浙江财经大学东方学院

网络安全管理制度汇编

信息技术部

二零二一年五月

目　录

一、安全管理手册

（一）发布说明

为落实国家与浙江省网络安全与等级保护的相关政策，贯彻网络安全管理体系标准，提高网络安全管理水平，按照业务信息和系统服务的安全保护等级、ISO/IEC 27001：2005《信息安全管理体系要求》、ISO/IEC 17799：2005《信息安全管理实用规则》，以及 GB/T 22239-2008《信息系统安全等级保护基本要求》，编制完成了网络安全管理体系文件，现予以批准颁布实施。

安全管理手册是纲领性文件，是指导网络安全管理体系的行动准则，全体人员必须遵照执行。

安全管理手册于发布之日起正式实施。

信息技术部

2021 年 05 月

（二）授权书

为了贯彻执行 ISO/IEC 27001：2005《信息安全管理体系要求》、ISO/IEC 17799：2005《信息安全管理实用规则》，以及 GB/T 22239-2008《信息系统安全等级保护基本要求》，加强对网络安全管理体系运作的管理和控制，特授权信息技术部负责网络安全工作，并保证网络安全管理职责的独立性，履行以下职责：

1、负责建立、修改、完善、持续改进和实施浙江财经大学东方学院网络安全管理体系。

2、负责向网络安全领导小组报告网络安全管理体系的实施情况，提出网络安全管理体系改进建议，作为管理评审和网络安全管理体系改进的基础。

3、负责向下属单位全体人员宣传网络安全的重要性，负责网络安全教育、培训，不断提高全体人员的网络安全意识。

4、负责网络安全管理对外联络工作。

（三）网络安全方针和要求

网络安全方针

浙江财经大学东方学院信息系统安全坚持“安全第一、预防为主，管理和技术并重，综合防范”的总体方针，实现信息系统安全可控、能控、在控。依照“分区、分级、分域”总体安全防护策略，执行网络安全等级保护制度。

网络安全总体要求

1、建立信息化资产（软件、硬件、数据库等）目录。

2、单位重要信息系统，按照等级保护相关要求进行建设和运维。

3、编制完成网络安全事件总体应急预案，并组织应急演练。

4、按需开展网络安全风险评估。

5、每年开展 1 次全系统范围内的信息系统安全检查（自查）。

6、每年组织 2 次全系统范围的网络安全管理制度宣传。

（四）主要安全策略

1、建立网络安全管理组织机构，明确网络管理员、系统管理员、安全管理员、机房管理员等安全管理相关岗位及职责，建立健全网络安全管理责任制，使得网络安全各项职责落实到人。

2、对网络安全管理体系进行定期内审和管理评审，对各项安全控制措施实施后的有效性进行测评，并实施相应的纠正和预防措施，以保证网络安全管理体系持续的充分性、适宜性、有效性。

3、对信息系统中所存在的安全风险进行有计划的评估和管理。定期对信息系统实施网络安全风险评估，根据评估结果选择适当的安全策略和控制措施，将安全风险控制在可接受的水平。在信息系统发生重大改变后，应进行风险评估。

4、所有信息系统分等级保护。按照国家等级保护有关要求，对信息系统及信息确定安全等级，并根据不同的安全等级实施分等级保护。

5、规范信息资产化（包括硬件、软件、服务等）管理流程，建立信息资产管理台帐，明确资产所有者、使用者与维护者，对所有信息资产进行标记，实现对信息资产购买、使用、变更、报废整个周期的安全管理。

6、加强所有人员（在编人员、外聘人员、维护人员）的安全管理，明确岗位安全职责，制定针对违规行为的惩戒措施，落实人员聘用、在岗和离岗时的安全控制，与敏感岗位人员签署保密协议。

7、通过正式的网络安全培训，以网站、简报、会议、讲座等形式开展网络安全教育活动，不断加强全体人员的网络安全意识，提高他们的网络安全技能。

8、保障机房物理与环境安全。部署机房空调、UPS 等环境保障设施，对机房设施运转情况进行定期巡检和维护。严格对机房人员和设备的出入管理，进出需登记，外来人员需由相关管理人员陪同方能访问机房。

9、加强对信息系统外包业务与外包方的管理，在与信息系统外包方签署的服务协议中，对信息系统安全加以要求。通过审批、访问控制、监控、签署保密协议等措施，加强外包方访问业务系统、信息系统维护的管理，防止外包方危害信息系统安全。

10、对重要信息系统（包括基础设施、网络和服务器设备、系统、应用等）应有文档化的操作和维护规程，使得各个相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发网络安全事件的可能性。

11、在外网上统一部署网络防恶意代码软件，并进行恶意代码库的统一更新，防范恶意代码、木马等对业务、系统的影响。通过强化恶意代码防范的管理措施，如加

强介质管理，严禁擅自安装软件，加强人员安全意识教育，定期进行恶意代码检测等，提高系统对恶意代码的防范能力。

12、对重要的信息和信息系统进行备份，并对备份介质进行安全地保存，对备份数据定期进行备份测试验证，保证各种备份信息的保密性、完整性和可用性，确保所有重要信息系统和重要数据在故障、灾难后及其它特定要求下进行可靠的恢复。

13、采用技术和管理两方面的控制措施，加强对门户网站等外网的安全控制，不断提高网络的安全性和稳定性。通过实施网络访问控制等技术防范措施，加强使用安全管理，对接入进行严格审批。加强对系统内各下属单位网络使用的安全培训和教育，确保网络的安全。

14、加强网络安全日常管理，包括系统口令管理、无人值守设备管理、屏幕保护、便携机管理等，促使每位人员的日常工作符合网络安全策略和制度要求。

15、按照“仅知”原则，通过功能和技术配置，对重要信息系统、数据等实施访问控制。对系统特殊权限和系统实用工具的使用进行严格的审批和监管。

16、进一步重视软件开发安全。在各类信息系统立项和审批过程中，同步考虑网络安全需求和目标。应保证系统设计、开发过程的安全，重点加强对软件代码安全性的管理。属于外包软件开发的，应与服务提供商签署保密协议。系统开发完成后，应通过第三方安全机构的软件安全性测评。

17、在符合国家密码管理相关规定的条件下，合理使用密码技术和密码设备，严格密钥生成、分发、保存等方面的安全管理，保障密码技术使用的安全性。

18、重视对 IT 服务连续性的管理，建立对各类网络安全事件的预防、预警、响应、处置、恢复机制，编写针对业务平台等重要系统的应急预案，并定期进行测试和演练，在信息系统发生故障或事故时，能迅速、有序地进行应急处置，最大限度地降低因信息系统突发事件或意外灾害给信息系统所带来的影响。

19、对所适用的国家网络安全相关法律法规进行定期的识别、记录和更新，并对系统下属各单位网络安全管理现状与法律法规的符合性进行检查，确保各项网络安全工作符合国家网络安全相关法律法规要求。

二、文件（制度）控制程序

（一）术语与定义

1、安全管理手册：是信息技术部建立网络安全管理体系的纲领性文件，是指导和实施网络安全管理体系的活动准则。

2、操作规程：是程序文件的支撑性文件，是某一类网络安全管理活动的具体要求。

3、记录文档：记录程序文件或操作规程的执行结果，以及项目运作过程中产生的结果性文档。

4、外来文件：来自信息技术部外部的文件。包括：外来图纸、文件、标书、技术规范、法律、法规及相关网络安全标准。

（二）职责

1、信息技术部职责：

负责单位安全管理手册和程序文件的批准发布。

2、各类系统管理员职责：

负责网络安全文件的归档管理。

3、安全管理员职责：

负责组织编制和修订安全管理手册和程序文件。

负责组织网络安全管理体系文件的评审。

（三）文件的编制

1、安全管理员根据 ISO/IEC 27001：2005《信息安全管理体系要求》，结合部门职责及网络安全管理流程，负责组织编制网络安全管理制度文件，形成初稿。

2、安全管理员负责组织对安全管理制度文件的评审，并将审核后的文件报信息技术部主任，由信息技术部主任对网络安全管理体系文件进行核准，形成最终的报审稿。

（四）文件的批准、发布

1、安全管理员负责对安全管理制度文件的报审稿进行登记、核稿后，报送领导审阅、签批。

2、组织相关人员进行评审，领导审阅、签批后发布。

（五）文件的发放

1、安全管理制度文件由安全管理员发放到相关职属范围人员。

2、岗位人员变动时，由文件主管部门及时收回原岗位各类文件，发放现岗位工作所依据的文件，以保证安全管理制度的有效运行。

3、岗位人员调离或退休时，应先向信息技术部交回其所领用的文件后，方可办理有关手续。

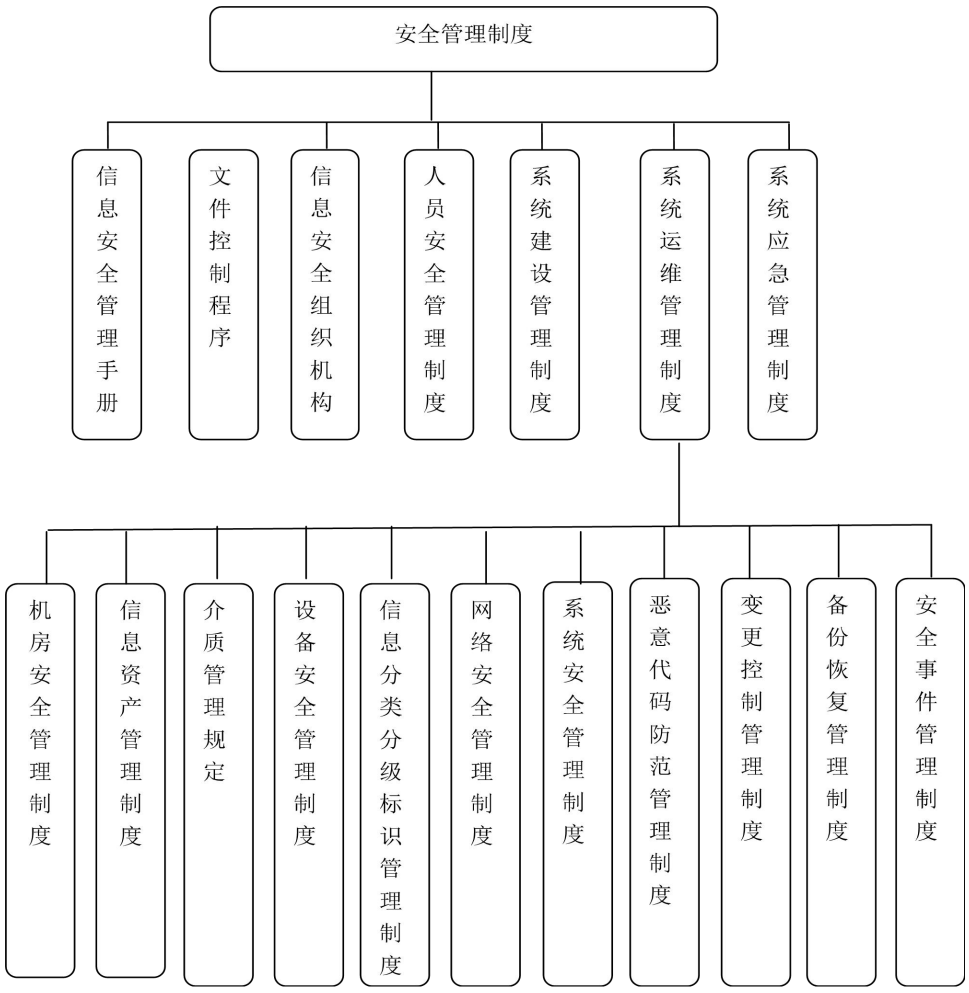
（六）文件的归档

安全管理手册和程序文件制发后，需保留 1 份，连同签批原件和电子版一并归安全管理员存档。

（七）文件评审管理

由信息技术部每年检查一次文件的适用情况，并对现有文件的有效性进行评审。对不合适的地方进行修订，必要时更换新版。

（八）安全管理制度的结构图



三、网络安全组织机构

（一）总则

➢ 为明确信息系统安全管理组织机构、角色、职责等，促进信息系统安全管理的组织建设，指导信息技术部网络安全管理工作，落实网络安全管理责任制，特制定本管理办法。

➢ 网络安全管理组织的建设、管理，均适用本管理办法。

（二）网络安全组织机构

包含信息技术部主任、系统维护人员、安全管理员以及外包服务公司。

安全管理员不可兼任其他岗位。

（三）工作职责及岗位说明书

信息技术部主任工作职责：

1、贯彻嘉兴市关于网络安全方面工作的方针政策，审定信息技术部信息系统安全建设规划。

2、对信息系统安全工作的重大事项做出决策。

3、研究审定信息技术部信息系统安全建设和管理工作中的制度、标准及相关政策，并协调相关部门监督制度、政策的实施情况。

4、组织、协调和指导网络安全的宣传、普及教育工作。

信息技术部部门工作职责：

1、负责贯彻落实网络安全领导小组关于信息系统安全工作的要求和规定。

2、根据信息化建设的总体目标，负责信息系统的安全管理体系，包括：制度建设、技术保障和操作规范等各方面的逐步建成。

3、组织制订和贯彻信息系统运行安全保障和维护工作制度。

4、负责落实网络安全领导小组部署的各项工作。

各岗位工作职责：

安全管理员：

1、负责安全制度的贯彻执行。

2、负责制订信息系统安全规划，并在实施过程中逐步完善。

3、负责制定安全设备或系统的相关资产清单。内容包括资产管理的责任部门、信息分类和资产标识的方法和资产名称、重要程度、所处位置等。

4、负责规范安全设备或系统管理流程，建立管理台帐，明确资产所有者、使用者与维护者，对安全设备或系统进行标记，实现对机房资产购买、使用、变更、报废整个周期的安全管理。

5、负责制定安全设备或系统的文档化的操作和维护规程，使得相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发网络安全事件的可能性。

6、负责对安全设备或系统运行维护管理，对安全设备或系统运转情况进行定期巡检、维护、故障处理和变更管理。负责组织实施安全设备或系统各类事故（故障）的应急处理。

7、负责协助领导安排安全培训，协助制定每年安全教育计划，加强信息系统的安全教育，通过各种方式进行宣传和培训，提高全系统安全防范意识。

8、负责制定安全检查计划，至少每季度组织一次检查。检查包括安全职责、检查周期、检查范围、检查内容、检查报告的编制、整改措施、检查通报等。对信息系统安全检查情况进行通报。对检查记录进行收集、整理、归档。

9、当出现安全事件时，负责对发生的安全事件及时上报，并配合相关的调查和纠正工作。

10、当信息系统运行发生重大问题时，协助相关人员正确判断原因，根据指令立即采取安全措施启动相关处理程序。

11、负责与外部安全机构的协调联系，在发生重大安全事件时以协调获取外部安全机构的支持。

12、负责对介质的管理。对介质的归档、查询和借用进行记录，对介质进行定期盘点并记录，对故障介质的进行送修和销毁并记录，对于保密性高的介质销毁需要申报领导批准，并进行记录。对介质物理传输的交接进行记录。

13、负责对各种记录文档、表单，半年一次进行汇总，并对制度开展情况向网络安全领导小组汇报。

14、加强对信息系统外包业务与外包方的管理，在与信息系统外包方签署的服务协议中，对信息系统安全加以要求。通过审批、访问控制、监控、签署保密协议等措施，加强外部方访问信息系统的管理，防止外部方危害信息系统安全。

15、重视对 IT 服务连续性的管理，建立对各类网络安全事件的预防、预警、响应、处置、恢复机制，编写针对重要系统的应急预案，并定期进行测试和演练，在信息系统

发生故障或事故时，能迅速、有序地进行应急处置，最大限度地降低因信息系统突发事件或意外灾害给信息系统所带来的影响。

16、在符合国家密码管理相关规定的条件下，合理使用密码技术和密码设备，严格密钥生成、分发、保存等方面的安全管理，保障密码技术使用的安全性。

机房管理员

1、负责保障机房物理与环境的安全建设管理，对实施方责任、时间进度、任务要求、质量控制等进行监督管理。

2、负责制定机房基础设施的相关资产清单。内容包括资产管理的责任人、信息分类和资产标识的方法和资产名称、重要程度、所处位置等。

3、规范机房资产（包括机房物理与环境等）管理流程，建立机房资产管理台帐，明确资产所有者、使用者与维护者，对所有机房资产进行标记，实现对机房资产购买、使用、变更、报废整个周期的安全管理。

4、负责制定重要基础设施等的文档化的操作和维护规程，使得相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发网络安全事件的可能性。

5、负责保障机房物理与环境安全。实施包括温度监控、报警等安全防范措施，确保机房物理安全。部署机房空调、UPS 等环境保障设施，对机房设施运转情况进行定期巡检、维护、故障处理和变更管理。严格对机房人员和设备的出入管理， 进出需登记，外来人员需由相关管理人员陪同方能访问机房。

6、负责对机房基础设施变更、重要操作、物理访问等审批，重大变更上报到网络安全领导小组。

7、负责组织实施机房基础设施各类事故（故障）的应急处理。

系统运维岗人员

网络管理员

1、负责保障网络安全建设管理，对实施方责任、时间进度、任务要求、质量控制等进行监督管理。

2、规范网络管理流程，建立网络相关资产管理台帐，明确资产所有者、使用者与维护者，对所有信息资产进行标记，实现对信息资产购买、使用、变更、报废整个周期的安全管理。

3、采用技术和管理两方面的控制措施，加强对单位外网的安全控制，不断提高网络的安全性和稳定性。通过实施网络访问控制等技术防范措施，对接入进行严格审批并登记，加强使用安全管理，加强对各部门网络使用的安全培训和教育，确保单位外网的安全。

4、对重要网络设备应有文档化的操作和维护规程，使得各个相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发网络安全事件的可能性。

5、负责保障网络安全。协助安全管理员部署网络安全产品，确保网络安全。对网络设备运转情况进行定期巡检、维护、故障处理和变更管理。

6、负责对网络系统变更、重要操作、访问等审批，重大变更上报到网络安全领导小组。

7、负责组织实施网络各类事故（故障）的应急处理。

系统管理员

1、负责保障主机（包括服务器设备、操作系统、数据库系统、数据备份）安全建设管理，对实施方责任、时间进度、任务要求、质量控制等进行监督管理。

2、负责主机运行维护体系和主机技术支持平台的建设与运行管理。负责建立服务器设备、操作系统、数据库系统、数据备份文档化的操作和维护规程，使得各个相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发网络安全事件的可能性。

3、负责灾难备份系统及相关设施的完善及日常管理工作。制订并完善灾难备份系统运行的评估标准，形成标准化管理模式。监控灾难备份系统运行状况，定期或不定期组织防灾备灾演练，对灾难备份系统的运行状况进行审计和评估，并提出改进意见。

4、对重要的信息和信息系统进行备份，并对备份介质进行安全保存，保证各种备份信息的保密性、完整性和可用性，确保所有重要信息系统和重要数据在故障、灾难后及其它特定要求下进行可靠的恢复。

5、在网络上统一部署网络防恶意代码软件，并进行恶意代码库的统一更新，防范恶意代码、木马等病毒程序对信息系统的影响。通过强化恶意代码防范的管理措施，如加强主机管理，严禁擅自安装软件，定期进行恶意代码检测等，提高信息系统对恶意代码的防范能力。负责全系统的计算机恶意代码防治和主机安全的管理工作，制定检查计划（包含在主机巡检工作中），督促检查工作。

6、加强网络安全日常管理，包括系统口令管理、无人值守设备管理、屏幕保护、便携机管理等，促使每位人员的日常工作符合系统网络安全策略和制度要求。

7、按照“仅知”原则，通过功能和技术配置，对重要信息系统、数据等实施访问控制。对系统特殊权限和系统实用工具的使用进行严格的审批和监管。

8、规范主机（包括服务器设备、操作系统、数据库系统、数据备份）资产管理流程，建立主机相关资产管理台帐，明确资产所有者、使用者与维护者，对所有信息资产进行标记，实现对主机相关资产购买、使用、变更、报废整个周期的安全管理。

9、负责对主机系统变更、重要操作、访问等审批，重大变更上报到网络安全领导小组。

10、负责组织实施系统各类事故（故障）的应急处理。

应用管理员

1、负责保障软件开发管理，对实施方责任、时间进度、任务要求、质量控制等进行监督管理。进一步重视软件开发安全。在信息系统立项和审批过程中，同步考虑网络安全需求和目标。应保证系统设计、开发过程的安全，重点加强对软件代码安全性的管理。属于外包软件开发的，应与服务提供商签署保密协议。系统开发完成后，应对软件安全性进行测评。

2、规范信息资产管理流程，建立信息资产管理台帐，明确资产所有者、使用者与维护者，对所有信息资产进行标记，实现对信息资产购买、使用、变更、报废整个周期的安全管理。

3、负责建立重要应用的文档化操作和维护规程，使得各个相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发网络安全事件的可能性。

4、规范应用系统资产管理流程，建立应用系统资产管理台帐，明确资产所有者、使用者与维护者，对所有信息资产进行标记，实现对主机相关资产购买、使用、变更、报废整个周期的安全管理。

5、加强网络安全日常管理，包括应用系统口令管理、授权审批管理等，促使每位人员的日常工作符合网络安全策略和制度要求。

6、负责对应用系统变更、重要操作、访问等审批，重大变更上报到网络安全领导小组。

7、负责组织实施应用系统各类事故（故障）的应急处理。

审计管理员

负责对涉及系统安全的事件和各类操作人员的行为进行审计和监督，主要职能包括：

1、按操作时间审计；

2、按操作类型审计；

3、事件类型进行审计；

4、日志管理等。

（四）关键活动的授权和审批

1、在系统运维过程中，网络安全领导小组把对信息系统的访问、变更等授权给信息技术部。机房管理员负责机房相关事务的授权和审批；系统维护人员负责网络、主机、应用等相关事务的授权和审批。

2、授权审批流程：

a) 由信息技术部判断职责、然后授权给相应的管理员；

b) 由外包服务公司申请，相应的管理员进行授权、审批；

c) 填写授权审批表，经审批通过后进行授权，审批表专人保管。

（五）审核和检查

组织专门人员（或上级单位）定期进行安全检查（如：每季度自查），包括网络、安全设备、系统等各方面的安全检查。记录检查结果。规范安全检查的内容并统一分析检查结果。组织会议讨论明确安全检查的具体内容，编写《安全检查要求》和《安全检查表》。检查内容包括：

1、计算机系统管理：各类主机系统、数据库系统的用户及密码管理、权限管理、备份管理、系统监控及系统日志管理等。

2、计算机网络管理：网络访问控制策略、IP 地址管理、备份管理、因特网管理、网络监控、网络系统日志管理情况等。

3、网络安全产品管理：防火墙、防病毒和入侵检测等网络安全产品的使用管理情况等。

4、科技文档管理：信息系统开发、设计及运行文档，各类科技档案的管理情况等。

5、计算机机房安全管理：计算机机房布线、门禁、消防、供电系统、UPS、空调、

机房监控、机房值班等管理情况。

6、计算机资产管理：信息资产管理及计算机硬件设备管理情况等。

7、业务连续性管理：重要信息系统应急处理方案的制定情况，应急方案定期的培训或演练情况等。

（六）沟通合作

1、加强各类管理人员、内部机构、网络安全职能部门内部之间的合作与沟通，定期或不定期召开协调会议，共同协作处理网络安全问题；

2、加强与兄弟单位、公安机关、电信公司、网通公司的合作与沟通；

3、建立外联单位联系表，包括外联单位名称、合作内容、联系人和联系方式等信息；

4、对协调会议、安全评审等进行记录。

四、人员网络安全管理制度

1、信息技术部应根据各岗位网络安全特性和业务特点，确定各岗位网络安全角色和职责。网络安全角色及职责应包括以下内容：

- 在网络安全管理组织架构中的角色和职责；
- 在执行网络安全方针和目标方面的职责；
- 在遵守国家、地方各种网络安全相关法律法规方面的职责；
- 在保护信息资产免受未授权访问、泄露、修改、销毁或干扰方面的职责；
- 执行特定的安全过程或活动方面的职责；
- 在报告网络安全事故和弱点方面的职责。

2、人员录用和上岗时的网络安全要求

- 指定或授权专门的部门或人员负责人员录用；
- 严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；
- 岗位人员在任用之前应签署保密协议；
- 应通过教育和培训活动，确保本单位员工、外来人员在上岗前，理解其岗位网络安全角色和职责；
- 应确保在针对本单位员工的岗前培训中，包括网络安全管理体系和相关管理制度、岗位网络安全职责等网络安全相关的内容；
- 信息技术部应根据已确定的岗位安全角色和职责，在岗位职责或协议中通过网络安全相关条款加以明确。网络安全相关条款可以包括以下方面：
- 岗位相关的法律职责和权利；
- 信息系统相关资产的管理职责；
- 操作其他组织和机构信息的职责；
- 保护个人信息方面的安全职责，包括对个人隐私保密，不滥用个人信息等；
- 在办公区域外和正常工作时间之外的职责；
- 网络安全违规将受到的惩戒措施。

3、信息技术部应根据岗位安全职责，对重要岗位制定相应的保密协议。保密协议可包括以下方面的内容：

- 岗位所要保护的信息；

- 协议有效期；
- 协议终止时所应采取的措施；
- 为避免泄密，签字人的职责和行为；
- 保密协议与知识产权保护、商业秘密保护的关系；
- 涉密信息的许可使用，及签字人使用信息的权力；
- 对涉密信息的活动的审核和监视；
- 涉密信息泄露或被破坏后的处理程序；
- 协议终止时信息的归档或销毁的措施；
- 违反协议后应采取的措施。

4、人员在岗时的网络安全管理

岗位网络安全检查

- 各部门应提高安全意识，定期对本部门岗位进行网络安全检查，确保网络安全规定得到了有效地执行；
- 信息技术部应不定期抽查各部门网络安全职责的落实情况，确保网络安全职责的落实。

网络安全违规的纪律处理

- 对于网络安全事故和在网络安全检查中发现的违规行为，由信息技术部根据有关考核规定上报网络安全领导小组对该人员进行处罚；
- 对于情节特别严重的违规行为，还应借助网络、简报等媒介在系统内部进行普遍宣传，避免同类问题再次发生。

5、人员考核

- 定期对各个岗位的人员进行安全技能及安全认知的考核；
- 对考核结果进行记录并保存。

6、安全意识教育和培训

- 对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；
- 对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；
- 对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对网络安全基础知识、岗位操作规程等进行培训；

- 对安全教育和培训的情况和结果进行记录并归档保存。

7、人员离职和转岗的安全管理

信息技术部应明确人员离职和转岗时的手续，明确离职和转岗管理职责。职责一般包括：

- 在归还资产方面各相关部门的职责；
- 在撤销访问权方面各相关部门的职责；
- 在岗位人员变动方面各相关部门的职责；
- 离开岗位后还应承担的责任，如保密限制等。

资产的归还

- 离岗人员在离岗时归还其使用的信息设备资产，包括所有先前发放的软件、访问卡、文件和设备等。相关部门应与离岗人员进行离岗交接，并做好记录；
- 离岗人员应就其涉及到的专利、技术文档等及时向所在部门上交；
- 人员在离岗时，应对正在实施的项目中的相关信息形成文档并提交给相关部门，进行项目交接；
- 如离岗人员离开本单位，请部门将离岗人员的相关资产交信息技术部并修改存档信息。

撤销访问权

- 在人员任用终止时，应按照离岗手续，人教处通知相关部门对该人员使用信息和信息系统的权限进行调整；
- 依照相关人员的个人权限清单和网络安全管理要求，修改、限制或删除相关信息和信息系统的访问权限，包括物理访问、逻辑访问、密钥及 ID 卡等，并作相应记录；
- 相关部门应立即撤销或停用离岗人员所使用的账户，或者修改离岗人员所掌握的系统帐户口令。

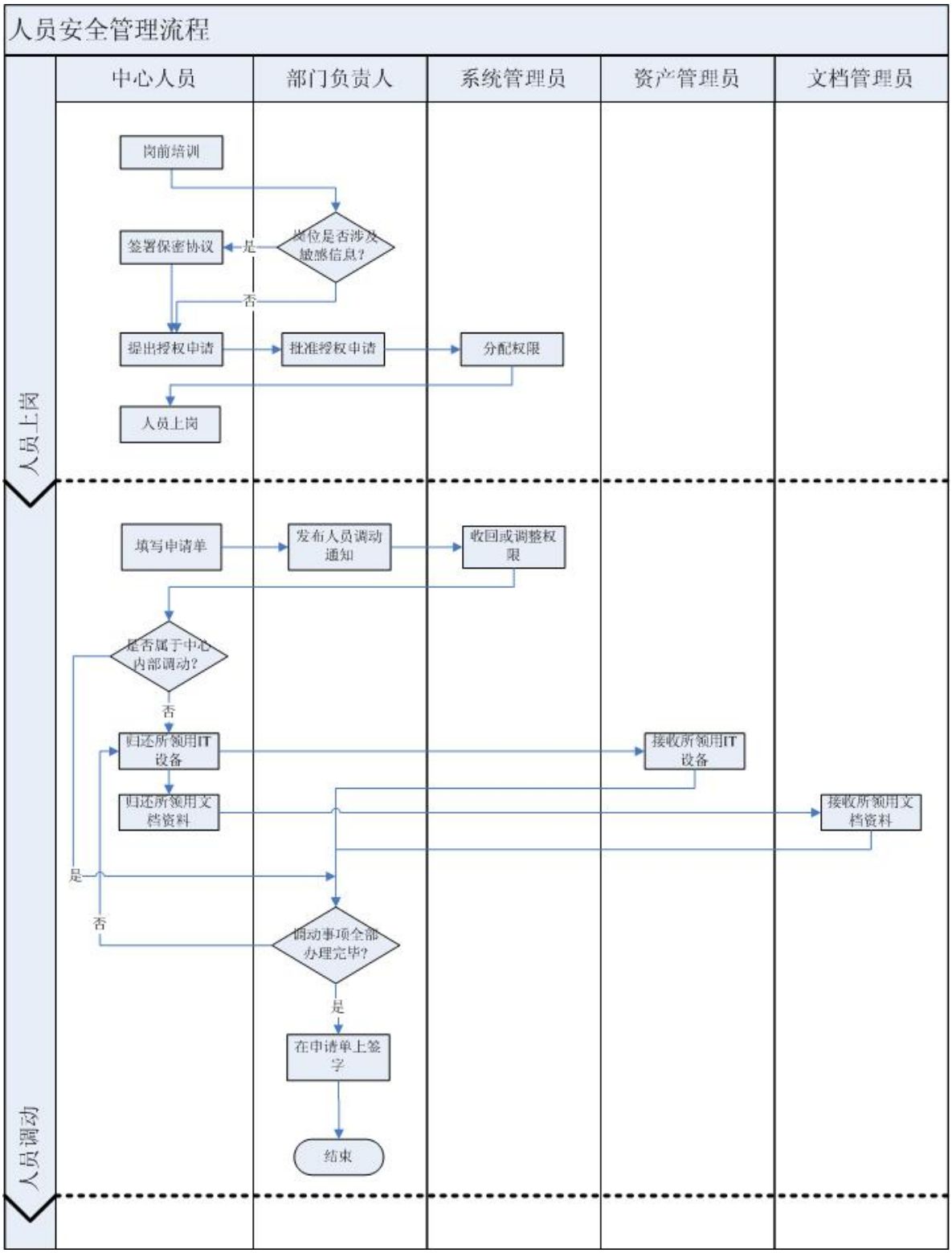
离职后网络安全职责的追踪和管理

- 离职人员应明确其离职后仍需担负的安全责任和义务，以及违反安全责任和义务所引发的后果；
- 如发生有离职人员违反其应负的安全责任，泄露敏感秘密，按照网络安全保密有关规定和相关协议追究其法律责任。

8、外来人员的网络安全管理

- 外来人员来信息技术部访问、参观时，应对其进行网络安全意识教育，确保其理解和遵守访问、参观时应注意的网络安全规定。
- 各部门在与外部方签订合同时，应按照岗位角色和职责要求，在合同中对外来人员进行约束。
- 各部门应要求外部方根据合同要求，对其人员进行安全职责的宣传和教育，确保外来人员理解其应担负的安全责任和义务。
- 各部门应按照有关网络安全管理规定以及合同要求，对所有外来人员进行监督和检查，并就安全违规情况按合同条款中的要求进行处理。
- 确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案。
- 禁止非本中心机房技术人员携带工作物品如笔记本电脑、移动硬盘、U 盘等移动存储设备进入中心机房。必须携带的，应办理有关手续，由管理部门负责人批准，履行登记手续。

人员安全管理流程


人员安全管理流程
中心人员
部门负责人
系统管理员
资产管理员
文档管理员
人员上岗
岗前培训
岗位是否涉及敏感信息?
是
签署保密协议
否
提出授权申请
批准授权申请
分配权限
人员上岗
人员调动
填写申请单
发布人员调动通知
收回或调整权限
是否属于中心内部调动?
否
归还所领用IT设备
接收所领用IT设备
归还所领用文档资料
接收所领用文档资料
是
否
调动事项全部办理完毕?
是
在申请单上签字
结束

五、系统建设安全管理制度

（一）规划设计

1、总体安全规划阶段的工作流程

- 安全需求分析
- 总体安全设计
- 安全建设项目规划

2、安全需求分析

- 基本安全需求的确定
- 额外/特殊安全需求的确定
- 形成安全需求分析报告

3、 总体安全设计

- 总体安全策略设计
- 安全技术体系结构设计
- 整体安全管理体系结构设计
- 设计结果文档化

4、安全建设项目规划

- 安全建设目标确定
- 安全建设内容规划
- 形成安全建设项目计划

（二）设备选型

信息系统采取有关网络安全技术措施和采购装备相应的设备时，应遵循下列原则：

1、应确保产品采购和使用符合国家网络安全的有关规定；（采购产品时需对供应商的资质进行审核，必须具有公安部颁发的网络安全产品销售许可证；采用密码技术的安全专用产品必须提交国家密码管理部门的审批文件。）

2、应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

3、尽量采用我国自主开发研制的网络安全技术和设备。

4、采用境外网络安全产品时，产品必须通过国家网络安全测评机构的认可。

5、严禁使用未经国家密码管理部门批准和未通过国家网络安全质量认证的密码设备。

（三）采购和安装

软件的采购和安装

1、信息系统所使用的操作系统、应用软件、数据库、安全软件、工具软件必须是正式版本，严禁使用测试版和盗版软件。

2、重要的操作系统和主要应用软件必须在安全管理员的监督之下进行安装。

3、应指定或授权专门的部门负责产品的采购。

设备的采购和安装

1、设备符合系统选型要求并获得批准后，方可购置。

2、凡购回的设备均应在测试环境下经过连续 72 小时以上的单机运行测试和联机 48 小时的应用系统兼容性运行测试。

3、通过上述测试后，设备才能进入试运行阶段。试运行时间的长短可根据需要自行确定。

4、通过试运行的设备，才能投入系统，正式运行。

（四）软件开发管理

软件自行开发管理

1、系统应用软件的开发必须根据信息密级和安全等级，同步进行相应的安全设计，并制定各阶段安全目标，按目标进行管理和实施。

2、系统应用软件的开发，必须有安全管理专业的技术人员参加，其主要任务是：对系统方案与开发进行安全审查和监督，负责系统安全设计和实施。

3、开发环境和现场必须与办公环境和工作现场分开，软件设计方案、数据结构、安全管理、操作监控手段、数据加密形式、源代码等，只能在有关开发人员及有关管理机构中流动，严禁散失或外泄。

4、应用软件开发必须符合软件工程规范[GB8566-88]、[GB1526-89]。

5、确保提供软件设计的相关文档和使用指南，并由专人负责保管；项目开发阶段需要提交给项目管理员的文档有：设计说明书、用户使用手册、系统维护手册。

6、明确说明开发过程的控制方法和人员行为准则。（例如：项目开发分为需求分

析、系统设计、详细设计、编码、测试、上线等阶段。项目负责人在各个阶段均应填写《软件开发维护过程控制表》，对开发设计工作进行管理。开发人员根据系统设计文档，合理划分功能模块，做到程序结构清晰、层次分明、命名规范、程序头部及函数定义都需有明确注释，对于逻辑复杂的地方应有详细的备注说明。对原程序的更改应该在修改的地方加注修改人、修改时间、修改原因、原程序逻辑、现程序逻辑。使程序可读性强，容易维护。）

外包软件开发管理

1、应要求开发单位提供软件设计的相关文档和使用指南；如：购买商品化软件时，供应商应提供《功能说明书》、《系统安装手册》、《系统维护手册》等技术文档。

2、在托开发过程中，应加强开发过程中的安全管理和监控，重点考虑资质、许可证、代码所有权和知识产权；审核工作质量和访问权限，代码质量和安全功能达到合同要求。特殊情况应测试恶意代码和特洛伊木马。

3、应要求软件开发商在所开发的信息系统内设计实现了安全控制措施，确保信息在系统中得到了正确处理。

4、在开发过程中，应采取控制措施，减少信息泄露的可能性，重点考虑：规范开发过程中的通信行为，以减少第三方从这些行为中推断信息的可能性；在现有法律或法规允许的情况下，定期监视个人和系统的活动；监视计算机系统的资源使用；防止非授权的网络访问；对程序源代码的防护管理。

5、信息技术部应要求软件开发商对程序源代码进行管理与控制。程序源代码应集中保存在代码库中，对代码库实施安全保护。保护措施主要包括：建立程序源代码和源程序库管理规范；对访问源程序库人员进行授权管制；程序列表应保存在安全的环境中；建立对源程序库所有访问的审核日志；维护和拷贝源程序库应受严格的限制。

6、应根据开发需求检测软件质量。（如：软件投入运行前，测试人员应针对软件的功能满足程度及程序运行的准确性、运行效率、容错性等编制测试样本，进行功能测试，对测试中发现的问题进行详细的记录，递交软件开发人员进行改进。）

7、应在软件安装之前检测软件包中可能存在的恶意代码，对软件包中的恶意代码进行查杀，并对恶意代码检测结果进行记录。

8、应要求开发单位提供软件源代码，并审查软件中可能存在的后门。（如：软件投入运行前，测试人员应进行计算机项目漏洞扫描检测，并出具软件安全性检测报告。）

（五）工程实施

1、指定或授权专门的部门或人员负责工程实施过程的管理，必要时可引入外部信息工程监理机构进行工程实施的监理。

2、由实施方制定详细的工程实施方案控制实施过程，由信息技术部认可并要求工程实施单位能按计划执行工程实施。

（六）测试验收

1、应对系统进行安全性测试，并出具安全性测试报告，要求建设单位根据测试结果及时进行整改。

2、在测试前应根据设计方案或合同要求等制订测试方案，在测试过程中应详细记录测试结果，并形成测试报告，测试通过后方可进行验收。

3、指定或授权专门的部门或人员负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作。

4、组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

（七）系统交付

1、应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。

2、制定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和确认。

3、对负责系统运行维护的技术人员进行相应的技能培训，以及对系统最终用户的操作进行相应的培训。

（八）系统建设服务商选择

1、确保系统建设服务商的选择符合国家网络安全的有关规定，必要时应选择有安全集成相关资质的服务商。

2、与选定的系统建设服务商签订与安全相关的保密协议，明确约定相关责任。

3、确保选定的系统建设服务商提供技术培训和服务承诺，必要时与其签订服务合同。

六、机房安全管理制度

（一）汇集机房管理规定

1、配置要求

机房的基本设施配置应不低于附表一中标准，根据实际需求可适当提高配置标准。

2、监控

机房管理人员要利用机房远程监控系统实时监控各汇聚点机房环境和设备信息，主要包括机房环境参数、设备运行参数、设备状态指示灯、视频监控图像等，值班人员每天做一次监控情况记录。

3、维护和巡检

相关系统维保单位在日常维护和例行巡检过程中需要检查、维护机房的环境情况和系统的运行情况，包括清除机房内垃圾积灰、报废物品；对相关设备、线缆进行卫生保洁和整理；对系统的运行状况进行分析；对配置信息收集和更新；更换易耗件；更新标贴和机柜布置图等。维护和巡检完成后由网络管理员审核并确认结果。此项工作完成情况需作为考核维保单位工作质量的标准之一。

4、应急处置

机房管理人员若在监控过程中发现异常情况，需在计算机报修系统中进行登记并通知网络管理员，由网络管理员实施派工并督促相关系统维保单位或网络管理员自己及时处置，维保单位或网络管理员在排除异常后要在计算机报修系统中记录维修情况，由网络管理员审核登记完成情况，重大事故（断电、超温、重要设备损毁等）要上报网络安全小组领导。

5、档案管理

每次日常维护和例行巡检后由网络管理员负责更新有关技术档案。维保单位在维保月报中要提交机房维护和巡检的相关内容。

6、安全管理

- 人员出入机房必须预先报机房管理员，得到批准方可进入施工，出入情况和工作内容由机房管理员记录在案。
- 严禁无关人员和手续不全者接触该部分设备。
- 设备维护必须由相关系统维保单位专业人员实施并保留操作记录。
- 设备登录和配置密码，由网络管理员保管，不得向无关人员泄露。

（二）接入机房建设管理办法

1、制定目的

为加强对网络各接入点机房的维护管理，提高维护管理质量，确保信息系统网络的正常运行，特制定本规定。

2、适用范围

本办法仅适用于本单位系统相关机房。

3、 建设要求

各相关部门（单位）在建设网络接入机房时应满足以下要求：

一、建筑装饰要求

（一）机房地面负荷每平方米应不小于350kg。

（二）机房净高应在2.6米以上。

（三）机房面积应不小于16平方米，满足D类中心机房建设规范。（D类中心机房主机房区总面积一般在30m^{2}以下。）

（四）机房主要门的大小应满足设备的搬运需要。（中心机房门的材料必须坚固，防止入侵者用强力打开；中心机房的门锁必须具有一定的防盗等级；中心机房门的铰链必须有保护，避免入侵者使用工具进行拆卸。）

（五）机房顶棚、墙、门、窗、地面应不脱落，不渗水，不易起尘，不易积灰，并能防尘砂侵入。要求屋顶，不掉灰，装饰材料应用非燃烧材料或难燃材料。

（六）机房内不允许水、气管道通过。

二、电气要求

（一）条件许可的情况下，机房应配备2路以上的强电引入。

（二）交流配电系统安全接地、设备工作接地和配线架防雷接地可采用联合接地，接地电阻不大于1Ω。

（三）机房水泥地面应铺设防静电地板，防静电地板应经限流电阻及连接线与接地装置相连，限流电阻的阻值为1MΩ。

（四）机房须配备UPS设备，备用时间大于30分钟。

4、环境要求

（一）机房照明需满足目视及摄像机观测照度，离地0.8m处照度应不低于200lx。

（二）机房内需安装独立商用空调，保持室内温度在18℃～28℃的范围内。中心

机房内应安装温湿度探测器等设备，设置温、湿度自动调节设施，使温、湿度在以下允许的范围内变化（C、D 类中心机房的主机房区温度为18-28℃，相对湿度为35%—75%，温度变化率为<10℃/h，不结露）。

5、安全要求

满足消防设计要求，机房内需配备烟感、温感报警器等设备，并配备干式灭火器或气体灭火装置。（中心机房应同时设置两种火灾灭火探测器，如温感和烟感探测器，安装火灾自动报警系统。中心机房应安装防盗报警系统。）

6、其他设施要求

（一）机房内配备 19”标准机柜，以满足服务器、网络、UPS、安防等设备的安装，机柜侧面应标贴与实际情况相符的机柜布置图。

（二）机房内需布置弱电桥架，连接垂直桥架和户外信息管线。

（三）设备和线缆标贴按照统一的命名规范清晰标注、易识别。

7、管理要求

一、明确管理职责

信息技术部是网络接入机房的业务主管部门，负责机房建设及日常管理工作。

二、落实管理人员

网络接入机房的管理责任人为该单位网管员。

三、做好日常管理

（一）网络接入机房的管理人员要对机房进出情况进行登记，禁止无关人员入内。

（二）机房每日至少巡检一次，控制合适的温、湿度，保证稳定的电力供应，保持环境整洁，清除废弃物品及易燃易爆物。

（三）做好机房各类设施、设备的维护工作，工作内容要有记录。

四、制定应急预案

需制定网络接入机房应急预案，当机房发生重大突发状况时（例如断电、超温、重要设备损毁等），机房管理人员要按照应急预案及时安排处置并报网络安全领导小组。

（三）机房维护管理办法

1、制定目的

为加强对网络机房的维护管理，提高维护管理质量，确保网络的正常运行，特制定本规定。

2、适用范围

本办法适用于机房。

3、机房出入管理

1) 若非必要，不要随便进入机房；最后离开机房的人员要关灯、锁门。外部人员进出需专人陪同，需填写《外部人员出入登记表》。

2) 保管好机房钥匙，不能随意转借。丢失要及时声明。

3) 自觉保持机房卫生。

4) 严禁携带易燃易爆物品、强磁物品、食品及其它与工作无关的物品进入机房。

4、机房环境管理

1) 值班人员要打扫机房卫生，保持地面干净，机柜无尘土，各种设备摆放整齐。

2) 机房内禁止吸烟，注意防火。

3) 工作人员进入机房要检查设备情况（包括空调温、湿度、电力系统、网络设备、服务器），离开时察看灯、门、窗、锁是否关闭好。

4) 电力设施注意相关机房内设备不要插入墙壁插座。

5、机房介质管理

1) 对应用系统使用、产生的介质或资料要按其重要性进行分类，对存放有关键或重要数据的介质（资料），分别存放在不同的安全地方并建立严格的保密保管制度。

2) 保留在机房内的介质（资料），应为系统有效运行所必需的最少数量，除此之外，不应保留在机房内。

3) 存放机房内的介质（资料）应该存放于防火、防高温、防震、防电磁场、防静电及防盗的房间或保险柜中。

4) 介质（资料）库，应设专人（资产管理员）负责登记保管，未经批准，不得随意提供介质（资料）。

5) 对所有介质（资料）应定期检查，要考虑介质的安全保存期限，及时更新复制。

6、机房服务器管理

1) 应统一将服务器编号、操作系统、应用系统、负责人、IP 地址、出厂序号、切换器编号等信息以标签方式张贴在服务器前面板明显位置，未经许可，任何人不得撕毁、篡改。服务器按应用级别和管理责任不同分为重要、普通、测试、托管四类，用不同颜色标签区分。测试服务器原则上不与其他服务器安排在同一机柜内。标签每半年复核一次。

2) 服务器等设备是机房的重要设备，必须按要求放置在机房指定机柜内，不得擅自配置、移动、更换，更不能挪作它用。服务器物理位置一经确定，不得随意变更。如需变更，由项目主管填写《服务器变更申请表》，经主机系统负责人（管理员）确认后方可变更。

3) 根据系统建设需要将服务器连入或断开网络，变更服务器用途，应用系统重大升级，变更密码，改变目录等，由项目主管填写《服务器变更申请表》，经主机系统负责人（管理员）确认后方可变更。同时，网络管理人员根据实际情况，在两个工作日内调整网管软件监控信息，存储备份相关配置。

4) 对服务器必须建立维护档案，项目主管是服务器维护档案的第一责任人，维护档案由项目主管负责，项目开发人员，安全服务人员，机房管理人员，值班人员对服务器的任何更改操作均要报项目主管进行记录。

5) 服务器及相关配套软件的申请采购、验收由各项目主管负责。服务器完成验收后，才能分配机柜位置及联入网络。各项目主管填写《服务器接入申请表》，报主机系统负责人（管理员）进行确认。

6) 如果服务器运行多个应用系统，按应用系统的重要程度确定第一责任人。重要应用系统的项目主管是第一责任人。

7、机房布线管理

1) 机房布线应按照规范铺设在防静电地板下,设备调试时使用的临时布线应在调试完成当天撤换。(主机房区弱电布线设计可根据大楼实际情况选择地板下走线方式或顶棚上走线方式,如采用地板下走线方式,弱电线路布线与电缆布线保持一定距离,各类线缆宜采用封闭式桥架，同时应注意桥架与空调风道方向一致。)

2) 机房所有网络线路维护、连接、拆除由专人施工，禁止其他人员未经许可随意

连接、拆除网线。

3) 电源线和通信线缆应隔离铺设，避免互相干扰。

8、机房网络设备管理

1) 对网络设备建立维护档案，由基础组负责维护，项目主管是网络维护档案的第一责任人，对网络设备的任何更改均要有记录。

2) 应统一将网络设备编号、负责人等信息以标签方式张贴在网络设备前面板明显位置，未经许可，任何人不得撕毁、篡改。

3) 设备发生故障或故障隐患时非管理人员不可对路由器、交换机、服务器、光纤、网线及各种设备进行任何调试，对所发生的故障、处理过程和结果等做好详细登记。严格按照相关规定处理故障，及时与管理人员沟通，并对有关故障做出书面报告。

4) 网络设备及相关配套软硬件的申请采购、验收由基础组负责。设备完成验收后，分配机柜位置及联入网络。填写《网络设备接入申请表》，报网络负责人（管理员）进行确认。

9、机房巡视管理

1) 没有特殊情况，值日人员应按照要求每天巡视机房二次，检查机房各种设备的运行情况，并做好巡视记录。

2) 遇到各种设备故障，值日人员应按照《机房管理办法》上描述的操作步骤对设备进行处理，遇到问题及时与管理人员沟通，并对有关故障做出书面报告。

3) 所有相关的巡视报告、故障报告等需要相关负责人员进行确认，并存档管理。

10、机房进出设备管理

1) 新购设备或临时迁入机房的设备需经机房管理员确认，按《设备迁入机房登记表》的相关项目详细填写登记。

2) 机房设备需要迁出机房时需通知当日值日人员，填写《设备迁出机房登记表》，并报登记备案。

11、违规处理

如果发现违规行为，要进行书面检讨。违规事件应报相关负责人进行记录并通报。

（四）机房值班管理办法

1、机房巡查

1) 每日早晚现场巡查主机房、UPS 机房以及各类设备各一次。

2) 检查防火、防盗、防水、防雷击、供电及门窗关闭等情况，机房环境温度应控制在 18℃ ～ 24℃，湿度控制在 40% ～ 60%。

3) 下班前应进行安全检查，关掉计算机终端、照明及其它非 24 小时常开设备的电源，在关闭机房和值班室后才能离开。

2、机房监控

开启监控机房环境和设备运行状态参数（UPS 供电，空调温、湿度、网络等），发现异常情况通知相关人员处置，并及时报告中心领导。

3、报修管理

1) 报修登记。接到报修后，应检查报修设备的备案信息，准确登记报修内容。对于不属于报修范围的事项，应耐心解释。

2) 派工维修。做好维修人员调度，及时安排维护人员前往现场维修。如遇特殊情况应视情况优先安排，暂时无法派工的应及时与报修人联系。

3) 完工检查。及时查看维修记录，督促维护人员及时反馈维护情况。备案信息不完整或有变更的督促部门网管员完成信息维护。

4) 汇总。每周报修处理情况应进行汇总分析。

4、机房管理

1) 出入机房随手关门。

2) 无关人员未经允许不得擅自进入机房。因工作需要进入机房的外来工作人员，需按要求进行登记，并在中心相关责任人的全程陪同下进入机房工作，离开时由陪同人员登记离开时间。外来人员进入机房时，除必要工具外，不得带入与工作无关的物品。

3) 未经信息技术部领导同意，任何单位和个人不得擅自移动、拆卸、带出或带入设备，如需进行有关施工，必须经领导同意后方可实施，实施时责任人应在场。

4) 保持环境整洁和适度照明,每月督促机房维护人员清除机柜内和设备表面的积尘，做好日常机房保洁工作。

5、工作要求

1) 准时上岗，坚守岗位。如需离岗处理其他事务，应安排其他人员代岗，代岗人员应履行当班人员工作职责。

2) 履行职责，严守纪律。机房重地，严禁带入火种或易燃、易爆物品，不得在机房吸烟或饮食，注意用电安全。

3) 文明接待，仪态端庄。办事不推诿，不拖延，不懈怠。接听电话要礼貌用语，规范用语，做好记录，及时安排；对工作范围之外的电话，耐心解答。

4) 规范操作，确保安全。严格遵守操作规范，不得擅自变更网络连接、加装网络设备及变更设置参数。

5) 重大情况，及时报告。遇有重大情况或本人无法解决的问题，应及时向中心领导汇报。

6) 机房整洁，环境优美。不随意堆放物品，技术资料、维修工具使用后及时交还保管人，如需出借需通知保管人进行登记，报废设备及设备包装物及时清理。

7) 机房日志，认真填写。值班巡检、网络和设备监控数据、故障处置、设备进出机房和外来人员出入机房等情况，应按要求如实登记在值班日志上。

8) 服从组织安排，认真完成领导交办的其他事项。

（五）附表

1、附表一：

机房的基本设施配置

序号	设　备	达到要求
1	空调	控制环境温度介于18℃至28℃之间；
2	UPS	输出功率：≥2kva； 输出电压：220V±4%； 输出频率：50Hz ±0.5%； 备用时间：≥30 分钟；

		类型：在线式
3	照明设施	满足目视照度
4	机房远程监控系统	实时图像监控； 温湿度监测； 照明监控； UPS 状态参数监测；
5	19”标准机柜	满足光缆设备、光电转换设备、网络交换设备、UPS、机房远程监控系统安装
6	机柜布置图	与实际情况相符，标贴于机柜侧面
7	设备标贴	标贴按照命名规范，清晰标注、易识别
8	防火设施	配备普通干式灭火器

七、信息资产管理制度

（一）职责

信息技术部

1、负责检查数据资产的安全管理情况。

2、负责本文件的编制和管理。

3、负责固定资产的管理，包括固定资产的采购、记录、变更、报废等。

4、负责备品备件的出入库管理。

5、负责对有形资产进行分类、分级和标记。

6、负责对备品备件进行分类。

7、在有形资产发生变更、报废或销毁时，负责检查资产中信息的处理情况。

8、负责检查台帐、信息系统中信息资产相关记录，并将记录情况纳入考核计划中。

各部门

1、负责对本部门数据资产的、分类分级和标记。

2、负责对备品备件的分级、标记和登记。

3、按资产的使用规则和限制，正确使用信息资产。

4、在有形资产和备品备件发生变更、报废或销毁时，负责检查并清除介质中敏感信息。

（二）工作程序

资产的分类分级

1、资产分类分为关键资产和非关键资产：

- 关键资产：对业务连续性和系统可用性影响大的资产（价格或价值较高的资产）。
- 非关键资产：对业务连续性和系统可用性影响小的资产（价格或价值较低的资产）。

2、数据资产可以按其对信息系统的重要性程度，以及信息的保密性、完整性、可用性被破坏后对信息系带来的影响，划分为以下几种安全级别：

- 敏感信息：涉及工作秘密等信息
- 一般信息：不涉及工作秘密的信息

资产的登记与标记

1、信息技术部对固定资产进行分类分级、登记，确定该资产的类型、编号、用途、位置、格式、规格、价值等具体信息；

2、各部门根据发放的资产清单及设备标牌，对有形资产进行粘贴标记，并指定资产责任人，由资产责任人对所负责的资产进行保护；

3、各部门在资产新增、更新、调拨、报废时，向信息技术部提出需求，由信息技术部审核，报主管领导批准后按照相关规定执行，由信息技术部更新《固定资产清单》；

4、信息技术部定期检查有形资产的标记与使用情况，对资产丢失，标签缺损的情况进行记录；

资产的使用与维护

1、各部门人员，应明确他们使用信息资产时的限制条件，应对信息资产的使用和管理负责。

2、各部门人员应确保在采用移动介质进行数据传输时，传输完毕应及时删除介质上保留的数据信息，对于只读介质，由本部门网络安全专员进行保存。

3、存储介质在长期存储时，应确保介质贮存地点应符合防火、防水、防震、防潮、防霉、防鼠害、防虫蛀、防静电、防磁等方面的安全要求，介质的存储要符合介质生产商对介质存储的要求。

4、定期对本部门存储介质中的数据进行备份和恢复测试，并进行测试记录，防止由于介质老化而导致的重要信息丢失。

5、涉及国家秘密的信息通过移动介质进行存储时，各部门应参照国家有关规定执行。

资产的移动管理

1、所有有形资产的移动必须经过资产责任部门的授权。

2、物理介质在物理地点之外运送时，为了防止未授权访问、不当使用或被毁坏，各部门应采取以下必要的措施：

- 物理介质的包装应采取防篡改的包装进行密封（即封口破坏后无法恢复原状，可以很容易发现未授权访问的企图），防止信息在送信的过程中泄漏或被修改。
- 含有敏感信息的物理介质必须由内部人员亲自押运，不得交由第三方公司单

独运送。

3、所有有形资产的移动必须登记。

资产的销毁

1、各部门检查并清空待报废设备内的所有信息，交信息技术部统一处理。

2、信息技术部对报废设备进行清点，形成《待报废设备清单》。

3、信息技术部定期对报废设备进行统一处理，处理前对设备的存储信息进行检查。

4、各部门根据介质上存储的信息的敏感程度，采取适当的措施对已报废的介质进行处理：

- 包含敏感信息的介质，应按照国家要求，去专门地点删除原有介质上的数据信息或进行消磁处理；对于只读介质，可采用粉碎等方式进行处理。
- 应对处置敏感介质做记录，以便保持审核踪迹。

八、介质管理规定

（一）介质购置

介质由信息技术部负责统一计划采购，编号，发放和登记管理。其余部门不得擅自购买使用。

（二）介质使用及维护管理

介质包括磁带、U 盘、光盘、硬盘、存储卡和打印出的文件等，对移动介质的管理如下：

1、移动介质在接入信息系统前，必须进行恶意代码、木马检测和杀毒处理，防止恶意代码侵入和传染给其它信息系统。

2、如果信息不再需要，需删除可重复使用的移动介质中的信息。

3、如果信息需要保存，则使用人应该保存在个人计算机中，而不应该放在移动介质中。

4、介质在长期保管时，其保管的地点必须满足防火、防水、防震、防潮、防霉、防鼠害、防虫蛀、防静电、防磁等方面的安全要求，介质的保管要符合介质生产商对介质保管的要求。

5、防止由于介质老化、失效而导致的重要数据丢失。

6、实行存储介质借用制度，由借用人填写《介质借用/领用申请表》，介质使用后应及时归还。管理员应做好相关的登记管理工作。

7、存储介质的保管工作必须符合国家相关管理制度。各类存储介质如未经批准严禁由个人私自带离单位。

8、根据所承载数据和软件的重要程度对介质进行分类和标识管理。

9、非涉密存储介质不得用于存储涉密信息，涉密存储介质也不得任意用作他途。涉密存储介质不得在非涉密计算机上使用。已定为涉密存储介质的密级不可降低。

（三）介质定期检查

定期对存储介质进行清点，收回不使用介质，核对使用人员登记表。定期对移动存储介质进行统一杀毒处理。

（四）介质维修

介质送出维修之前应进行申请审核，确保删除敏感信息，维修地点要送到专门的定点单位。如可能有敏感信息，维修过程应安排人员全程监督。

（五）介质的报废

对存储敏感信息的存储介质应在指定地点，由指定人员（并有人监督）进行安全的报废和处置，以免敏感信息外泄。

磁带可通过消磁或物理破坏的方式进行处置，确保消除磁带上所存储的敏感信息。

U 盘、硬盘、存储卡等可通过专业软件或多次格式化进行处置，或者采用物理方式进行破坏。

光盘可通过物理方式进行粉碎处理。

（六）附表 1 介质领用申请单

介质磁盘领用申请单

编号：

领用人		部 门		领用时间	
载体类型	移动磁盘□ U 盘□ 其它□（ ）			数 量	
申请理由：					
本部门领导审批意见： 签名 年 月 日					
执行机构审批意见： 签名 年 月 日					
注：1、本表由管理员负责填写 2、本表由信息技术部磁盘管理员负责存查					

（七）附表 2 介质借用/使用登记单

介质借用/使用登记表

部门名称：

介质编号	借用日期	借用人	归还日期	管理员	备注

九、设备安全管理制度

（一）IT 设备的购买

1、信息技术部在购买 IT 设备前，应对拟购买的 IT 设备进行试用，测试其性能及安全功能是否满足需求，若不能满足，则应考虑其他供应商或采取相应的控制措施。

2、选购网络安全产品，应对产品资质进行审查，选购通过国家权威机构认证的网络安全产品。

3、选购密码类产品，应对产品资质进行审查，使用国家保密主管机构批准的密码类产品。

（二）IT 设备的登记及领用

1、所有采购来的 IT 设备，应先由信息技术部资产管理员处进行资产登记，在设备台帐中记录该设备的品牌、型号、S/N 号、详细配置、保修期限等，在设备上粘贴设备标签后，资产入库。

2、需使用 IT 设备的，应由资产使用人提出资产领用申请，经部门负责人审批后，至资产管理员处办理领用。资产管理员在资产台帐中记录该资产的领用人，领用人在设备标签上进行签字后，方能办理资产出库，交由领用人使用。

（三）IT 设备的维护

1、各领用人为该 IT 设备的责任人，负责该 IT 设备的正常使用，在设备发生问题时负责联系相关部门进行维修。如因领用人责任造成该 IT 设备损坏，则领用人需照价赔偿。

2、各领用人应按照信息设备维护要求的时间间隔和规范，对设备进行维护。

3、IT 设备如需升级或维修，因由领用人提出申请，经主管领导批准后，进行维修或升级。

4、送外单位维修的 IT 设备不得存储内部敏感信息。在送修前应由中心安全管理员对送修设备是否存有内部敏感信息进行检查。如有，应先拆除硬盘等存储部件，或使用信息清除软件对磁盘信息进行彻底清除后，方能送修。

5、重要 IT 设备的维护人员在现场维护过程中，应有信息技术部人员在场，外部人员的访问应进行登记，必要时要求其签署保密协议。

6、IT 设备进行升级或维修后，如设备配置进行了变更，则应由负责设备升级人员将配置后的信息报资产管理员备案。

7、任何IT设备搬入或搬离中心机房必须提交申请，由中心机房管理部门负责人签字同意后方可执行。

（四）IT设备的报废

1、IT设备确因设备老化、性能落后等原因，造成设备无法继续使用的，由资产管理员提出报废申请，资产原值1万元以下的设备，经分管财务领导批准后，实施报废处理；资产原值1万元以上的设备由党组会议讨论通过并报财政局审批后实施报废处理。报废设备在资产台帐中登记。

2、IT设备在报废处理前，应由安全管理员对其是否存有内部敏感信息进行检查。如有，应对其存储部件进行消磁或物理毁坏，确保不会因设备处置不当造成泄密。

（五）设备的操作规程

应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。（参照设备的操作规程、技术手册、使用说明书）

十、信息分类分级标识管理制度

（一）信息资产分类标准分类原则

根据信息资产的表现形式，可将信息资产分为系统相关信息、业务信息等。

（二）信息等级划分标准

信息包括数据和文档，各部门需将所有信息按照敏感性和重要程度分为不同的等级，并按不同的等级进行标识和处理。

（三）等级划分标准

信息等级划分标准描述如下：

涉及国家秘密的信息数据按照相关国家保密要求进行处理。涉及国家秘密的信息不准进入信息系统。

这里只涉及业务系统秘密的信息。

1、敏感信息：最重要的业务系统秘密，泄露会使业务系统安全遭受特别严重的损害。

保存方法：统一存放在保险柜，根据相关保密规定。

处置方法：对于敏感信息需严禁复制、存储、邮寄、传真和 E-MAIL，不允许将其通过电话和手机等以交谈方式告诉第三方，如需借阅必须经过授权或填写借阅记录。

2、内部信息：重要的业务系统秘密，泄露会使系统的安全和利益遭受严重的损害。

保存方法：各部门分别存放在加锁文件柜中。

处置方法：可在得到授权的情况下对机密文件进行复制、存储、邮寄、传真和 E-MAIL，可在授权的情况下将其部分内容通过电话和手机等以交谈方式告诉相关人员，如需借阅必须经过授权或填写借阅记录。

3、公开信息：一般的业务系统秘密，泄露会使业务系统安全遭受损害。

保存方法：指定专人管理，具有专门存放的文件夹。

处置方法：对于秘密文件可以在本单位内或部门内部复制、存储，可以传真和 E-MAIL 给相关人员，可以将其通过电话和手机等方式告诉相关人员，如需借阅必须经过授权或填写借阅记录。

4、可以公开：可以在单位内部传阅。

保存方法：各人文件夹。

（四）标记与处理

在对信息划分等级的同时，必须对信息进行标记。信息的标记遵循以下规范：

1、电子文档的右上角加上方框来，方框高 2cm，宽 3cm，方框内加注字体大小为 4 号，字体为宋体。

2、敏感信息在输出时要携带合适的分类标记，输出方式可以表现为打印出的报告、屏幕显示、记录媒体（例如磁带、磁盘、CD）、电子报文和文件传送等。

3、所有的数据复印都要清楚，以便使授权的接收者注意。

十一、网络安全管理制度

（一）职责

信息技术部：

1、负责制定和管理本文件。

2、负责制定专网访问控制策略。

3、负责受理对专网的访问申请和授权。

4、负责对专网设备状态、网络运行状况的日常检查工作。

5、负责维护专网运行记录；负责对专网安全管理工作进行监督和检查。

（二）网络安全规划

信息技术部在网络系统规划、升级、改造建设过程中，应组织相关人员对网络建设方案进行评审，使方案满足网络安全管理要求。

（三）网络接入控制

1、各部门对涉及到网络变更方面的需求（如网络结构变更、终端网络需求变更（如 Hub 的接入））、非常规性网络访问（如外来人员临时性访问），需向信息技术部提出书面申请，经确认后方可进行操作。

2、无线网络由信息技术部统一管理，其他人员不得擅自接入，特殊需要时，需向信息技术部提出申请，经同意后由中心负责接入并及时回收。

3、信息技术部负责网络与其他外部单位网络的安全防护，在网络边界处采取安全措施进行有效隔离防护，并对违规行为进行检查和阻断。

4、信息技术部负责网络的 VLAN 和安全域划分，不同业务应用系统尽量安排在不同的安全域中，各 VLAN 和安全域间应采取有效的访问控制措施。

5、信息技术部对网络设备、网络设备之间的连接线缆进行标识，重要网络端口也须进行详细标识。

6、应保证所有与外部系统的连接均得到授权和批准。

（四）网络安全审计

1、信息技术部采取开启网络设备日志，记录与网络安全相关的操作与活动，并定期分析并对结果进行记录。

2、日志保存时间应至少保证在一个月以上。

3、信息技术部在网络关键位置采取网络审计手段，对网络访问操作行为进行记

录，定期对记录进行分析并对结果进行记录。

（五）网络设备管理

1、信息技术部制定网络备份策略（如网络配置备份，并做好相应备案）。

2、信息技术部每月对网络配置文件进行备份，并做好备份记录。

3、信息技术部做好网络配置、网络设备日志及网络设备备件的保存与管理，保证备份的安全性。

4、根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份。

5、建立日志服务器，保存日志时间要求超过 6 个月。

6、定期（每半年）对网络设备口令进行更新。

（六）网络安全检查

1、信息技术部制定详细的网络检查项目，负责进行网络系统运行的日常检查工作，将检查结果进行记录。检查内容参考《安全检查表》。

2、信息技术部定期对网络设备配置进行检查和评估，确保网络配置与安全策略保持一致，并对检查结果进行记录。

3、定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补。

（七）网络访问控制

1、信息技术部制定网络访问控制策略，并做好相应备案。

2、访问控制策略内容应包括：

- 根据业务、管理等情况，对不同的部门接入进行划分。
- 明确各部门只能访问被允许访问的网络和网络服务。
- 规定各部门访问网络和网络服务使用的手段（如拨号、VPN 等）。

3、信息技术部基于专网访问控制策略进行网络路由控制。

4、如有部门需要接入网络，由信息技术部审核开通，确保网络用户的访问权限符合网络访问控制策略。

十二、系统安全管理制度

（一）系统维护管理

1、信息技术部的操作人员上岗前必须经过上岗前的专业知识培训，包括专门的网络安全培训，能正确地执行本岗位操作工作。

2、重要信息系统的操作手册和系统运行维护保养手册应作为工作秘密由各部门加以保护，由信息技术部存档。应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。可通过运维安全审计系统监控并记录用户的日常操作，设置系统日志的保存时间。

3、定期对运行日志和审计数据进行分析，以便及时发现异常行为。

4、定期对系统使用中的网络安全管理情况进行检查，检查内容参加《网络安全检查细则》。

5、信息技术部应对系统中运行的软件版本进行严格控制，对系统软件版本升级、补丁更新、安全加固等活动组织评审和测试，防止因上述变更影响到应用系统的正常运行。

6、系统补丁的安装：应安装系统的最新补丁程序，在安装系统补丁前，应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装。

7、系统安全策略中应明确系统的安全配置，如 IBM AIX 安全配置、Linux 安全配置、SCO UNIX 安全配置、Windows2000 安全配置、Windows2003 安全配置、Windows XP 安全配置、Windows NT 安全配置。（如：Windows2003 安全配置包括：1、**限制不必要的用户数量。**去掉所有的测试用账户、共享账号、普通部门账号等不必要账号。用户组策略设置相应权限，并且经常检查系统的账户，删除已经不使用的账户。**2、禁用不必要的服务**建议禁用如下服务：Remote Registry Service、Routing and Remote Access、DNS Client、DHCP Client、Messenger、Terminal Services、Telnet；其它的系统安全配置：禁止 Guest 账号、限制不必要的用户数量、系统 administrator 账号改名、设置屏幕保护密码、禁用 TCP/IP 上的 NetBIOS、设置审核策略、删除默认共享、防止 SYN 洪水攻击、禁止 IPC 空连接、禁止响应 ICMP 路由通告报文、防止 ICMP 重定向报文的攻击、不支持 IGMP 协议等。）

8、定期对系统进行漏洞扫描，对发现的系统安全漏洞及时进行修补。

（二）系统访问控制

基于业务和访问的安全要求，建立各应用系统的访问控制策略，作为系统维护手册的一部分。

1、访问控制策略应考虑到下列内容：

- 各个业务应用的安全要求；
- 业务应用中工作角色和用户访问需求；
- 网络环境中的访问权限的管理要求；
- 访问控制角色的分离，例如访问请求、访问授权、访问管理；
- 用户访问请求的正式授权管理要求；
- 用户访问控制的定期检查与评审要求；
- 用户访问权的取消。

2、基于访问控制策略，对操作系统的登录程序加以控制：

- 不显示系统或应用标识符，直到登录过程已成功完成为止；
- 显示只有已授权的用户才能访问计算机的告警通知；
- 在登录过程中，不提供对未授权用户的帮助消息；
- 限制所允许的不成功登录尝试的次数；
- 记录不成功的尝试和成功的尝试；
- 如果达到登录的最大尝试次数，向系统控制台发送警报消息。

3、系统管理员应限制用户对应用系统远程访问的范围和内容，在远程访问过程结束后应确保断开连接。

4、系统管理员负责记录用户远程访问操作过程，包括访问时间、连接方式、访问用户、操作过程等。

（三）系统用户安全管理

1、系统用户注册与注销程序

- 在服务器和系统进行安装时，要改变默认的操作系统管理员账号名称和数据库账号名称。
- 各信息系统管理人员负责定期（每月）检查并取消或封锁多余的用户 ID 和账号，确保多余的用户 ID 不会发给其他用户。

2、系统用户口令管理

➢ 在用户初次使用应用系统时，系统管理员应提供给一个安全的临时口令，并强制其立即修改；临时口令应以安全的方式给予用户，不得使用第三方或未保护的（明文）电子邮件消息；

➢ 系统管理员应对用户口令设置进行指导和要求，如口令长度和复杂性、定期更换等，口令字符数字结合，长度超过6位，每半年更新一次；

➢ 系统管理员应确保口令不以未保护的形式存储在计算机系统内；

➢ 各系统管理员应在系统或软件安装后改变提供商的默认口令。

3、特殊权限管理应遵守用户注册和注销管理程序的规定，特殊权限包括操作系统、数据库管理系统和每个应用程序，特殊权限应被分配一个不同于正常业务用途所用的用户ID。

（四）系统备份

1、信息技术部制定系统备份策略，包括系统配置备份和设备备份，并做好相应备案。

2、信息技术部根据系统备份策略定期做好系统配置备份和系统设备备份。

3、信息技术部做好系统配置及设备备份的保存与管理，保证备份的安全性。

4、信息技术部定期对配置备份恢复和测试，确保系统备份的可用性。

十三、恶意代码防范管理制度

（一）职责

建立防杀计算机恶意代码的责任制。

信息技术部职责：

1、 负责开展技术培训；

2、 负责防恶意代码系统的统一升级；

3、 负责各系统的补丁升级、软件升级和分发；

4、 负责配置防恶意代码系统策略，定期对系统恶意代码进行扫描，并组织相关部门进行恶意代码查杀；

（二）防恶意代码系统的规划与部署

1、每台接入网络的计算机，必须安装统一的网络版杀毒软件，主系统将自动启动计算机恶意代码特征码升级和本机恶意代码查杀功能，查杀结果将会自动上传至防恶意代码系统控制台。

2、安装统一的网络版杀毒软件的计算机，不得自行卸载或安装第二套防杀恶意代码软件，以免造成杀毒功能失效或系统不稳定情况。

3、任何人员不得擅自停用杀毒软件。

（三）恶意代码防范的日常管理

1、定期进行培训，提高所有用户的防恶意代码意识和安全技能。

2、及时告知防恶意代码软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行恶意代码检查，对外来计算机或存储设备接入网络系统之前也应进行恶意代码检查。

3、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。

4、定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防恶意代码产品、防恶意代码网关和邮件防恶意代码网关上截获的危险恶意代码或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

5、终端用户要及时进行补丁升级，避免因操作系统漏洞而造成的恶意代码入侵，并做好本机重要数据的备份。

6、加强计算机恶意代码、木马防范基础工作，计算机终端应设置开机密码，严格设置共享资源读、写权限；介质（磁盘、光盘和U盘等）复制、使用前先作恶意代

码检测，确认无恶意代码后才能使用。

7、连接互联网的终端用户应提高警惕,不下载和运行来历不明的程序，对于不明来历的邮件附件也不要随意打开。下载的软件、信息和数据要先查毒后使用。

8、各部门负责本部门所辖设备的安全管理，移动介质、移动设备接入网络要进行严格控制，如因上述原因发生恶意代码事件，由本部门承担责任。

9、各部门负责本部门所辖安全管理，禁止任何人在系统上传递无关信息，如因上述原因发生恶意代码事件，由本部门承担责任。

10、各部门负责本部门所辖网络的接入管理，禁止任何人私自扩展、加装计算机网络和私自跳接计算机连网的信息点，并严禁在网上侦听，如因上述原因发生网络安全事件，由本部门承担责任。

11、因业务需要使用外来移动介质（设备）的，必须将介质接入杀毒专用计算机（与各系统物理隔离）进行恶意代码检测，确认无毒后，方可接入网络内使用。

12、信息技术部定期检查网络内服务器的杀毒软件运行状态，并将检查结果进行记录；并将检查结果纳入部门考核。

（四）恶意代码的查杀与处理

1、一旦发生恶意代码入侵事件，进行恶意代码查杀工作，如下载专杀工具、进行手工杀毒等。

2、一旦部门局域网内计算机发生感染恶意代码疫情，为避免计算机恶意代码扩散，信息技术部将采取直接断开网络，采取进一步措施查杀恶意代码，在疫情警报解除后，再恢复网络间物理链路的连接。

十四、变更控制管理制度

（一）职责

变更申请人

1、指系统相关人员，如系统维护人员、用户、厂商等；

2、负责识别变更需求，提出变更申请；

3、重大变更：由日常变更审批人根据系统相关人员申请，提出重大变更申请。

重大变更审批人

1、重大变更审批：指局领导或信息技术部领导负责；

2、负责组织重大技术变更的审批、评估；

3、负责组织重大技术变更的计划，回退过程的测试与演练；

4、负责组织重大技术变更的测试、实施；

5、负责重大技术变更后的跟踪与反馈。

日常变更审批人

1、日常变更审批人：指信息技术部各系统负责人；

2、审批日常变更申请；

3、负责组织制定日常变更计划；

4、负责组织人员实施日常变更；

5、负责向网络安全领导小组进行重大技术变更的申请和报告；

6、负责本文件的编制和管理；

7、参与重大变更的审批、评估；

8、参与重大变更的计划，回退过程的测试与演练；

9、参与重大变更的测试、实施；

10、参与重大变更后的跟踪与反馈。

信息技术部

1、协助变更审批人对变更申请进行审核；

2、协助制定、调整变更计划及发布实施计划；

3、向网络安全负责人汇报变更过程中发现的问题及对变更实施的改进建议。

（二）变更的申请和审批

1、日常变更申请人识别具体的变更需求（如范围、可交付成果、时限、组织等），

填写《变更申请表》，交给变更审批人进行审批。

2、相应的变更审批人对变更申请进行审核，如判断此变更属于日常变更，由日常变更审批人审批后自行组织实施；如属于重大技术变更，则提交网络安全领导小组审批。

3、重大技术变更的审批：

- 由日常变更审批人将《变更申请表》进行签字确认后提交网络安全领导小组审批；
- 网络安全领导小组负责领导组织进行变更评估及编写变更方案（包括变更需求的详细描述；可以选择的变更方式；变更所需的成本及带来的利益；变更的风险；变更对业务、系统或项目带来的影响；变更对原有安全措施以及数据完整性的影响；变更的建议和计划）；
- 由网络安全领导小组负责领导组织对变更方案进行审批，经同意后组织实施。

（三）日常变更的实施

1、变更实施前由变更实施人员进行备份，变更实施后进行变更情况记录；

2、如变更不成功，立即按照变更实施计划中的回退计划实行变更回退过程，使其状态回到变更前的状态，并进行记录；

3、变更完成后由变更实施人员进行后期跟踪及反馈，并进行记录。

（四）重大变更的实施

1、对测试情况进行记录；

2、变更实施前通知所有将受变更影响的用户；

3、变更实施前由变更实施人员进行备份，变更实施后进行变更情况记录。

（五）重大变更的验证和归档

1、变更完成后由网络安全领导小组负责领导组织进行后期跟踪及反馈，并进行记录；

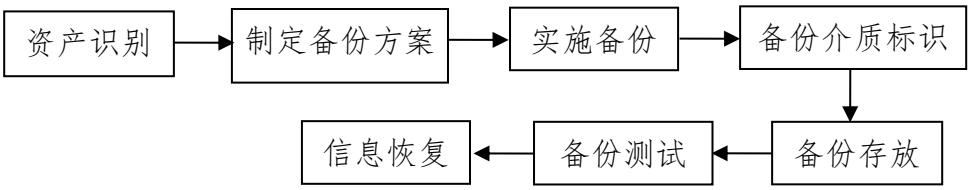
2、重大变更结束后，对相关文件进行更新，报网络安全领导小组负责领导。

变更申请表

申请公司名称		申请人		提交时间	
联系电话			移动电话		
申请变更内容描述					
申请变更时间			变更结束时间		
受影响的网络、用户或服务					
需求提出公司系统负责人意　见	签字：　　年　　月　　日				
以上内容为需求变更提出系统建设、运维公司或厂商填写					
日常变更审批负责人意见	签字：　　年　　月　　日				
重大变更审批负责人意见（重大变更时填写）	签字：　　年　　月　　日				
评审员会或专家意见	签字：　　年　　月　　日				
备　注					

十五、备份恢复管理制度

（一）程序



产识别

1、收集需要备份的资产相关信息，主要包括资产的重要性、资产的保护级别等属性；对确定的重要业务数据、操作系统、应用系统、数据库等进行备份。需要检查的信息资产可能包括：业务运作数据、重要的信息数据、操作系统、系统配置参数、技术文件、档案资料、应用软件、软件源代码等。

2、无法备份的信息，尽量多使用其复制件，保存原件。

（三）制定备份与恢复策略

根据资产识别的结果和备份级别制定备份计划，具体包括：

1、确定备份周期：根据信息更新速度、易损坏成度及备份介质的有效期，确定周期。

2、确定备份介质类型：确定备份使用的介质，一般是光盘、软盘或硬盘，要同时考虑成本与可靠性。

3、确定备份方式：一般采用复制、双系统同步、转储、压缩复制等。

4、确定备份工具：备份使用的工具，如光盘记录机、复印机、软驱、压缩软件等，选择工具时，要确定在信息失效之前，对应的恢复工具可用。

5、确定备份数量：确定备份的数量，一般信息备份一份即可，对于特别重要的信息需要备份多份。

6、存放位置：备份信息须与原始信息分开存放，要根据信息保密级别有相应的保密措施。

7、责任人：确定备份的责任人。

8、备份方案需提交给相关部门负责人，经部门主任确认并批准后予以实施。

9、当责任人没有足够的工具或条件时，可要求相关工程师协助。

（四）备份计划实施

对分散的信息进行整理、归类；处理信息，在备份信息前，先将其复制到有备份工具的计算机上；执行备份程序；检查备份数据的可用性；清理过程数据。

（五）备份的介质标识

标识应依据介质本身的特点，加标签或直接手写在介质上；对于已经有标识的纸面文档的复印件，可不用再另加标识；各部门应采取适宜的方法对备份信息介质进行标识，防止备份信息的误用，标识的内容包括：

1、备份信息的名称；备份的日期；版本号；必要时，备份还原工具。

2、考虑信息本身在被使用时的特点，确定标识的内容。

（六）备份介质的安全存放

备份完毕，备份操作员应提交备份成果：备份介质；备份过程中的相关文件，如：备份记录文件、备份恢复工具或软件、备份恢复指导书等；将备份介质保存到指定的位置，需按时间顺序存放。

介质的存储主要考虑以下几个方面：备份介质须保存在适宜的环境中；对备份介质进行异地存储，以避免主要场地发生灾难时资产受到损坏；备份介质存储场地的物理和环境保护；分配专人对备份介质进行管理，对备份介质的访问进行控制。

（七）信息恢复

当重要信息被篡改、破坏或丢失时，使用备份数据恢复信息；当存在多份备份时，应根据需要选择合适的备份；备份信息使用前，应检查备份信息的完整性和可用性。

十六、安全事件管理制度

（一）网络安全事件分类

网络安全事件一般可以分为攻击类、故障类和灾害类等，可能造成的后果是业务中断、系统宕机、网络瘫痪、信息破坏等。根据专网的网络安全事件的发生原因、性质和机理，网络安全事件主要分为有害程序事件、网络攻击事件、信息破坏事件、设备设施故障和灾害性事件五类：

1、有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马、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。

2、网络攻击事件分为拒绝服务攻击事件、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。

3、信息破坏事件分为信息篡改事件、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。

4、设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

5、灾害性事件是指自然灾害等其他突发事件导致的网络和信息系统故障。

（二）网络安全事件分级

根据网络安全事件的分级考虑要素，并结合嘉兴的工作特点，将网络安全事件划分为四个级别：特别重大事件、重大事件、较大事件和一般事件。

1、特别重大事件是指能够导致特别严重影响或破坏的网络安全事件，包括以下情况：全部或大部分主要信息系统瘫痪，造成本单位全部业务长时间无法正常进行；数据由于各种原因遭受特别严重损坏，导致核心数据无法恢复；对公众发布信息功能受到特别严重破坏，或者所发布信息被篡改，引起社会不良影响。

2、重大事件是指能够导致严重影响或破坏的网络安全事件，包括以下情况：核心业务信息系统遭受严重的系统损失，导致业务工作在一段时间内无法正常进行；或核心业务信息系统的数据遭受严重损失，数据库需要作恢复备份操作。

3、较大事件是指能够导致较严重影响或破坏的网络安全事件，包括以下情况：核心业务信息系统局部遭受较严重的系统损失，但不影响整体业务正常开展；核心业务数据局部遭到严重破坏，但不影响整体数据质量。

4、一般事件是指能够导致较小影响或破坏的网络安全事件，包括以下情况：业

务系统运行维护过程中，出现的常见故障，能够及时恢复，损失在可控范围内，不会影响业务数据的完整性和正确性。

（三）网络安全事件的通报

突发事件具有突发性、不可预测性和紧急性，信息系统及运行环境遇突发事件时应及时通报，可通过IT服务台、邮箱、电话、短信等通知形式，向突发事件领导小组及时通报，提高突发事件的预警管理水平。

业务系统恢复正常后，信息技术部负责通过IT服务台公告、手机短信等方式通知突发事件领导小组及相关业务部门。

（四）网络安全事件的预防

1、必须积极贯彻预防为主、严格管理的原则，评价事件发生的潜在因素和可能程度；组织制定和监督实施预防措施、操作规程或工作标准；配置必要资源；开展教育培训、检查、考核和整改活动，控制或消除可能导致事件发生的各种因素。预防措施应下达至直接相关的层次和岗位。

2、信息技术部应根据事件发生可能造成的危害、损失，组织制定不同级别的应急预案，并对应急预案的可靠性进行评价。应急预案应当受控和备案，并发放至直接相关层次和岗位，保存相关记录。应急预案应定期进行演练和培训，必要时组织修订。

（五）网络安全事件的应对

1、事件发生时，信息技术部应立即启动应急预案或采取有效措施，组织相关人员全力而有序地组织抢救抢修，防止事件扩大，消除各种危险，尽快恢复系统，将损失减到最低程度。

2、相关人员应在事发或接到事发报告后尽快到达事发现场，开展事件处理工作。

发生重大网络安全事件，在迅速进行应急处理或者请求其他力量支援进行应急处理的同时，尽可能保存好原始证据，保护好现场；如涉及违法犯罪的，还应当同时依法报告公安、安全等部门。

3、在应急处理过程中，应当采取手工记录、截屏、文件备份和影像设备记录等多种手段，对应急处理的步骤和结果进行详细记录。

（六）网络安全事件的事后处理

1、对于网络安全事件，在故障排除或采取必要措施后，信息技术部应做出事故评定报告，存档备案。必要时，可邀请托维护单位以外有能力的机构做出技术鉴定。.

2、信息技术部应在事后了解事件发生经过，收集相关资料，查明事件发生的原因、危害程度及造成的损失等情况，检查预防和控制事件发生的措施以及事件发生后应急预案是否得当并得到落实，确定事件的级别和性质，查明相关责任并提出处理建议，提出防止类似事件再次发生的措施和建议。

（七）网络安全事件的整改

信息技术部应在事件调查结束后迅速组织制定和下达事件整改措施，明确措施内容、完成期限和检查方式，并监督实施。在规定的期限内，完成相应的整改工作，防止同类事件的再次发生。

（八）事件备案

事后应当及时登记存档备案，对事件发生原因，造成损失，处理方法，解决时间，最终结果等相关信息详细记录。并为相关问题处理提出方案，防止事件再次发生。

（九）附表 1:《安全事件登记表》

安全事件登记表

事件发生部门：	事件发生时间：
事件调查处理部门：	调查人员：
事件类型：	
事件级别：　　☐重大　　☐较大　　☐一般	
事件描述及处理经过	
调查负责人：	日期：

事件影响及原因分析	
调查负责人：	日期：
处理意见	
批准人：	日期：
纠正预防措施	
责任部门：	日期：
纠正预防措施的验证	
验证人：	日期：