ICS 65.160
X 89
备案号：44828—2014

YC

中华人民共和国烟草行业标准

YC/T 495—2014

烟草行业信息系统安全等级保护实施规范

Implementation specifications for classified protection of information system of tobacco industry

2014-03-24 发布　　2014-04-15 实施

国家烟草专卖局　发布

目　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本标准的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准由国家烟草专卖局提出。

本标准由全国烟草标准化技术委员会信息分技术委员会(SAC/TC 144/SC 7)归口。

本标准起草单位:国家烟草专卖局烟草经济信息中心、广东中烟工业有限责任公司、公安部第一研究所。

本标准主要起草人:庄红、王海清、李超、耿欣、易伟文、林惠真、焉鹤、吕由。

烟草行业信息系统安全等级保护实施规范

1 范围

本标准规定了烟草行业信息系统安全等级保护实施过程中的流程、等级划分与确定方法、技术保护和安全管理的要求。

本标准适用于指导烟草行业新建和已投入使用的信息系统安全等级保护的实施，为烟草行业信息系统的定级、技术防护、安全管理提供依据。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 2887—2011 计算机场地通用规范

GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南

GB/T 21052—2007 信息安全技术 信息系统物理安全技术要求

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 25058—2010 信息安全技术 信息系统安全等级保护实施指南

GB 50016—2006 建筑设计防火规范

GB 50057—2010 建筑物防雷设计规范

GB 50174—2008 电子信息系统机房设计规范

GB 50222—1995(2001年修订版) 建筑内部装修设计防火规范

SJ/T 10796—2001 防静电活动地板通用规范

信息安全等级保护管理办法(公通字[2007]43号文件)

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全保护能力 security protection ability

系统能够抵御威胁、发现安全事件以及在系统遭到损害后能够恢复先前状态等的程度。

[GB/T 22239—2008，定义 3.1]

3.2

系统服务 system service

信息系统为支撑其所承载业务而提供的程序化过程。

[GB/T 22240—2008，定义 3.4]

3.3

等级测评 classified security testing and evaluation

确定信息系统安全保护能力是否达到相应等级基本要求的过程。

[GB/T 25058—2010,定义 3.1]

3.4

恢复时间目标 recovery time objective

灾难发生后,信息系统或业务功能从停顿到必须恢复的时间要求。

[GB/T 20988—2007,定义 3.18]

4 烟草行业信息系统安全等级保护实施流程

4.1 实施流程

烟草行业新建信息系统安全等级保护实施流程如图 1 所示。

烟草行业已投入使用的信息系统安全等级保护实施流程如图 2 所示。

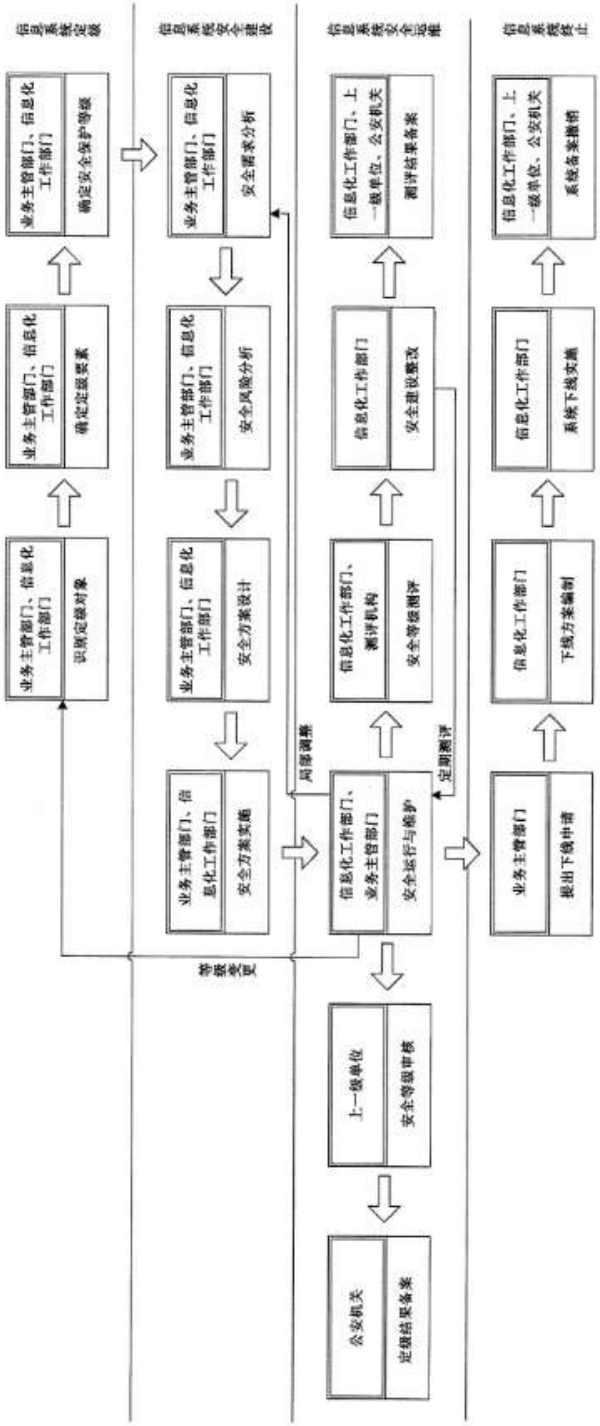

图 1　新建信息系统安全等级保护实施流程图

图 2　已投入使用的信息系统安全等级保护实施流程图

4.2 实施活动

4.2.1 新建信息系统

新建信息系统安全等级保护实施主要活动如下：

a) 信息系统定级

信息系统定级主要内容包括识别定级对象、确定定级要素和确定安全保护等级。信息化工作部门和业务主管部门应按照国家和行业有关标准、规定，确定需要定级的信息系统及定级要素，根据定级要素初步确定信息系统的安全保护等级。

b) 信息系统安全建设

信息系统安全建设主要内容包括安全需求分析、安全风险分析、安全方案设计和安全方案实施。信息化工作部门和业务主管部门应根据信息系统定级情况，明确安全需求，分析安全风险，按照附录A中相应等级的基本要求，设计合理的、满足等级保护要求的安全方案，指导信息系统安全建设项目实施。

c) 信息系统安全运维

信息系统安全运维主要内容包括安全运行与维护、安全等级测评、安全整改和系统备案。在信息系统正式上线运行后，信息化工作部门应按照国家和行业有关标准、规定，将信息系统定级结果报上一级单位进行审核，报公安机关进行备案；同时应和业务主管部门按照国家和行业有关标准、规定，根据附录A中信息系统安全等级保护的基本要求，开展安全运维工作和安全等级测评工作，对发现的问题进行及时整改，将信息系统测评结果报公安机关和上一级单位。

在信息系统安全运维阶段，信息系统因需求变化等原因导致局部调整而系统的安全保护等级并未改变，应重新进行安全方案设计，调整和实施安全措施，确保满足等级保护的要求；信息系统发生较大变更导致系统安全保护等级发生变化时，应重新开始信息系统安全等级保护的实施过程。

d) 信息系统终止

信息系统终止主要内容包括提出下线申请、下线方案编制及审批、系统下线实施和系统备案撤销。当信息系统停止运行时，业务主管部门应向信息化工作部门提出下线申请，信息化工作部门受理后按照系统下线方案进行实施，并及时到公安机关办理备案撤销手续，同时将有关情况报上一级单位。

4.2.2 已投入使用信息系统

已投入使用信息系统安全等级保护实施主要活动如下：

a) 信息系统定级

信息系统定级主要内容包括识别定级对象、确定定级要素、确定安全保护等级、安全等级审核和定级结果备案。信息化工作部门和业务主管部门应按照国家和行业有关标准、规定，确定需要定级的信息系统及其定级要素，根据定级要素确定信息系统的安全保护等级，将信息系统定级结果报上一级单位进行审核，审核通过后报公安机关进行备案。

b) 信息系统安全运维

信息系统安全运维主要内容包括安全运行与维护、安全等级测评、安全整改和测评结果备案。信息化工作部门和业务主管部门按照国家和行业标准、规定，根据确定的信息系统安全保护等级，按照附录A中相应的基本要求，开展安全运维工作和安全等级测评工作，对发现的问题进行及时整改和测评，并将信息系统测评结果报公安机关和上一级单位。

在信息系统安全运维阶段，信息系统发生较大变更导致系统安全保护等级发生变化时，应按照新建信息系统安全等级保护实施过程开展信息系统等级保护工作。

c) 信息系统终止

信息系统终止主要内容包括提出下线申请、下线方案编制及审批、系统下线实施和系统备案撤销。当信息系统停止运行时，业务主管部门应向信息化工作部门提出下线申请，信息化工作部门受理后按照系统下线方案进行实施，并及时到公安机关办理备案撤销手续，同时将有关情况报上一级单位。

5 信息系统安全保护等级

5.1 等级划分

参照 GB/T 22240—2008，烟草行业信息系统安全保护等级由低到高依次划分为自主保护级、指导保护级、监督保护级、强制保护级和专控保护级五个安全等级。信息系统安全等级划分见表 1。

表 1 信息系统安全等级划分

等级	描　　述
第一级	信息系统受到破坏后(主要指系统无法运行，或者系统数据被泄露、被篡改或丢失。以下同)，会对公民的合法权益、其他组织的合法权益、本单位的合法权益以及生产经营活动造成损害，但不损害国家安全、社会秩序和公共利益。各单位按有关规定对第一级信息系统进行自行保护，它需要实施系统安全运行所需的基本的技术要求和安全管理要求
第二级	信息系统受到破坏后，会对公民的合法权益、其他组织的合法权益、本单位的合法权益以及生产经营活动造成严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。各单位在国家烟草专卖局(以下简称国家局)有关部门的指导下对第二级信息系统进行保护，它需要实施系统安全运行所需的一定程度的技术要求和安全管理要求
第三级	信息系统受到破坏后，会对行业的合法权益以及行业生产经营活动造成严重损害，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。各单位在国家局有关部门的监督下对第三级信息系统进行保护，它需要实施系统安全运行所需的高程度的技术要求和严格的安全管理要求
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。各单位应依据国家有关管理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对第四级信息系统信息安全等级保护工作进行强制监督、检查
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。各单位应依据国家管理规范、技术标准和业务特殊安全需求进行保护。国家指定专门部门对第五级信息系统信息安全等级保护工作进行专门监督、检查

5.2 安全保护等级确定方法

5.2.1 识别定级对象

信息化工作部门和业务主管部门应根据烟草行业信息系统的重要程度和业务对信息系统的依赖度进行综合分析，确定需要定级的信息系统。作为定级对象的信息系统应当满足以下条件：

——明确了业务主管部门；

——具有信息系统的基本要素，是指由相关配套的设备、设施按照一定的应用目标和规则组合而成的有形实体，某个单一的系统组件，如服务器、终端、网络设备等不作为单独定级对象；

——承载单一的或相对独立的业务应用。

若承载多个业务应用的信息系统进行集成，且业务应用流程和数据相互关联，则可作为一个定级对象，如企业资源计划系统(简称 ERP 系统)、生产执行系统(简称 MES 系统)；若需定级的信息系统构成

比较复杂，则可根据信息系统承载的多项业务类型、提供的服务范围等方式，将系统划分为若干业务子系统分别定级。

5.2.2 确定定级要素

在确定安全保护等级时，应遵循 GB/T 22240—2008 的要求，根据信息系统受到破坏时所侵害的客体及侵害的程度来确定安全保护等级。受到破坏时所侵害的客体及侵害的程度应根据以下定级要素进行判断：

a） 业务信息类型

业务信息类型反映了信息资产在信息系统中应受到的保护程度，业务信息类型分类如下：

——公开信息：是指国家公开共享的信息、组织机构公开共享的信息、公民个人可公开共享的信息。当公开信息被篡改或受到破坏，可能会造成经济纠纷、法律纠纷和较小社会影响等；

——专有信息：是指国家或组织机构内部共享、内部受限、内部专控信息，以及公民个人专有信息。当专有信息被泄露或受到破坏，可能会造成经济纠纷、法律纠纷和一定社会影响等；

——重要信息：是指国家秘密信息以外的受国家法律保护的商业秘密和个人隐私信息，以及地理、人口、法人、统计等基础信息。重要信息被泄露或受到破坏，可能产生较大社会不良影响，可能侵害公共利益、国家安全。

b） 系统服务范围

烟草行业信息系统的服务范围可划分为局部性、区域性和全局性：

——局部性：系统遭到破坏后，只对本单位内部范围内的业务工作造成影响，可能会给本单位造成一定的财产损失、法律纠纷等。不影响本单位对所属单位的管理工作，不会对社会造成不良影响，不会影响与其他单位有关联的各项工作；

——区域性：系统遭到破坏后，对本省范围内的业务工作造成影响，不涉及与其他单位有关联的各项工作。可能会造成业务能力下降，产生一定社会不良影响；

——全局性：系统遭到破坏后，对省级单位之间的相互关联工作造成影响，甚至给全行业范围的业务和管理工作带来较大影响或造成较大社会不良影响，可能侵害公共利益。

c） 系统运行环境

——互联网：运行在互联网上的信息系统，面向社会公众，社会影响力较大，当系统受到破坏后，可能给全行业范围的业务和管理工作带来较大影响或造成一定社会不良影响，可能侵害社会公共利益和公共秩序；

——内联网：运行在内联网上的信息系统，面向行业内部员工，社会影响力小，当系统受到破坏后，仅对行业内部的业务和管理工作带来影响，不会侵害社会公共利益和公共秩序。

d） 恢复时间目标

——系统在遭到破坏后恢复时间目标在 8 h 以上，对烟草行业业务影响较小且经济损失较少；

——系统在遭到破坏后恢复时间目标在 4 h～8 h 内，对烟草行业业务影响较大且造成损失较大；

——系统在遭到破坏后恢复时间目标在 4 h 内，对烟草行业业务影响大且造成损失严重。

5.2.3 确定保护等级

确定需要定级的信息系统后，应依据信息系统业务信息类型、系统服务范围、系统运行环境、恢复时间目标四个定级要素，参考以下原则确定安全保护等级。特别重要的信息系统视情参照GB/T 22240—2008 定为第四级或第五级。第一级至第三级信息系统应根据业务信息类型和系统服务范围初步确定信息系统安全保护等级，最终确定安全保护等级还应考虑系统运行环境和恢复时间目标。运行在互联网上的信息系统安全保护等级应按较高一级要求进行保护，恢复时间目标在 4 h 以内的信息系统安全保护等级应按较高一级要求进行保护。业务信息类型、系统服务范围与安全保护等级的关系如表 2

所示。

表 2　业务信息类型、系统服务范围与安全保护等级的关系

业务信息类型		系统服务范围		
		局部性	区域性	全局性
公开信息		第一级	第二级或第三级	第三级
专有信息	不含专卖管理、生产、营销等专有信息	第一级或第二级	第二级或第三级	第三级
	含专卖管理、生产、营销等专有信息	第二级	第二级或第三级	第三级
重要信息		第二级或第三级	第三级	第三级

——承载信息为公开信息、系统服务范围为局部性的信息系统应定为第一级；
——承载信息为公开信息、系统服务范围为区域性的信息系统应定为第二级或第三级；
——承载信息为公开信息、系统服务范围为全局性的信息系统应定为第三级；
——承载信息为不含专卖管理、生产、营销等专有信息、系统服务范围为局部性的信息系统应定为第一级或第二级；
——承载信息为不含专卖管理、生产、营销等专有信息、系统服务范围为区域性的信息系统应定为第二级或第三级；
——承载信息为不含专卖管理、生产、营销等专有信息、系统服务范围为全局性的信息系统应定为第三级；
——承载信息为含专卖管理、生产、营销等专有信息、系统服务范围为局部性的信息系统应定为第二级；
——承载信息为含专卖管理、生产、营销等专有信息、系统服务范围为区域性的信息系统应定为第二级或第三级；
——承载信息为含专卖管理、生产、营销等专有信息、系统服务范围为全局性的信息系统应定为第三级；
——承载信息为重要信息、系统服务范围为局部性的信息系统应定为第二级或第三级；
——承载信息为重要信息、系统服务范围为区域性的信息系统应定为第三级；
——承载信息为重要信息、系统服务范围为全局性的信息系统应定为第三级。

6　技术防护

6.1　支撑环境保护

6.1.1　机房环境保护

行业各单位机房环境应符合附录 A 中的第三级基本安全要求，参见附录 B 中的 B.1 进行建设、防护，包括但不限于以下内容：

——应对机房进行区域划分，安装电子门禁系统、防盗报警系统和视频监控系统；
——机房应配备 UPS，采用双路供电方式，并建立备用供电系统；
——应部署火灾自动消防系统；
——应部署机房环境监控系统，对空调、UPS、门禁系统等的运行状况以及机房供配电、漏水、温湿度、烟雾等情况进行实时监控，并提供报警功能；

——机房应配备机房专用空调；
——电源线和通信线缆应隔离铺设。

6.1.2 网络环境保护

行业各单位网络环境应符合附录 A 的第三级基本安全要求，参见 B.2 进行建设、防护，包括但不限于以下内容：

——应根据网络结构、业务需求和区域安全防护要求划分网络区域；
——应提供核心网络设备、通信链路的冗余；
——应配置 QoS(服务质量)或具有带宽/流量管理能力，对通信链路带宽进行优先级分配；
——应具有对入侵事件防护能力，在发生较严重入侵事件时应提供报警及防护；
——应具有病毒防护能力，对网络恶意代码进行检测和阻断，对防病毒软件进行统一管理、统一升级；
——应采用用户名、密码和行业数字证书相结合的方式，对登录网络设备的用户进行身份鉴别。

6.1.3 应用支撑环境保护

应用支撑环境应按照信息系统的安全保护等级进行建设、防护，符合附录 A 中相应级别的基本安全要求，同时还应参见 B.3 进行建设、防护，包括但不限于以下内容：

——应采用用户名/密码和行业数字证书相结合的方式，对登录服务器操作系统和数据库系统的用户进行身份鉴别；
——应提供服务器的冗余；
——应具有服务器防病毒能力；
——应对用户终端集中统一管理，统一安装防病毒软件、统一安装系统补丁等；
——应对移动存储介质进行统一管理，重要数据应存储在专用的移动存储介质中，并对重要数据进行保密性处理；
——应对移动终端接入网络系统进行控制。

6.2 应用软件安全

应用软件开发应按照信息系统的安全保护等级进行建设、防护，符合附录 A 中相应级别的基本安全要求。安全保护等级定为第二级(含)以上的信息系统还应参见 B.4、B.5 进行建设、防护，安全保护等级定为第三级(含)以上的信息系统还应包括但不限于以下内容：

——应采用用户名/密码和行业数字证书相结合的方式，对登录应用系统的用户进行身份鉴别；
——应提供身份鉴别、用户身份标识唯一、鉴别信息复杂度检查、用户登录失败处理、用户操作超时限制、并发会话连接数限制和数据有效性校验等功能；
——应提供访问控制功能，具有限制用户访问系统功能、业务信息等权限；
——应提供安全审计功能，对用户登录过程、操作行为等进行记录，并能对审计日志进行统计、分析，生成审计报表；
——应具有用户退出应用系统后及时擦除存储空间中身份鉴别信息、清除内存中临时文件的功能；
——应采用密码技术保证通信过程中数据的完整性和保密性；
——应具有在请求的情况下为数据原发者或接收者提供数据原发证据和接收证据的功能；
——应能够检测到系统管理数据、鉴别信息和重要业务数据在传输和存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；
——应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输和存储的保密性。

6.3 安全运维管控系统建设

为保障第三级(含)以上信息系统安全稳定运行,应建立安全运维管控系统,安全运维管控系统主要功能包括但不限于以下内容:

——能够监控到所属单位信息系统运行情况;

——具备运维安全审计功能,对运行维护人员操作权限进行管理和记录;

——具备内控管理功能,对用户行为、系统资源的异常使用、重要系统命令的使用等进行记录和分析;

——具备资源监控功能,对服务器的 CPU、内存、磁盘、网络等资源的使用情况和应用软件的服务能力进行实时监控;

——具备对审计日志进行查询、统计、分析和生成报表的功能;

——应明确运行监控预警指标,当超过预先规定的阈值后及时报警;

——应能收集网络安全事件信息,对病毒、攻击等信息安全事件进行报警和提供影响分析。

7 安全管理

7.1 安全责任

应明确信息系统的业务主管部门、运行部门和运维部门(单位)的安全责任,设立安全管理和运行维护岗位(包括但不限于应用管理员、系统管理员、安全管理员、安全审计员等),明确相应的岗位职责,并对相关人员定期进行安全技能、安全认知等培训和考核。

7.2 管理制度体系

要建立体系化的管理制度体系,包括但不限于以下内容:

——制定信息安全工作的总体方针和安全策略,明确信息安全工作的总体目标、范围、原则和安全框架等;

——制定信息安全管理制度,包括物理、网络、系统、应用、建设和管理工作等各层面的主要内容;

——制定安全检查管理制度,明确安全检查的内容、检查方式、检查要求等主要内容;

——建立日常操作手册,指导各级管理人员或操作人员执行日常管理操作;

——建立监督管理制度体系文件执行的检查机制。

7.3 系统建设管理

系统建设管理包括但不限于以下内容:

——根据信息系统业务需求、等级划分情况、现有安全保障措施和安全风险等确定安全要求,明确信息系统的安全保护策略,制定信息系统建设工作计划,形成信息系统安全方案,其中安全风险可参见附录 C 进行分析;

——信息安全产品和密码产品的采购和使用要符合国家有关主管部门的要求;

——制定软件源代码管理规则,建立软件开发管理流程;

——编制实施方案,对实施过程进行进度和质量控制;

——制定系统测试验收方案,第三级(含)以上信息系统上线前要委托第三方机构进行安全性测试;

——编制系统交付清单,明确开发商需提供软件开发设计相关的文档、软件源代码等。

7.4 系统运维管理

7.4.1 机房管理

机房管理包括但不限于以下内容：

——建立机房日常巡检及值守机制：工作日正常工作时间应有专人在机房值守，其他时间应采取对机房和信息系统的监控及报警措施，实时监控机房和信息系统运行情况；

——应对机房内设备、线缆进行标识管理。

7.4.2 日常管理

日常管理包括但不限于以下内容：

——建立安全运维流程，包括服务级别管理、问题管理、事件管理、变更管理、配置管理和发布管理等；

——制定日常检查规范，明确日常检查的检查内容、检查对象、检查步骤等内容；

——建立安全事件预警机制，定期分析系统运行记录，及时处理发生的安全事件；

——应对日常运维操作进行痕迹化管理。

7.4.3 备份管理

备份管理包括但不限于以下内容：

——应识别需要定期备份的重要业务信息、系统数据及软件系统等，制定备份计划列表；

——应建立控制数据备份和恢复过程的程序，定期执行恢复程序，检查和测试备份介质的有效性，确保可在恢复程序规定的时间内完成备份的恢复。

7.4.4 应急管理

7.4.4.1 事件管理

应按照 GB/Z 20986—2007 对信息安全事件进行分类、分级管理。信息安全事件分为六个类别，包括有害程序事件、网络攻击事件、信息破坏事件、信息内容事件、设备设施故障和灾害性事件。信息安全事件分为四个级别，包括特别重大事件、重大事件、较大事件和一般事件。

发生特别重大、重大、较大信息安全事件的单位，应立即报告上一级单位，由上一级单位报告国家局。发生一般信息安全事件的单位，应立即报告上一级单位信息化工作部门，每季度由省级单位信息化工作部门汇总后报告国家局。

——特别重大事件是指能够导致特别严重影响或破坏的信息安全事件，包括会使特别重要信息系统（如等级保护第四级和第五级系统）遭受特别严重的系统损失、或产生特别重大的社会影响等情况。

——重大事件是指能够导致严重影响或破坏的信息安全事件，包括会使特别重要信息系统遭受严重的系统损失、或使重要信息系统（如等级保护第三级系统）遭受特别严重的系统损失、或产生重大的社会影响等情况。

——较大事件是指能够导致较严重影响或破坏的信息安全事件，包括会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失、或使较重要信息系统（如等级保护第二级系统）遭受特别严重的系统损失、或产生较大的社会影响等情况。

——一般事件是指不满足以上条件的信息安全事件，包括会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失、或使较重要信息系统或者一般信息系统（如等级保护第一级系统）遭受严重或严重以下级别的系统损失、或产生一般的社会影响等情况。

7.4.4.2 预案编制

应编制机房环境、网络保障环境、应用支撑环境和应用软件等应急处置预案，建立相应的应急处置流程，实施应急处置要对处置过程进行全面记录，应包括但不限于事件的发生(或发现)时间、影响范围、处置措施、处置情况，以及报告情况等内容。

7.4.4.3 应急演练

应参照附录D的要求定期开展应急演练，对应急预案的有效性、处置流程的可执行性和应急保障资源的可用性进行验证，形成演练记录，及时对应急预案进行修订完善。应急演练主要包括但不限于以下内容：

——应急演练方案应包括演练场景、演练机构、演练职责、演练步骤、保障措施等；

——在应急演练前应组织进行培训，通过应急技能培训，使所有参加演练单位和人员掌握演练过程中涉及的相关设备的操作和使用技能；

——在演练结束后，应根据演练记录对演练效果与作用、演练组织与实施、演练人员表现以及演练过程中发现的问题和隐患进行分析总结，包括演练基本情况、发现的问题和隐患、取得的经验和教训、下一步整改措施和工作建议等。

7.5 系统终止管理

系统终止管理包括但不限于以下内容：

——当信息系统停止运行时，业务主管部门应向信息化工作部门提出下线申请，明确需转移、暂存和清除的业务信息情况；

——信息化工作部门受理下线申请后，应按照GB/T 25058—2010中9.2、9.3、9.4的要求，编制下线方案，包括信息资产、硬件设备、存储介质的处理方式和处理过程等；

——下线方案经主管领导批准后，信息化工作部门方可按照下线方案进行下线实施，详细记录下线处理过程，包括参与的人员、处理方式、残余信息检查结果等，形成系统下线报告；

——信息化工作部门应按照国家和行业有关规定，在信息系统下线后及时到公安机关办理备案撤销手续，并报上一级单位。

附 录 A
（规范性附录）
烟草行业信息系统安全等级保护基本要求

A.1 范围

本要求规定了烟草行业不同安全保护等级信息系统的安全要求，包括基本技术要求和基本管理要求，适用于烟草行业按照等级保护要求进行安全建设、测评和监督管理等工作。

A.2 烟草行业信息系统安全等级保护概述

A.2.1 基本技术要求和基本管理要求

基本安全要求是针对不同安全保护等级信息系统应该具有的基本安全保护能力提出的安全要求，根据实现方式的不同，基本安全要求分为基本技术要求和基本管理要求两大类。技术类安全要求与信息系统提供的技术安全机制有关，主要通过在信息系统中部署软硬件并正确地配置其安全功能来实现；管理类安全要求与信息系统中各种角色参与的活动有关，主要通过控制各种角色的活动，从制度、规范、流程以及记录等方面做出规定来实现。

基本技术要求从物理安全、网络安全、主机安全、应用安全和数据安全几个层面提出；基本管理要求从安全管理制度、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几个方面提出，基本技术要求和基本管理要求是确保信息系统安全不可分割的两个部分。

基本安全要求从各个层面或方面提出了系统的每个部分应该满足的安全要求，信息系统具有的整体安全保护能力通过不同组件实现基本安全要求来保证。除了保证系统的每个组件满足基本安全要求外，还要考虑组件之间的相互关系，来保证信息系统的整体安全保护能力。

对于涉及国家秘密的信息系统，应按照国家保密工作部门的相关规定和标准进行保护。对于涉及密码的使用和管理，应按照国家密码管理的相关规定和标准实施。

A.2.2 基本技术要求的三种类型

根据保护侧重点的不同，技术类安全要求进一步细分为：保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改的信息安全类要求（简记为 S）；保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用的服务保证类要求（简记为 A）；通用安全保护类要求（简记为 G）。本要求中对基本安全要求使用了标记，其中的字母表示安全要求的类型，数字表示适用的安全保护等级。

A.2.3 烟草行业信息系统安全要求的选择和使用

信息系统定级后，不同安全保护等级的信息系统可能形成的定级结果组合见表 A.1。

表 A.1 各等级信息系统定级结果组合

安全保护等级	信息系统定级结果的组合
第一级	S1A1G1
第二级	S1A2G2,S2A2G2,S2A1G2
第三级	S1A3G3,S2A3G3,S3A3G3,S3A2G3,S3A1G3

对于确定了安全保护等级的信息系统,选择和使用基本安全要求时,可以按照以下过程进行:

a) 明确信息系统应该具有的安全保护能力,根据信息系统的安全保护等级选择基本安全要求,包括技术要求和管理要求。简单的方法是根据本要求,一级系统选择第一级基本安全要求,二级系统选择第二级基本安全要求,三级系统选择第三级基本安全要求,以此作为出发点。

b) 根据信息系统的定级结果对基本安全要求进行调整。根据系统服务保证性等级选择相应等级的系统服务保证类(A 类)基本安全要求;根据业务信息安全性等级选择相应等级的业务信息安全类(S 类)基本安全要求。

c) 针对烟草行业不同系统的特点,分析可能在某些方面的特殊安全保护能力要求,选择较高级别的基本安全要求或补充基本安全要求。对于本要求中提出的基本安全要求无法实现或有更加有效的安全措施可以替代的,可以对基本安全要求进行调整,调整的原则是保证不降低整体安全保护能力。

保证不同安全保护等级的信息系统具有相应级别的安全保护能力,满足相应级别的基本安全要求,是信息系统等级保护的核心。选用本要求中提供的基本安全要求是保证信息系统具备一定安全保护能力的一种途径和出发点,在此基础上,可以参考等级保护的其他相关标准和安全方面的其他相关标准,调整和补充基本安全要求,从而实现信息系统在满足等级保护基本要求基础上,又具有自身特点的保护。

A.3 第一级基本要求

A.3.1 技术要求

A.3.1.1 物理安全

A.3.1.1.1 物理访问控制(G1)

机房出入应安排专人负责,控制、鉴别和记录进入的人员:

a) 应对人员进出机房进行管理,采取有效的保护措施;

b) 应安排专人对人员进出机房进行管理,保存人员进出机房的登记记录。

A.3.1.1.2 防盗窃和防破坏(G1)

本项要求包括:

a) 应将主要设备放置在机房内:设备应放置在机房内或其他不易被盗窃和破坏的可控范围内。

b) 应将设备或主要部件进行固定,并设置明显的不易除去的标记:

1) 设备或主要部件应当安装、固定在机柜内或机架上;

2) 设备或主要部件应贴有明显且不易除去的标识,如粘贴标签或铭牌等。

A.3.1.1.3 防雷击(G1)

机房建筑应设置避雷装置:

a) 机房或机房所在大楼应安装避雷装置，如避雷针或避雷器等；
b) 应具有经国家有关部门验收或检测合格的相关证明文件。

A.3.1.1.4 防火(G1)

本项要求包括：

a) 机房应设置灭火设备：
   1) 应制定机房消防应急预案，对相关人员进行消防培训；
   2) 机房应按照 GB 50174—2008 中 A 级机房的消防要求配备灭火设备，摆放位置合理。
b) 机房内装修材料应采用难燃材料和不燃材料：机房内的装修材料应满足 GB 50222—1995(2001 年修订版)规定的难燃材料和不燃材料的要求。

A.3.1.1.5 防水和防潮(G1)

本项要求包括：

a) 应对穿过机房墙壁和楼板的水管增加必要的保护措施：水管安装，尽量避免穿过屋顶和活动地板，穿过墙壁和楼板的水管应使用套管，并采取可靠的密封措施。
b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透：
   1) 机房外墙壁若有对外的窗户，应对窗户进行密封、防水处理；
   2) 应对机房屋顶、地面和墙壁进行防水处理，防止出现漏水、渗透和返潮现象；
   3) 应对机房屋顶进行保温处理，防止产生冷凝水。

A.3.1.1.6 温湿度控制(G1)

机房应设置必要的温、湿度控制设施，使机房温、湿度的变化在设备运行所允许的范围之内：机房应配备温湿度自动调节设施，对机房温湿度进行控制，满足 GB 50174—2008 中的“环境要求”A 级技术要求。

A.3.1.1.7 电力供应(A1)

应在机房供电线路上配置稳压器和过电压防护设备：计算机系统供电线路上应设置稳压器和过电压防护设备(如 UPS)，有效控制电源稳压范围满足计算机系统正常运行。

A.3.1.2 网络安全

A.3.1.2.1 结构安全(G1)

本项要求包括：

a) 应保证关键网络设备的业务处理能力满足基本业务需要：
   1) 应保证关键网络设备的 CPU 使用率满足业务处理能力的需要；
   2) 应使用监控系统监控关键网络设备的运行状态。
b) 应保证接入网络和核心网络的带宽满足基本业务需要：应保证主要网络设备接口带宽配置满足基本业务访问需要。
c) 应绘制与当前运行情况相符的网络拓扑结构图：
   1) 应绘制完整的网络拓扑结构图，包含相应的网络配置表、设备 IP 地址等主要信息并与当前运行情况相符且及时更新；
   2) 拓扑结构图应明确网络拓扑区域的划分。

A.3.1.2.2 访问控制(G1)

本项要求包括：

a) 应在网络边界部署访问控制设备，启用访问控制功能：
   1) 应在网络边界处部署防火墙并配置访问控制列表；
   2) 若网络边界处未部署防火墙或其他安全访问控制设备，则应启用路由器或交换机的访问控制功能。
b) 应根据访问控制列表对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包出入；网络边界访问控制设备应设定过滤规则集，规则集应涵盖对所有出入边界的数据包的处理方式，对于没有明确定义的数据包，应缺省拒绝。
c) 应通过访问控制列表对系统资源实现允许或拒绝用户访问，控制粒度至少为用户组；应在防火墙或其他设备上设置用户或用户组，结合访问控制规则实现用户认证功能。

A.3.1.2.3 网络设备防护(G1)

本项要求包括：

a) 应对登录网络设备的用户进行身份鉴别：
   1) 应设置设备的登录口令；
   2) 应删除默认用户或修改默认用户的口令，根据管理需要开设用户；不得使用缺省口令、空口令、弱口令。
b) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；应设置非法登录次数为 3 次，登录连接超时时间为 8 min。
c) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；应采用 ssh、https 等加密协议方式对设备进行交互式管理。

A.3.1.3 主机安全

A.3.1.3.1 身份鉴别(S1)

应对登录操作系统和数据库系统的用户进行身份标识和鉴别；登录用户的身份标识应采用用户名，鉴别方式采用口令。

A.3.1.3.2 访问控制(S1)

本项要求包括：

a) 应启用访问控制功能，依据安全策略控制用户对资源的访问：
   1) 服务器系统应根据安全策略限制用户访问文件的权限及关闭默认共享；
   2) 数据库系统应限制主体(如用户)对客体(如文件或系统设备、数据库表等)的操作权限(如读、写或执行)。
b) 应限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令：
   1) 应重命名 Windows 系统已有默认账号 administrator；
   2) 系统无法修改访问权限的特殊默认账户，可不修改访问权限；
   3) 系统无法重命名的特殊默认账户，可不重命名。
c) 应及时删除多余的、过期的账户，避免共享账户的存在：
   1) 应删除系统多余和过期的账户，如 GUEST；
   2) 不允许多人共用一个相同的账户。

A.3.1.3.3 入侵防范(G1)

操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并保持系统补丁及时得到更新：

a) 应关闭系统多余和危险的服务；

b) 应持续跟踪厂商提供的系统升级更新情况，应在经过充分的测试评估后对必要补丁进行及时更新。

A.3.1.3.4 恶意代码防范(G1)

应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库：

a) 主机应安装防恶意代码软件并及时更新恶意代码库；

b) 未安装防恶意代码软件的主机，应采用网络防恶意代码防范措施；

c) 应制定统一的病毒管理策略，进行软件的统一更新、恶意代码的定时查杀等。

A.3.1.4 应用安全

A.3.1.4.1 身份鉴别(S1)

本项要求包括：

a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别，应用系统应具有专用的登录控制模块对登录用户的用户名/密码进行核实。

b) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施：

1) 应用系统应限制用户的非法登录次数不超过3次；

2) 登录失败超过5次的账户将被锁定，由系统管理员解锁；

3) 应设置应用系统连接超时时间，超时需重新登录连接。

c) 应启用身份鉴别和登录失败处理功能，并根据安全策略配置相关参数：应用系统应保证身份鉴别、鉴别信息复杂度以及登录失败处理功能的开启，并根据a)、b)、c)相关要求配置参数。

A.3.1.4.2 访问控制(S1)

本项要求包括：

a) 应提供访问控制功能控制用户组/用户对系统功能和用户数据的访问，应用系统应根据安全策略限制用户对系统功能和用户数据的访问。

b) 应由授权主体配置访问控制策略，并严格限制默认用户的访问权限：

1) 访问控制列表的授权与控制应有专人进行管理；

2) 应用系统应重命名正在使用的默认账户，如admin等；

3) 应用系统应及时删除不被使用的账户，一般指应用系统的公共账户或测试账户。

A.3.1.4.3 通信完整性(S1)

应采用约定通信会话方式的方法保证通信过程中数据的完整性：应用系统中通信双方应利用约定通信会话方式保证数据完整性。

A.3.1.4.4 软件容错(A1)

应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求：应用系统应对输入数据进行有效性校验(如：数据格式、数据长度、空否等)。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。

A.3.1.5 数据安全及备份恢复

A.3.1.5.1 数据完整性(S1)

应能够检测到重要用户数据在传输过程中完整性受到破坏;应具有对重要用户数据在传输过程中的完整性进行检测的功能。

A.3.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复:对关键主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件在变更前后进行备份,至少每周对关键数据库和应用系统重要信息进行备份,备份介质场外存放。

A.3.2 管理要求

A.3.2.1 安全管理制度

A.3.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度:应从物理、网络、主机、数据、应用、建设和管理等层面分别建立安全管理制度。

A.3.2.1.2 制定和发布(G1)

本项要求包括:

a) 应指定或授权专门的人员负责安全管理制度的制定;
b) 应将安全管理制度以某种方式发布到相关人员手中:应明确安全管理制度的发布方式,并按此要求将安全管理制度发布到相关人员手中。

A.3.2.2 安全管理机构

A.3.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责:

a) 信息化工作部门应至少设立系统管理员、网络管理员、信息安全管理员岗位;
b) 各单位内设部门应设立信息安全员岗位,负责本部门各项安全措施的落实;
c) 应制定信息安全组织机构和岗位职责文件,明确上述涉及的各个岗位的职责。

A.3.2.2.2 人员配备(G1)

应配备一定数量的系统管理员、网络管理员、安全管理员等:

a) 应按照 A.3.2.2.1 的岗位设置要求,结合实际情况,对各个岗位配备足够的人员;
b) 应针对各个信息系统建立系统管理员、数据库管理员、网络管理员、信息安全管理员等安全管理岗位人员的信息表。

A.3.2.2.3 授权和审批(G1)

应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批:

a) 应明确需审批的关键活动,并授权审批部门及批准人对关键活动进行审批;
b) 关键活动至少包括系统上线、网络接入、重要资源访问、系统变更、外部人员访问、信息发布等。