码。

第六条 应避免在纸上记录密码，或以明文方式记录计算机内。

第七条 不要在任何自动登录程序中使用密码，如在宏或功能键中存储。

第八条 用户忘记密码时，管理员必须在对该用户进行适当的身份识别后才能向其提供临时密码。

第九条 常规情况下，用户至少每半年更改一次密码，避免再次使用旧密码或循环使用旧密码。

.

第十条 允许用户选择和变更他们自己的密码，并且包括确认程序，以便考虑到输入出错的情况;。

第十一条 当正在录入时，在屏幕上不显示密码。

5.9.3、 密码使用要求

第十二条 密码应由不少于8位的大小写字母、数字以及标点符号等字符组成。帐号口令必须是在必要时间或次数内不循环使用。

第十三条 密码应在90天内至少更换一次，对重要设备和系统可采用一次性口令方式进行认证。

第十四条 密码设置不得使用最近5次以内重复的口令；密码重复尝试5次以后应暂停该帐号登录。

第十五条 各级密码保管落实到人，密码所有人须妥善保存，各级密码不得以任何形式明文存放于可公共访问的设备中。

第十六条 采取有效措施，保证用户密码在传输和存储时的安全，例如对密码进行加密传输和保存。

第十七条 以下情况时相关密码必须立即更改并做好记录：

（一）掌握密码的网络管理人员离开岗位；

（二）工程施工、厂商维护完成；

（三）因工作需要，由相关厂家或第三方公司使用了登

陆帐号及密码后；

（四）一旦有迹象表明密码可能被泄露。

第十八条 当发生以下情况时，系统或帐号管理人员应立即取消帐号或更改密码，并做好记录：

（一）帐号使用者已经离开；

（二）帐号使用者由于工作的变动不再需要访问权限；

（三）帐号使用者违背了有关密码管理规定；

（四）发生其他情况，由上级主管人员认为不应再具有访问权限的。

第十九条 系统管理员修改帐号密码时，应提前（或同时）通知帐号使用人，以免影响其正常使用。

第二十条 系统的超级管理员帐号的密码属于系统最高机密，应该严格限定使用范围；其他人员确因工作需要而使用超级管理员帐号和密码的，应遵守“帐号管理”中，有关超级管理员帐号的管理规定。

第二十一条 用户应对系统中的帐户密码进行定期检查核实，对不符合要求账户密码及时进行整改。

第二十二条 第三方人员使用系统账号权限时，同样需要遵守“最小权限原则”。

5.9.4、 附则

第二十三条 本制度的解释权归吉林省某某单位。

.

第二十四条 本制度自发布之日起生效。

.

5.10、 变更管理制度

5.10.1、 总则

第一条 为规范吉林省某某单位信息系统变更管理流程，控制变更产生的影响，减少变更发生的问题，保障信息系统安全运行和使用，特制订此制度。

第二条 本制度适用于吉林省某某单位。

5.10.2、 变更定义

第三条 员工应了解进行有效访问控制的责任，特别是密码使用和员工设备安全的责任。

第四条 变更是指对系统/平台需求的增补或修改，所做增补或修改可能会影响生产环境的稳定性。变更区域包括但不限于硬件、系统软件(OS)、应用软件、网络、环境(冷却、供热等等)以及服务文件(如服务等级协议)。变更又分为计划型变更和应急变更。

第五条 影响系统安全状态的变更如：

（一）新的版本或修订；

（二）作业系统执行状态的变化；

（三）作业系统调度变更；

.

（四）网络设备软件安装补丁、更新。

（五）增/减软件或补丁；

（六）软件修改或增强；

（七）操作系统升级；

（八）增加/移动/变更相关业务处室硬件配置，包括磁盘、磁带、CPU 等；

（九）硬件和网络设备变更。

第六条 对于有计划的变更申请需要进行审批，变更前应预留一定的时间通知变更有关各方，通知时限取决于变更的严重程度。

第七条 应急变更是为了改正生产环境下的某一个重要问题而必须立即实施的变更，应急变更也需要进行审批，但在紧急情况下可免去通知时间和正常的变更程序要求。

5.10.3、 变更过程

第八条 变更申请人填写变更申请表提交各业务部门领导审批，变更申请应在计划变更实施日期之前预留必要的准备时间。

第九条 变更申请表中需要描述以下内容：

（一）变更内容、变更原由、实施时间和期限、执行人以及联络方式；

（二）对相关业务部门/用户/系统/平台的影响；

.

（三）特殊的变更指示；

（四）变更前的准备工作；

（五）变更执行步骤；

（六）保证变更成功的测试方法；

（七）变更失败时应采取的倒回程序。

第十条 变更申请人将审批的变更申请表提交运维小组。

第十一条 运维小组在变更计划执行日期前2天对提交的变更申请进行批复，通知申请单位，对于批准的变更申请予以存档。

第十二条 变更实施前，执行人应通知相关业务部门的运行操作人员，以便变更进行时监控变更期内系统和服务的正常运。

第十三条 如发现对服务有影响，维护人员应通知实施者，如果是因变更导致的影响，变更执行人应立即对问题进行调查，如问题严重，变更执行人应采取紧急恢复措施或倒回程序，和维护人员配合，务求恢复服务。

第十四条 运行操作日志中应记录变更事件以备后查。

第十五条 变更执行人在执行后要测试变更结果并验证执行的成功与否。如果结果表明不成功，变更执行人应采取回退措施将变更倒回到变更执行前的状态并进行测试，保证倒回成功。

.

第十六条 变更程序开发完成后由实施方或协同各业务处室制订测试文档（包含测试用例）进行测试，并填写测试结果及签字确认。如未通过规定的测试，变更程序不得被移植入生产环境。变更程序的测试必须在独立于生产环境的测试环境中进行。

第十七条 完成变更步骤后，变更执行人在离开现场前要通知各业务处室维护管理人员，进行验收程序。负责程序移植的人员需要进行移植情况的检查，留下书面的检查报告并签字确认。

第十八条 变更执行人需待运行维护人员确定一切检查妥当方可以离开，确定变更成功。

第十九条 如果变更实施成功，申请人通知运维小组关闭变更申请并提供实际实施时间和结果。

第二十条 运维小组要确保相关业务处室的运行操作已更新所有的相关文件和记录。

第二十一条 应急变更属于特殊的变更申请,可以因问题紧迫取得特别批准，一般需要在变更申请批准后 24 小时内实施完成。申请人应随后创建一份变更申请，并补充相应的测试及审批文档。

5.10.4、 变更过程职责

第二十二条 对信息系统和应用程序的变更都需根据

.

运维小组下发的软件版本更新公文或填写规定格式的变更申请表单，由运维小组审批签字。表单应包含变更时间、申请人、变更原由、变更名称、实施时间和期限、影响分析、变更方案、审批意见、归档日期等内容。

第二十三条 运维小组是变更管理的职能部门,主要职责为：

（一）审核变更申请的准确性；

（二）确认变更申请的记录信息的完整性；

（三）确保执行计划和变更失败倒回程序的质量；

（四）对变更申请予以批复；

（五）监督变更申请的执行情况；

（六）确保相关业务处室根据变化情况修订有关文件和记录。

第二十四条 各信息系统维护人员职责：

（一）监督变更期间生产系统/平台的正常服务情况；

（二）在变更申请超出限制或影响服务时，警告执行者采取恢复/倒回措施；

（三）确保倒回程序的实施足以恢复正常服务；

（四）根据情况的变化修订有关的文件和记录；

（五）监督变更期间的出错报告并在报告有意外服务影响时，通知执行人和相关业务处室。

第二十五条 变更执行人员职责：

.

（一）执行已获批准的变更申请；

（二）变更失败时执行倒回程序。

第二十六条 变更申请人职责：

（一）确保变更可执行；

（二）列出变更范围；

（三）提出变更申请；

（四）指出变更影响的区域和相关各方；

（五）编制变更执行计划；

（六）编制倒回程序；

（七）确保必要时变更影响的用户都能得到通知、授权及批准。

5.10.5、 附则

第二十七条 本制度的解释权归吉林省某某单位。

第二十八条 本制度自发布之日起生效。

.

5.11、 备份与恢复管理制度

5.11.1、 总则

第一条 为加强吉林省某某单位对各类存储数据的备份和恢复管理，保障应用系统的正常运行，特制订本制度。

第二条 本制度适用于吉林省某某单位。

5.11.2、 备份恢复管理

第三条 由业务系统主管部门与信息化管理处根据信息系统的资产价值以及系统故障对业务正常开展造成的影响进行相应的备份需求分析，确保系统恢复的目标，如：关键业务功能、恢复的优先顺序、恢复的时间范围等。

第四条 信息化管理处要对定期备份的重要业务信息、系统数据及软件系统形成备份清单（附件 5-11-1）。

第五条 信息化管理处负责服务器端业务信息、系统数据及软件系统的备份。

第六条 数据备份和恢复策略文档，由业务系统主管部门与信息化管理处在委托运行合同中指定备份策略，并由信息化管理处细化，业务系统主管部门审核确认（附件 5-11-2）。

第七条 信息化管理处每年检查一次备份介质，保证在

.

紧急情况时可以使用。

第八条 信息化管理处每年执行一次恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

第九条 信息化管理处对所有备份恢复活动进行文档记录，其内容包括备份时间、备份内容、备份操作、备份介质存放等（附件 5-11-3）。

5.11.3、 附则

第十条 本制度的解释权归吉林省某某单位。

第十一条 本制度自发布之日起生效。

.

附件 5-11-1 定期备份清单

序号	需备份系统名称	备份周期	系统主管部门	联系人姓名	联系方式

.

附件 5-11-1 数据备份和恢复策略文档（模板）

单数据备份和恢复策略文档

数据备份有不同方式（如下所述）。根据这些方式的不同特点和应用范围，XXX 应该根据实际情况和具体的数据备份应用需求选择不同的备份方式（比如对于重要的、需要持续运作的业务系统可以采用双机热备份或 SAN 备份方式）。

XXX 数据备份与恢复策略

备份数据的存放场所：备份存储介质必须放置于安全位置，防止因异常事故发生而导致备份数据与业务数据被同时破坏。

文件命名规则：“应用系统名称+备份日期+备份方式（如全备、增备）”

备份介质替换频率：3 个月

数据离站传输方法：由专人负责备份介质的离站传输，确保传输过程的安全。

备份方式：根据系统数据的重要程度以及数据量的大小，采用不同的备份方式相结合，如全备份、增量备份。

根据数据的重要程度和更新频率设定备份周期。建议**备份周期**如下：

1） 应用系统每次修改后备份 1 次，并保留最新的版本；

2） 每周备份服务器上的相关文档；

3） 每周完全备份 Oracal、SQLServer 等数据库系统上的数据.；

4） 每月将主要数据刻录一张光盘作为历史数据保存；

5） 网站有重大改版时备份原网站信息；

6） 如遇系统有重大改动或更新,需要在改动之后当日进行备份。

备份介质：备份介质包括光盘、磁盘、磁带等；备份存储介质必须放置于安全位置，防止因异常事故发生而导致备份数据与业务数据被同时破坏。

备份介质保存期：由业务系统主管部门确定备份介质保存期，在保存期限过后运维部门可提交申请（备份介质清除或销毁申请单如下）对备份介质进行信息清除和销毁处理。

.

附件 5-11-2 备份介质清除或销毁申请单（模板）

备份介质清除或销毁申请单

运维部门		**申请人**	
申请人联系方式		**申请日期**	
备份介质内容			
备份介质保存期	年　月—　年　月	**处理方式**	清除□　销毁□
业务主管部门领导审批	签名：　日期：		
运维部门执行纪录	签名：　日期：		

.

附件 5-11-3 数据备份和恢复记录（模板）

备份介质清除或销毁申请单

序号	操作日期	备份内容	备份操作（备份或恢复）	备份介质存放位置	主管单位	操作人员（运维部门）	备注
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							

.

5.12、 安全事件报告和处置管理制度

5.12.1、 总则

第一条 为规范和加强吉林省某某单位安全事件报告和处置管理，明确安全事件的现场处理、事件报告和后期恢复的管理职责，保障系统的安全稳定运行，特制订本制度。

第二条 本制度适用于吉林省某某单位。

5.12.2、 安全事件定级

第三条 安全事件定义：信息安全事件是由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或对社会造成负面影响的事件。

第四条 安全事件分类：吉林省某某单位网络中的安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件及其他事件等。

（一）有害程序事件：包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件；

（二）网络攻击事件：包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、

.

干扰事件和其他网络攻击事件；

（三）信息破坏事件：包括信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件；

（四）信息内容安全事件：包括通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件；

（五）设备设施故障：包括软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障；

（六）灾害性事件：包括由自然灾害等其他突发事件导致的网络与信息安全事件；

（七）其他事件：包括不能归为以上6个基本分类的信息安全事件。

第五条 安全事件分级

安全事件分级原则：根据信息系统中断的时间长短、影响范围，以及信息系统中的数据丢失或被窃取、篡改、假冒时对国家安全和社会稳定构成威胁的严重程度或者造成的经济损失来对安全事件进行等级划分。

根据以上原则，同时参照《GB/Z20986-2007 信息安全技术 信息安全事件分类分级指南》，将吉林省某某单位网络中的安全事件分为四级：特别重大(I级)、重大(II级)、较大(III级)、一般(IV级)。

.

（一）特别重大安全事件（I 级）

是指能够导致特别严重影响或破坏的信息安全事件，包括以下情况：使特别重要的信息系统遭受特别严重的系统损失（比如全国联网的业务应用系统中断服务 2 小时以上等）；产生特别重大社会影响。

（二）重大安全事件（II 级）

是指能够导致严重影响或破坏的信息安全事件，包括以下情况：使特别重要的信息系统遭受严重的系统损失，或使重要的信息系统遭受特别严重的系统损失；产生重大的社会影响。

（三）较大安全事件（III 级）

是指能够导致较严重影响或破坏的信息安全事件，包括以下情况：使特别重要的信息系统遭受较大的系统损失，或使重要的信息系统遭受严重的系统损失、一般信息系统遭受特别严重系统损失；产生较大的社会影响。

（四）一般安全事件（(IV 级）：

是指不满足以上条件的信息安全事件，包括以下情况：使特别重要的信息系统遭受较小的系统损失，或使重要的信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失；产生一般的社会影响。

.

5.12.3、 安全事件报告和处置管理

第六条 网络与信息系统重大信息安全事件的报告和处置管理工作坚持“统一领导、归口负责”的原则。

第七条 发生信息安全事件的单位首先以口头方式立即向信息化管理处报告。同时应当立即对发生的事件进行调查核实、保存相关证据，并在事件被发现或应当被发现时起5小时内将有关材料报至数据管理中心（附件5-12-1）。

第八条 对于重大的信息安全事件，信息化管理处接到报告后，应当立即上报吉林省某某单位网络安全与信息化工作领导小组，并负责组织协调相关成员单位对事件进行调查和处理。

第九条 发生重大信息安全事件的单位应当在事件处理完毕后5个工作日内将处理结果报信息化管理处备案（附件5-12-2）。

第十条 发生重大信息安全事件的单位应当按照规定及时如实地报告事件的有关信息，不得瞒报、缓报或者授意他人瞒报、缓报。

第十一条 任何单位或个人发现有瞒报、缓报、谎报重大信息安全事件情况时，有权直接向吉林省某某单位网络安全与信息化工作领导小组举报。

第十二条 发生重大信息安全事件，有关责任单位、责任人有瞒报、缓报和漏报等失职情况，吉林省某某单位网络

.

安全与信息化工作领导小组将予以通报批评；对造成严重不良后果的，将视情节由有关主管部门追究责任领导和责任人的行政责任；构成犯罪的，由有关部门依法追究其法律责任。

第十三条 恢复重建工作按照“谁主管谁负责，谁运行谁负责”的原则，由事发单位负责组织制定恢复、整改或重建方案，报相关主管部门审核实施。

5.12.4、 安全事件报告和处理程序

第十四条 信息安全事件发生后，事发单位应立即启动相关安全事件报告和处理程序，实施处置并及时报送信息。

（一）事发单位先期处置，采取各种技术措施，及时控制事态发展，最大限度地防止事件蔓延。

（二）快速判断事件性质和危害程度。尽快分析事件发生原因，根据网络与信息系统运行和承载业务情况，初步判断事件的影响、危害和可能波及的范围，提出应对措施建议。

（三）事发单位在先期处置的同时要按照预案要求，及时向上级主管部门报告事件信息。

（四）做好事件发生、发展、处置的记录和证据留存。

第十五条 事件信息一般包括以下要素：事件发生时间、发生事故网络信息系统名称及运营使用管理单位、地点、原因、信息来源、事件类型及性质、危害和损失程度、影响单位及业务、事件发展趋势、采取的处置措施等。

.

第十六条 II级响应:吉林省某某单位网络安全与信息化工作领导小组启动II级响应，统一指挥、协调、组织应急处置工作。

（一）启动指挥体系。吉林省某某单位网络安全与信息化工作领导小组组织专家顾问组专家、人才库专家及专业技术人员研究对策，提出处置方案建议，为领导决策提供支撑。

（二）掌握事件动态。事件影响单位及时将事态发展变化情况和处置进展情况及时上报，吉林省某某单位网络安全与信息化工作领导小组组织全面了解网络与信息系统运行情况，及时汇总有关情况并上报。

（三）处置实施。控制事态防止蔓延。现场处理组全力组织事发单位及应急队伍，采取各种技术措施、管理手段，最大限度地阻止和控制事态发展。

（四）做好处置消除隐患。现场指挥部组织专家、应急技术力量、事发单位尽快分析事件发生原因、特点、发展趋势，快速制定具体的解决方案，组织实施处置，对业务连续性要求高的受破坏网络与信息系统要及时组织恢复。

第十七条 III级响应:事件发生单位主管部门启动III级响应，按照相关预案进行事件处置，信息化管理处根据需要指导、检查、协助应急处置工作。

（一）启动指挥体系。信息化管理处组织相关专家指导现场处置。

.

（二）掌握事件动态。现场处理组及时了解事发单位主管范围内的信息系统是否受到事件的波及或影响，并将有关情况及时报吉林省某某单位网络安全与信息化工作领导小组。

（三）处置实施。控制事态防止蔓延。现场处理组及时采取技术措施阻止事件蔓延；吉林省某某单位网络安全与信息化工作领导小组向XXX其余单位发布预警信息，督促、指导相关运行单位有针对性地加强防范。

（四）尽快分析事件发生原因，并根据原因有针对性地采取措施，恢复受破坏信息系统正常运行。

第十八条 IV级响应：事件发生单位启动IV级响应，按照相关预案进行事件处置。

（一）启动指挥体系。事件发生单位负责同志及时赶赴现场，组织协调、指挥所属技术力量进行事件处置工作，必要时请求信息化管理处支援处置。

（二）掌握事件动态。事发单位负责将事件信息、处置进展情况及时向吉林省某某单位网络安全与信息化工作领导小组报告。

（三）处置实施。根据需要，吉林省某某单位网络安全与信息化工作领导小组有关人员及时赶赴现场，指导、检查事发单位开展事件处置工作，协调相关专家、技术队伍参加事件处置。

.

（四）尽快分析事件发生原因，并根据原因有针对性地采取措施，恢复受破坏信息系统正常运行。

5.12.5、 附则

第十九条 本制度的解释权归吉林省某某单位。

第二十条 本制度自发布之日起生效。

.

附件 5-12-1 网络安全行为告知书（模板）

网络安全行为告知书

为保证通信以及互联网的网络与信息安全，维护国家安全和社会稳定，保障社会公众利益和公民合法权益，保障其他客户的合法权益，根据《中华人民共和国电信条例》、《互联网信息服务管理办法》、《互联网安全保护技术措施规定》、《计算机信息网络国际安全保护管理办法》、《中华人民共和国计算机信息系统安全保护条例》、《互联网电子公告服务管理规定》以及其他国家有关法律、法规和我单位网络安全相关规定。请您自觉遵守以下规定。

1、不得利用通信或互联网络制作、复制、发布、传播含有以下内容的信息：

（一）反对宪法所确定的基本原则的；

（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

（三）损害国家荣誉和利益的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）破坏国家宗教政策，宣扬邪教和封建迷信的；

（六）散布谣言，扰乱社会秩序，破坏社会稳定的；

（七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

（八）侮辱或者诽谤他人，侵害他人合法权益的；

（九）含有法律、行政法规禁止的其他内容的。

2、应建立和健全以下信息网络安全保护技术措施：

（一）加强自身网络安全政策法规及相关规章制度的学习及落实。

（二）在计算机主机、网关和防火墙上建立完备的系统运行日志，日志保存的时间至少为 180 天。

（三）对于互联网信息，用户上传的公共信息在网站上发布前，须进行人工审核后，方能上网发布。

（四）系统用户部门的各级主管人员有责任教育、监督本企业职工严格遵守以上条款。

.

3、不从事下列危害计算机信息网络安全的活动：

（一）未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的；

（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；

（四）故意制作、传播计算机病毒等破坏性程序的；

（五）其他危害计算机信息网络安全的。

4、系统用户应遵守安全保护管理制度、落实各项安全保护技术措施，保障本单位网络运行安全和信息安全。

5、系统用户应严格遵守国家有关法律法规，做好本单位信息网络安全管理工作，设立信息安全责任人和信息安全审查员，对发布的信息进行实时审核，发现有以上 1、2、3 点所列情形之一的，应当保留有关原始记录并在二十四小时内向主管领导报告。

6、本单位一旦发现系统用户违反上述情况，有权立即停止用户的网络接入，用户须自行承担由此造成的一切后果和责任。

吉林省某某单位

_____年___月___日

.

附件 5-12-2 信息安全事件报告表（模板）

信息安全事件报告表

单位名称		**报告人**	
联系电话		**通讯地址**	
报告时间		**电子邮件**	
发生信息安全事件的网络与信息系统名称及用途			
负责部门		**负责人**	
信息安全事件的简要描述（如以前出现过类似情况也应加以说明）			
初步判定的事故原因			
当前采取的应对措施			
本次信息安全事件的初步影响状况	事件后果	☐业务中断 ☐系统破坏 ☐数据丢失 ☐其他_____	
	影响范围	☐单台主机 ☐___台主机 ☐整个信息系统 ☐ 整个局域网 ☐_____	
	严重程度	☐极严重 ☐很严重 ☐严重 ☐一般 ☐不严重 ☐_____	
联系方式	值班电话： 传真： 邮件地址：		

.

附件 5-12-3 系统异常事件处理记录（模板）

系统异常事件处理记录

序号	事件类型	发生原因	发生时间	影响范围	补救措施	最终结果	处理人
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							

.

5.13、 应急预案管理制度

5.13.1、 总则

第一条 为科学应对吉林省某某单位信息安全突发事件、建立健全信息安全应急响应机制，有效预防、及时控制和最大限度地消除信息安全各类突发事件的危害和影响，特制定本应急预案。

第二条 本制度适用于吉林省某某单位。

5.13.2、 组织机构与职责

第三条 设立信息安全应急指挥办公室（简称“应急指挥办公室”），应急指挥办公室主要成员由信息化管理处技术人员组成，主要职责是：

（一）承担值守应急工作；

（二）收集、分析工作信息，及时上报重要信息；

（三）负责吉林省某某单位网络与信息安全的监测预警和风险评估控制、隐患排查整改工作；

（四）组织制订、修订网络与信息安全突发事件相关的应急预案；

（五）负责组织协调网络与信息安全突发事件应急演练；

.

（六）负责对吉林省某某单位网络与信息安全突发事件的宣传教育与培训。

第四条 借助外部力量成立网络与信息安全专家顾问组，专家顾问组的职责：

（一）在网络与信息安全突发事件预防与应急处置时，提供咨询与建议，必要时参与值班；

（二）在制定网络与信息安全应急有关规定、预案、制度和项目建设的过程中提供参考意见；

（三）及时反映网络与信息安全应急工作中存在的问题与不足，并提出改进建议；

（四）对吉林省某某单位网络与信息安全突发事件发生和发展趋势、处置措施、恢复方案等进行研究、评估，并提出相关建议；

（五）参与网络与信息安全突发事件应急培训及相关教材编审等工作。

5.13.3、 安全事件应急预案框架

第五条 应急指挥办公室根据需要，应编制信息安全事件应急预案，以指导安全事件的处理机制和流程。

第六条 安全事件应急预案框架的内容：

（一）启动应急预案的条件。描述启动每个计划前应遵循的过程；

.

（二）应急处理流程。描述危及业务操作的事故发生之后所要采取行动的应急程序；

（三）描述将基本业务活动或支持服务移到替代的临时地方，并在要求的时段内使业务过程回到运行状态的动作的回退程序；

（四）恢复和复原未完成时应遵循的临时操作程序；

（五）描述恢复正常业务操作的动作的恢复程序；

（六）规定如何及何时要检验该计划的维护时间表，以及维护该计划的过程；

（七）教育和培训活动，用来创建理解业务连续性过程，确保过程持续有效；

（八）各个人的职责，描述谁负责执行计划的哪个部分。若需要，应指定可替换的人；

（九）实行紧急的、回退和恢复程序所需的关键资产和资源。

5.13.4、 应急响应程序

第七条 系统故障应急预案

（一）当发生系统故障事件时，发现人应及时通知信息化管理处，同时根据情况及时上报吉林省某某单位网络安全与信息化工作领导小组办公室；

（二）信息化管理处领导组织安全管理员、系统管理员

.

及网络管理员等相关单位和人员及时分析事件发生源头，切断事件源头，控制事件范围，必要时停止系统运行；

（三）安全管理员应及时查看安全审计日志对异常事件发生源头、发生原因、影响范围做出判断，并提出补救措施；

（四）系统管理员立即停止发生问题的应用系统，对异常事件内容和范围予以确认；

（五）针对事件原因查找系统漏洞，提出系统安全策略调整方案，并报数据管理中心审批，《应急处置审批表》见0；

（六）审批通过后根据系统安全策略调整方案，对安全设备、应用系统等的安全控制策略做出相应调整，确认无误后恢复系统运行；

（七）安全管理员详细填写《系统异常事件处理记录》（0），并上报。

第八条 网络攻击应急预案

（一）网络管理员根据安全设备的报警和审计日志，确定攻击目标和攻击来源；

（二）通知系统管理员对攻击目标采取关闭或隔离措施，详细检查被攻击系统是否留有恶意代码，更改密码增强安全防范策略，必要是对系统和数据进行紧急备份；

（三）网络管理员对攻击来源进行隔离，分析原因，停止攻击行为，调整安全防范策略；

（五）网络管理员、系统管理员和安全管理员在对系统

.

进行安全评估后，恢复系统上线运行；

（六）安全管理员详细填写《系统异常事件处理记录》（0），对于恶意攻击上报有关主管部门。

第九条 病毒爆发应急预案

（一）安全管理员根据安全设备和网络杀毒软件的报警和日志，分析攻击来源，对攻击来源和攻击区域及时采取隔离措施；

（二）对重要的网络服务器和业务应用系统紧急备份，防止因病毒造成数据丢失，必要时可暂停系统运行；

（三）及时通知防病毒厂商，上报病毒爆发情况并寻求技术支持；

（四）获得处理建议后及时通过网站、电话等渠道公布并通知各部门网络安全员处理措施，控制病毒进一步传播、升级病毒库、清除病毒；

（五）分析病毒产生原因，传播途径，采取补救措施，纠正违规行为；

（六）安全管理员、系统管理员和网络管理员在对系统进行安全评估，确认病毒已得到控制或清除后，恢复系统上线运行；

（七）安全管理员详细填写《系统异常事件处理记录》（0），对于恶意制造或传播病毒的情况根据情况上报有关部门。

.

第十条 机房突发事件应急预案

（一）火警。值班人员要随时提高警惕，如发现机房内有异常气味，应仔细、认真地巡视机房各处,直到查清原因，确实无危险情况为止。 如发现机房内有烟雾，甚至火焰。首先切断电源（每个值班人员均应清楚电源开关位置并确保其畅通无阻)。对烟雾产生处，应检查原因，尽力扑灭。尤其应注意活动地板下的情况。对火情，一方面要尽快报警，同时要采取一切措施控制并扑灭火焰。火警电话：119 。

（二）水警。机房内如有水管破裂等严重水情时，要切断电源，然后设法排水，保护机房内各种设备的安全。对无法控制的严重水情，要立即报警。机房顶部漏水时，应设法用容器及塑料布保护机房各种设备不被淋湿。情况严重时应切断电源，并通知维修部门采取必要的措施。

（三）停电。网络系统因停电而启动暂停和恢复程序统一由系统管理员负责，如遇紧急情况需要由其他人启动，应得到系统管理员或信息化管理处领导授权；接到停电通知后，系统管理员应提前一天通过有效方式发布通知公告，通知内容应包括网络暂停原因、暂停时间及恢复时间等事项；如遇重大故障或系统受到攻击，需停机进行维护时，系统管理员应及时通知业务主管部门。为保证系统暂停程序有足够的时间，系统暂停应在停电前一小时开始操作；系统恢复应在确认来电后半小时内启动；发现意外停电应及时通知安全

.

保密管理员和系统管理员，并通知单位领导。询问信息化管理处，确定停电原因和初步恢复时间，如无法及时恢复系统，系统管理员应及时正常地关闭重要的网络设备、服务器、UPS和主电源。通知部门领导和重要部门，报告采取的措施及恢复供电和系统运行时间。确认供电恢复后，启动网络设备和服务器恢复系统运行。

第十一条 网络设备及应用服务器异常事件的应急预案

（一）信息化管理处组织安全管理员、系统管理员、网络管理员对网络设备及应用服务器异常事件进行原因分析；

（二）及时发布信息对事件原因、处理措施及恢复时间进行通知公告；

（三）如属于硬件故障及时启用备用设备，并将故障设备报修；

（四）如属于软件故障根据故障程度进行紧急调试或启用最近一次备份进行数据恢复；

（五）系统管理员详细填写《系统异常事件处理记录》（0）。

5.13.5、 应急预案审查管理

第十二条 应急指挥办公室定期对应急预案进行审查，根据实际情况，如演练过程中出现的问题等对内容进行更

.

新，以便更贴合吉林省某某单位实际情况。

5.13.6、 应急预案培训

第十三条 为确保应急预案有效运行，应急指挥办公室应定期或不定期地举办不同层次、不同类型的培训班或研讨会，以便不同岗位的应急人员都能全面熟悉并掌握信息安全应急处理的知识和技能。

5.13.7、 应急预案演练

第十四条 为提高信息安全突发事件应急响应水平，应急指挥办公室应每年至少组织一次预案演练；检验应急预案各环节之间的通信、协调、指挥等是否符合快速、高效的要求。通过演练，进一步明确应急响应各岗位责任，对预案中存在的问题和不足及时补充和完善。

5.13.8、 附则

第十五条 本制度的解释权归吉林省某某单位。

第十六条 本制度自发布之日起生效。

.

附件 5-13-1 应急处置审批表（模板）

应急处置审批表

基本信息			
事发地点		发生时间	
事发单位		报警时间	
起　　因		初定级别	
影响范围			
损失情况			
协调小组会议或领导决定应急处置意见			
核定事件级别			
是否启动应急预案			
总指挥			
现场总指挥			
是否发布预警或公告			
处置意见	领导（签名） 月　日　时　分		
是否应急扩大	领导（签名） 月　日　时　分		
应急结束	领导（签名）		

.

	月　日　时　分

.

附件 5-13-2 应急预案评审及审批意见（模板）

应急预案评审及审批意见

安全方案基本信息			
预案名称			
编制单位		**编制人员**	
编制时间		**评审类型**	□新建 □修订 □变更
所属系统			
内容简介			
相关附件			

评审记录			
评审专家	**所在单位**	**联系方式**	**评审意见**

审批意见	
信息安全负责人审批意见	负责人签字：　　_____年___月___日
网络安全与信息化工作领导小组审批意见	负责人签字：　　_____年___月___日
主管部门审批意见	负责人签字：　　_____年___月___日

.

第六章 其他管理制度

.

6.1、安全设备运行维护规范

6.1.1、 总则

第一条 为统一吉林省某某单位信息化管理处管理人员对吉林省某某单位信息系统中安全设备的运行维护规范，特制定本规范。

第二条 本规范适用于吉林省某某单位。

6.1.2、 适用产品范围

第三条 吉林省某某单位信息系统中的所有相关安全设备实施必须执行本规定，包括：

（一）安全防护类产品，如UTM、防火墙等；

（二）恶意代码防护类产品，如防病毒软件；

（三）监测审计类产品，如IDS、网络通讯协议分析系统等；

6.1.3、 安全策略配置规范

第四条 安全设备部署规范

（一）安全防护类产品：吉林省某某单位所有局域网内的出网连接必须通过安全防护类产品进行防护。安全防护类

.

产品至少部署在以下几个方面：

1. 互联网接入区；

2. 广域网接入区；

3. 内部各个区域边界与核心交换机之间。

（二）恶意代码防护类产品:对吉林省某某单位的整体网络建立有效的、多层次的恶意代码防护体系，恶意代码防护类产品应分别部署到网关、邮件服务器、应用服务器以及客户端，并采用集中管理的方式。

（三）监测审计类产品：吉林省某某单位信息系统中的重点服务器网段都应部署监测审计类产品。

第五条 安全设备策略配置规范

（一） 安全防护类产品策略配置规范如下：

1. 默认状态下拒绝通信：对于未明确允许的连接路径和互联网服务，必须通过安全防护类产品锁死，所有可允许通过的服务必须得到信息化管理处的批准并备案；

2. 所有访问吉林省某某单位网络的入站通信（除普通互联网用户外）必须通过统一部署的 VPN 网关进行加密；

3. 对所有的重要网段进行子网的划分；

4. 互联网出口安全防护产品必须使用网络地址转换功能，各区域间的安全防护产品采用网桥的方式透明接入网络中，并启用访问控制功能；

.

5. 除普通的互联网用户外，对外服务系统应当使用动态口令或数字证书对用户进行认证；

6. 对所配策略应做出相应的注释，标明该策略的作用范围；对于临时的配置变更策略，应在《安全设备配置变更申请表》（附件 6-1-1）中注明该策略生效时间，系统管理员配置临时策略时应对其添加时间限制策略。

（二）恶意代码防护类产品策略配置规范如下：

1. 设定每日进行预约更新；

2. 每日自动检测客户端的恶意代码定义文件是否都已经更新到最新版本；

3. 透过管理主控台，每周对各产品是否都已正常更新到新版的病毒定义状态进行检查；

4. 每周检查防病毒控制端软件的扫描记录文件；

5. 每两周对 PC 进行一次扫描；

6. 每月对服务器执行全面扫描,应当生成月报表记录。

（三）监测审计类产品策略配置规范如下：

1. 监测审计类产品监控范围应当包括重要应用服务器、各级网络设备等；

2. 监控策略配置为全策略，并不断优化。

6.1.4、 安全运维规范

第六条 报告及日志管理规范

.

（一） 安全防护类产品报告及日志管理规范：

1. 对于安全防护类产品的配置参数、已启用服务和允许的连接等任何变化以及意外情况的处理，必须予以记录。另外，所有违背安全策略的可疑行为也必须予以记录；

2. 至少保留两周日志，并保证日志的完整性；

3. 每月生成一次安全防护类产品运行状况的报告。

（二） 恶意代码防护类产品报告及日志管理规范：

1. 基于不同应用层次和操作系统上的恶意代码防护类产品必须进行实时监控，建立系统内部完整的层次化更新体系，收集和汇总网络范围内的病毒事件，并可以通过单一节点进行恶意代码防护类产品的日常管理。对于防病毒软件配置参数、部署情况的任何变化以及意外情况的处理，应当予以记录。

2. 至少保留六个月日志，并保证日志的完整性；

3. 当恶意代码防护类产品运行发生问题时，系统管理员应进行记录，并向安全管理员提交报告。

（三） 监测审计类产品报告及日志管理规范：

1. 对于配置参数、部署情况的任何变化以及意外情况的处理，必须予以记录。另外，所有违背安全策略的可疑行为也必须予以记录；

2. 至少保留两周日志，并保证日志的完整性；

3. 每月生成一次监测审计类产品运行状况的报告。

.

第七条 安全产品备份管理规范

（一） 应当每日对安全产品日志进行自动增量备份；

（二） 至少每个月对安全产品日志、配置文件、报告等进行全备份；

（三） 当配置发生变化或遇紧急事件的前后必须对这些数据进行全备份。

第八条 定期审查规范

（一） 安全防护类产品定期审查规范：

1. 必须每个月对安全防护类产品进行审查。审查内容至少必须包括对配置参数、启用的服务、允许的连接、日志以及安全措施是否充分等问题的考虑；

2. 必须每月使用漏洞扫描软件对安全防护类产品进行一次安全评估；

3. 审查必须由系统管理员或熟练的专业技术人员进行。

（二） 恶意代码防护类产品定期审查规范

1. 必须每周对恶意代码防护类产品的更新、病毒爆发事件、病毒清除等情况进行审查；

2. 必须每个月对恶意代码防护类产品的部署、策略管理、日志以及安全措施是否充分等进行审查；

3. 审查必须由系统管理员或熟练的专业技术人员进行。

.

（三） 监测审计类产品定期审查规范

1. 必须每个月对监测审计类产品进行审查。审查内容至少必须包括对配置参数、日志以及安全措施是否充分等问题的考虑；

2. 审查必须由系统管理员或熟练的专业技术人员进行。

第九条 日常维护规范

（一） 必须每周监控安全产品的运行状态；

（二） 安全产品的升级必须得到信息化管理处的书面批准，升级前必须对系统的变更进行测试。

第十条 配置变更管理规范

（一）当应用系统、网络系统出现变更需对安全设备的配置进行变更时，变更申请人应填写《安全设备配置变更申请表》，说明变更原因，系统管理员负责实施安全设备的配置变更操作，配置变更后应进行至少 3 小时的监控，若变更未达到预期效果，应向安全管理员反馈，并进行相关处理。

（二）系统管理员应填写《安全设备配置变更记录表》(附件 2)，及时备份安全设备的最新配置信息，并妥善保存。

6.1.5、 附则

第十一条 本规定的解释权归吉林省某某单位。

第十二条 本规定自发布之日起生效。

.

附件 6-1-1 安全设备配置变更申请表（模板）

安全设备配置变更申请表

申请变更原因	
申请变更时间	
变更范围	
变更生效时间	
变更类别	□硬件配置变更　□策略配置变更
具体变更内容	

.

附件 6-1-2 安全设备配置变更记录表（模板）

安全设备配置变更记录表

序号	变更时间	变更内容	测试情况	是否备份	变更申请人	变更执行人
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						

.