水利网络与信息安全体系建设
基本技术要求

（送审稿）

水利部信息化工作领导小组办公室

二零一零年三月

目录

1 目的与范围

1.1 目的

水利信息化发展快速，信息化基础设施及业务应用逐步建设并完善，与此同时，网络与信息安全体系也逐步建立和发展。但与日益增加的业务应用对安全的需求相比，水利行业网络与信息安全系统尚缺乏统一的规划、安排、组织和实施，现有的安全应用还比较单一，缺乏系统性和整体性，存在较大安全风险，远不能达到国家对信息系统安全防护的相关要求，如不及时解决将严重影响水利信息化的进一步发展。

《中华人民共和国计算机信息系统安全防护条例》(国务院令第147号）明确规定我国“计算机信息系统实行安全等级保护”。依据国务院147号令的要求而制订发布的强制性国家标准《计算机信息系统安全防护等级划分准则》(GB17859-1999）为计算机信息系统安全防护等级的划分奠定了技术基础。《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号）明确指出实行信息安全等级保护，“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度”。《关于信息安全等级保护工作的实施意见》(公通字[2004]66号）和《信息安全等级保护管理办法》(公通字[2007]43号）确定了实施信息安全等级保护制度的原则、工作职责划分、实施要求和实

施计划，明确了开展信息安全等级保护工作的基本内容、工作流程、工作方法等。信息安全等级保护相关法规、政策文件、国家标准和公共安全行业标准的出台，为网络与信息安全体系的建设提供了法律、政策、标准依据。《关于开展信息安全等级保护安全建设整改工作的指导意见》(公信安[2009]1429号)明确要求各部门在信息安全等级保护定级工作基础上，力争在2012年底前完成已定级信息系统(不包括涉及国家秘密信息系统)安全建设整改工作。水利部于2007年9月初组织开展了水利行业信息系统安全等级保护定级工作，目前定级工作已基本完成，这为水利行业网络与信息安全体系建设奠定了基础。

本标准编制的目的是依据国家信息系统等级保护相关标准及其他信息安全标准规范，结合水利信息化实际情况，对水利网络与信息安全体系的框架结构、安全要素基本要求等进行规范，指导水利行业各单位、各部门在信息安全等级保护定级和备案工作基础上，开展信息系统安全规划、整改及建设工作，落实安全防护技术措施，建立健全安全管理制度，进一步提高水利网络与信息系统的安全保障能力和防护水平，确保各单位、部门网络与信息系统的安全运行，推进水利信息化的安全、健康、协调发展。

1.2 范围

本技术要求适用于水利行业各单位，用于指导各单位政务外网（水利专网）的网络与信息安全体系规划、设计、建设和整改，及

各单位政务外网信息系统的安全设计、建设，保障信息系统的安全运行，也可作为水利行业信息安全职能部门进行监督、检查和指导的依据。各单位政务内网的网络与信息安全系统建设应遵循国家有关职能部门及水利部的相关规定。

1.3 规范性引用文件

1) GB 17859-1999《计算机信息系统安全防护等级划分准则》

2) 国务院令第 147 号 《中华人民共和国计算机信息系统安全防护条例》

3) 中办发[2003]27 号《国家信息化领导小组关于加强信息安全保障工作的意见》

4) 公通字【2004】66 号 关于印发《关于信息安全等级保护工作的实施意见》的通知

5) 公通字【2007】43 号 信息安全等级保护管理办法

6) 《信息安全技术　信息系统等级保护安全设计技术要求》（GB/T24856-2009）

7) 《信息安全技术　信息系统安全等级保护基本要求》（GB/T22239-2008）

1.4 术语、定义和缩略语

1) 定级系统安全保护环境　security environment of classified system

由安全计算环境、安全区域边界、安全通信网络和（或）安全管理中心构成的对定级系统进行安全保护的环境。

定级系统安全保护环境包括第一级系统安全保护环境、第二级系统安全保护环境、第三级系统安全保护环境、第四级系统安全保护环境、第五级系统安全保护环境以及定级系统的安全互联。

2) 安全计算环境 secure computing environment

对定级系统的信息进行存储、处理及实施安全策略的相关部件。

安全计算环境按照保护能力划分为第一级安全计算环境、第二级安全计算环境、第三级安全计算环境、第四级安全计算环境和第五级安全计算环境。

3) 安全区域边界 secure area boundary

对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。

安全区域边界按照保护能力划分为第一级安全区域边界、第二级安全区域边界、第三级安全区域边界、第四级安全区域边界和第五级安全区域边界。

4) 安全通信网络 secure communication network

对定级系统安全计算环境之间进行信息传输及实施安全策略的相关部件。

安全通信网络按照保护能力划分第一级安全通信网络、第二级安全通信网络、第三级安全通信网络、第四级安全通信网络和第五级安全通信网络。

5) 安全管理中心　security management center

对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台。

第二级及第二级以上的定级系统安全保护环境需要设置安全管理中心，称为第二级安全管理中心、第三级安全管理中心、第四级安全管理中心和第五级安全管理中心。

6) 系统安全互联　secure system interconnection

通过安全互联部件和跨定级系统安全管理中心实现的相同或不同等级的定级系统安全保护环境之间的安全连接。

2 总体建设要求

2.1 总体要求

本技术要求只是对网络与信息安全体系的框架和基本技术要求进行约定，而不是网络与信息安全体系建设的方案，各单位在网络与信息安全系统建设时，应依据本技术要求，结合各自实际情况，进行网络与信息安全系统规划、设计及建设。

本技术要求主要是对水利信息系统中已定级为第二级、第三级、第四级的信息系统的安全防护建设提出基本技术要求，对于定级为第一级或五级的信息系统的安全防护由各建设、管理单位参照等级保护的要求进行建设。

水利网络与信息系统安全体系建设，需要遵循以下总体要求:

1) 遵循等级保护的相关标准和规范的要求;

2) 按照本技术要求进行设计，保证系统结构完整，安全要素全面覆盖;

3) 网络与信息安全体系建设是一个逐步完善的过程，各单位应依据本技术要求进行统一规划，在建设时可以根据信息化的发展逐步建设与完善，首先保证重要信息系统的安全;

4) 本要求为基本要求，各单位在安全体系建设时，可根据具体信息系统的特点，适当调整部分安全要素要求;

5) 在保证关键技术实现的前提下，尽可能采用成熟产品，保证系

统的可用性、工程实施的简便快捷。

各单位在新建应用系统或对已有应用升级改造时,可参照第5章应用安全建设要求有关内容完善应用安全。

2.2 基本框架

依据信息系统安全等级保护基本要求及水利网络与信息系统状况，将水利行业网络与信息安全体系依据涉及的业务范围划分为政务外网、政务内网;依据单位的级别划分为部级节点、省、流域级节点、市级节点、县级节点。水利网络与信息安全体系框架结构如图2-1所示:

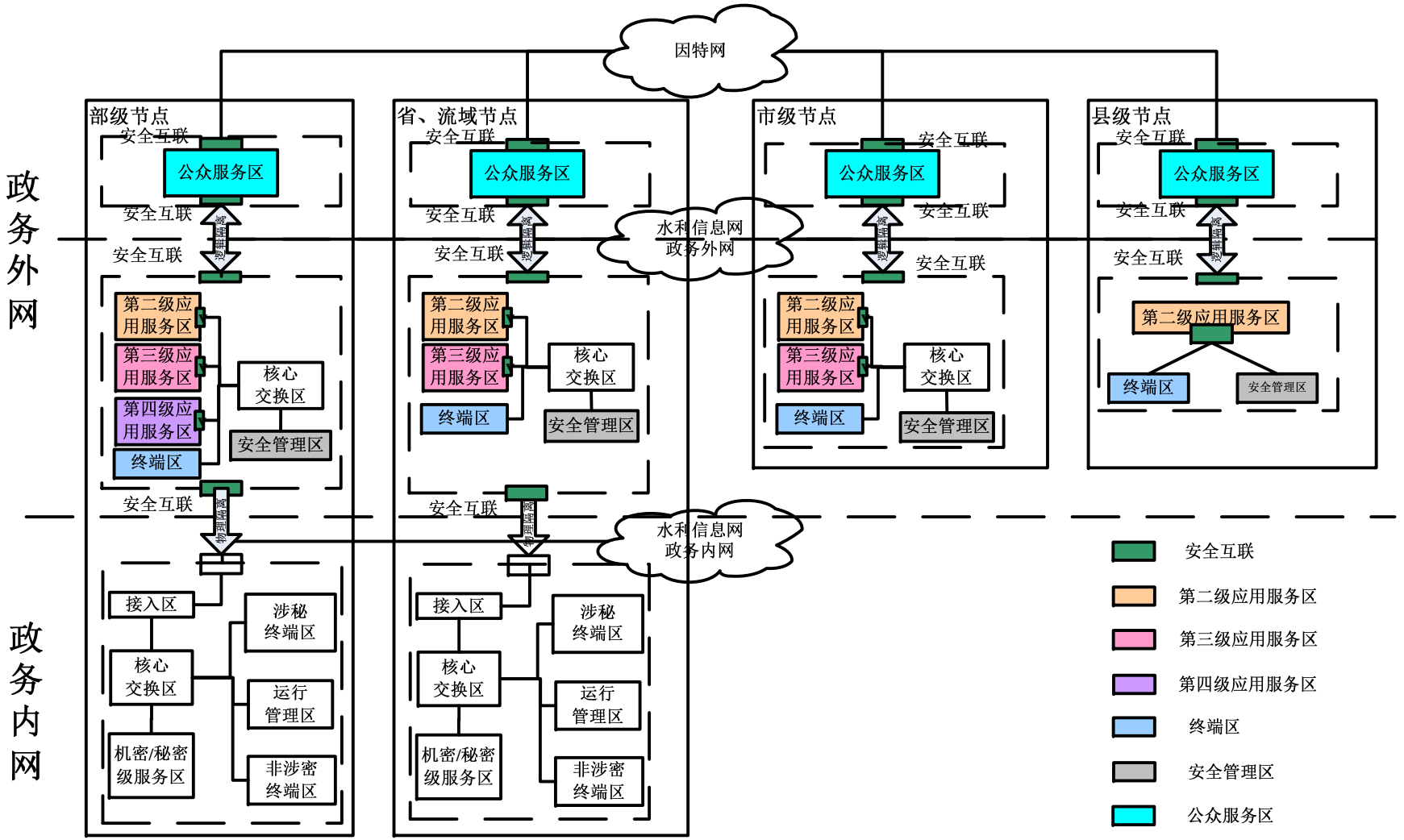

图 2-1 水利网络与信息安全体系框架结构图

水利行业信息系统分布于政务外网和政务内网两个物理隔离的网络，其中政务外网分公众服务区和业务服务区两部分。各级节点的政务外网公众服务区通过因特网互联，各级节点的政务外网业务服务区通过水利信息网政务外网互联，各级节点的政务内网通过水利信息网政务内网互联，采用安全互联设备进行安全防护。各节点的政务外网和政务内网网络与信息安全措施相对独立，在政务外网的互联区域达到等级保护第三级系统的安全防护要求时，在经过有关部门审批同意的情况下，可采用单向导入设备实现从政务外网到政务内网的单向信息导入；各节点的政务外网公众服务区和业务服务区采用统一的安全防护错措施，两个区域通过安全边界依据安全策略实现安全互联。各单位可根据需要建设控制调度网，实现重要水库、枢纽、灌区、供水、排水、调水等水利工程设施的调度，控制调度网宜与政务外网、政务内网物理隔离。

各信息系统根据定级情况，纳入相应等级的应用服务区，各级应用服务区提供一个相应等级的系统安全保护环境，保护信息系统安全，如图 2-2 所示。其中不同等级应用服务区可共用安全通信网络，该安全通信网络将按最高等级安全服务区安全通信网络要求建设。

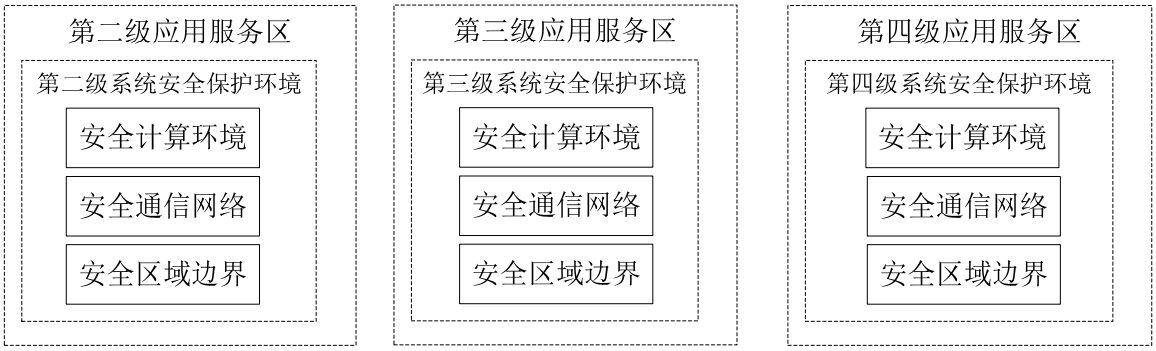

图 2-2 应用服务区结构图

本技术要求以下部分仅针对政务外网网络与信息安全体系，政务内网的安全体系遵循国家有关标准规范及水利部的有关要求。

2.3 信息系统安全定级

水利行业各单位在进行网络与信息安全体系规划、建设时，首先应进行信息系统的梳理和安全定级工作，根据安全定级将信息系统划入相应等级的安全保护区，多个信息系统可以放入同一安全保护区。水利行业主要信息系统的安全定级可参考如下规则：

1) “防汛抗旱指挥系统”可划分成“骨干网系统”、“数据库系统”和“应用系统（可根据实际应用情况再进行划分）”，三个系统的流域级、省级分支系统的安全保护等级应定为三级；三个系统的地市级及以下单位的分支系统的安全保护等级可定为二级。

2) “防汛抗旱异地会商视频会议系统”、“实时水情交换与查询系统”的流域级、省级分支系统的安全保护等级应定为三级；地市级及以下单位的分支系统的安全保护等级可定为二级。

3) 城市水资源实时监控与管理信息系统的安全保护等级可定为二级或以上。

4) “全国水土保持监测网络和信息系统”在系统结构上是一套全国联网、数据集中的信息系统，“全国水土保持监测网络信息系统”分支系统的安全保护等级可定为二级。

5) 重要水库、枢纽、灌区、供水、排水、调水等水利工程设施的调度和运行信息系统的安全保护等级应定为三级。

6) 流域级、省级单位“政府网站信息系统”的安全保护等级可定为二级。

7) 各单位内部局域网、日常办公等信息系统的安全保护等级可定为二级。

8) 其他信息系统可结合实际情况、按照相关规定进行定级。

3 节点建设要求

3.1 部机关安全系统建设要求

依据 GB 17859-1999《计算机信息系统安全防护等级划分准则》以及《信息安全技术　信息系统等级保护安全设计技术要求》等信息安全标准规范，水利部信息系统定级情况及水利部网络与信息系统状况，将水利部政务外网网络与信息系统划分为 7 个安全保护区和 1 个物理安全环境，7 个安全保护区分别为：第二级应用服务区、第三级应用服务区、第四级应用服务区、终端区、安全管理区、核心交换区、公众服务区，其中各安全保护区可以通过安全互联部件互联。水利部网络与信息安全系统结构如图 3-1 所示。

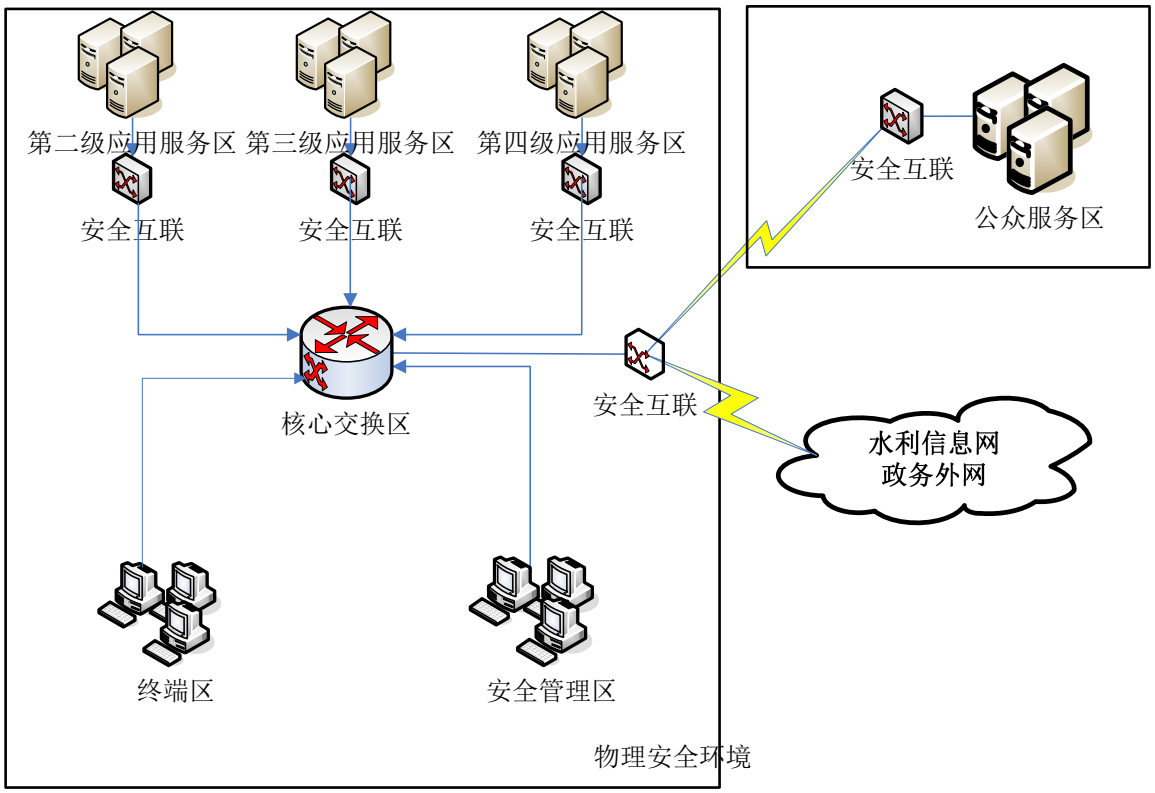

图 3-1 水利部网络与信息安全系统结构图

1) 第二级应用服务区：第二级应用服务区用于部署定级为第二级的信息系统，对这些信息系统提供统一的安全防护措施，并通过安全互联和核心交换区与其他区域和其他单位的信息系统进行数据交换。在第二级应用服务区内的不同第二级信息系统可以根据需要采用安全措施进行隔离。根据网络结构可以部署多个第二级应用服务区，每个第二级应用服务区保护一个或多个第二级信息系统。在第二级应用服务区需按以下安全防护要求建设：

- 用户身份鉴别。应支持用户标识和用户鉴别。在对每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录系统时，采用受控的口令或具有相应安全强度的其他机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护。
- 自主访问控制。应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户。访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。访问操作包括对客体的创建、读、写、修改和删除等。
- 系统安全审计。应提供安全审计机制，记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。该机制应提供审计记录查询、分类和存储保护，并可由安全管理中心管理。
- 用户数据完整性保护。可采用常规校验机制，检验存储的用户数据的完整性，以发现其完整性是否被破坏。
- 用户数据保密性保护。可采用密码等技术支持的保密性保护机制，对在安全计算环境中存储和处理的用户数据进行保密性保

护。

- 客体安全重用。应对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。
- 恶意代码防范。应安装防恶意代码软件或配置具有相应安全功能的操作系统，并定期进行升级和更新，以防范和清除恶意代码。
- 备份与恢复。应能对重要信息进行备份与恢复。
- 区域边界协议过滤。应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议和请求的服务等，确定是否允许该数据包通过该区域边界。
- 区域边界安全审计。应在安全区域边界设置审计机制，并由安全管理中心统一管理。
- 区域边界恶意代码防范。应在安全区域边界设置防恶意代码网关，由安全管理中心管理。
- 区域边界完整性保护。应在区域边界设置探测器，探测非法外联等行为，并及时报告安全管理中心。
- 通信网络安全审计。应在安全通信网络设置审计机制，由安全管理中心管理。
- 通信网络数据传输完整性保护。可采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护。
- 通信网络数据传输保密性保护。可采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。

2) 第三级应用服务区：第三级应用服务区用于部署定级为第三级的信息系统，对这些系统提供安全防护，并通过安全互联和核心交换

区与其他区域和其他单位信息系统进行数据交换。为了降低系统复杂度也可以将第二级的信息系统纳入第三级应用服务区，按第三级信息系统防护。在第三级应用服务区内的不同信息系统可以根据需要采用安全措施进行隔离。根据网络结构可以部署多个第三级应用服务区，每个第三级应用服务区保护一个或多个第三级信息系统。在第三级应用服务区至少需要落实以下安全技术要求:

- 用户身份鉴别。应支持用户标识和用户鉴别。在对每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录系统时，采用受安全管理中心控制的口令、令牌、基于生物特征、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护。
- 自主访问控制。应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户。自主访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级和（或）记录或字段级。自主访问操作包括对客体的创建、读、写、修改和删除等。
- 标记和强制访问控制。在对安全管理员进行身份鉴别和权限控制的基础上，应由安全管理员通过特定操作界面对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制。强制访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。应确保安全计算环境内的所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。

- 系统安全审计。应记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。应提供审计记录查询、分类、分析和存储保护；能对特定安全事件进行报警；确保审计记录不被破坏或非授权访问。应为安全管理中心提供接口；对不能由系统独立处理的安全事件，提供由授权主体调用的接口。
- 用户数据完整性保护。应采用密码等技术支持的完整性校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。
- 用户数据保密性保护。采用密码等技术支持的保密性保护机制，对在安全计算环境中存储和处理的用户数据进行保密性保护。
- 客体安全重用。应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。
- 程序可信执行保护。可采用可信计算等技术构建从操作系统到上层应用的信任链，以实现系统运行过程中可执行程序的完整性检验，防范恶意代码等攻击，并在检测到其完整性受到破坏时采取措施恢复。
- 备份与恢复。应能对重要信息进行本地备份与恢复，备份数据可通过网络定时传送到备用场地。
- 区域边界访问控制。应在安全区域边界设置自主和强制访问控制机制，实施相应的访问控制策略，对进出安全区域边界的数据信息进行控制，阻止非授权访问。

- 区域边界协议过滤。应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出该区域边界。
- 区域边界安全审计。应在安全区域边界设置审计机制，由安全管理中心集中管理，并对确认的违规行为及时报警。
- 区域边界恶意代码防范。应在安全区域边界设置防恶意代码网关，由安全管理中心管理。
- 区域边界完整性保护。应在区域边界设置探测器，例如外接探测软件，探测非法外联和入侵行为，并及时报告安全管理中心。
- 通信网络安全审计。应在安全通信网络设置审计机制，由安全管理中心集中管理，并对确认的违规行为进行报警。
- 通信网络数据传输完整性保护。应采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护，并在发现完整性被破坏时进行恢复。
- 通信网络数据传输保密性保护。应采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。
- 通信网络可信接入保护。可采用由密码等技术支持的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，确保接入通信网络的设备真实可信，防止设备的非法接入。

3) 第四级应用服务区域：第四级应用服务区用于部署定级为第四级的信息系统，对这些系统提供安全防护，并通过安全互联和核心交换区与其他区域和其他单位信息系统进行数据交换。在第四级应用服务区内的不同第四级信息系统可以根据需要采用安全措施进行隔离。根据网络结构可以部署多个第四级应用服务区，每个第四级应用服务区保护一个或多个第四级信息系统。在第四级应用服务区至少需要落

实以下安全技术要求:

- 用户身份鉴别。应支持用户标识和用户鉴别。在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录和重新连接系统时，采用受安全管理中心控制的口令、基于生物特征的数据、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，且其中一种鉴别技术产生的鉴别数据是不可替代的，并对鉴别数据进行保密性和完整性保护。
- 自主访问控制。应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限部分或全部授予其他用户。自主访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级和（或）记录或字段级。自主访问操作包括对客体的创建、读、写、修改和删除等。
- 标记和强制访问控制。在对安全管理员进行身份鉴别和权限控制的基础上，应由安全管理员通过特定操作界面对主、客体进行安全标记，将强制访问控制扩展到所有主体与客体；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制。强制访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。应确保安全计算环境内的所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。
- 系统安全审计。应记录系统相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。应提供审计记录查询、分类、分析和存储保护；能对特定安全事件进行报警，终止违例进程等；确保审计记录不被破坏或非授权访问以及防

止审计记录丢失等。应为安全管理中心提供接口；对不能由系统独立处理的安全事件，提供由授权主体调用的接口。

- 用户数据完整性保护。应采用密码等技术支持的完整性校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。
- 用户数据保密性保护。采用密码等技术支持的保密性保护机制，对在安全计算环境中的用户数据进行保密性保护。
- 客体安全重用。应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。
- 程序可信执行保护。应采用可信计算或其他技术构建从操作系统到上层应用的信任链，以实现系统运行过程中可执行程序的完整性检验，防范恶意代码等攻击，并在检测到其完整性受到破坏时采取措施恢复。
- 恶意代码防范。应安装防恶意代码软件或配置具有相应安全功能的操作系统，并定期进行升级和更新，以防范和清除恶意代码。
- 备份与恢复。应能对重要信息进行本地备份与恢复；应建立异地灾难备份中心，提供业务应用的实时无缝切换；备份数据可通过网络实时传送到备用场地。
- 区域边界访问控制。应在安全区域边界设置自主和强制访问控制机制，实施相应的访问控制策略，对进出安全区域边界的数据信息进行控制，阻止非授权访问。
- 区域边界协议过滤。应根据区域边界安全控制策略，通过检查

数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出受保护的区域边界。

- 区域边界安全审计。应在安全区域边界设置审计机制，通过安全管理中心集中管理，对确认的违规行为及时报警并做出相应处置。
- 区域边界恶意代码防范。应在安全区域边界设置防恶意代码网关，由安全管理中心管理。
- 区域边界完整性保护。应在区域边界设置探测器，例如外接探测软件，探测非法外联和入侵行为，并及时报告安全管理中心。
- 通信网络安全审计。应在安全通信网络设置审计机制，由安全管理中心集中管理，并对确认的违规行为进行报警，且做出相应处置。
- 通信网络数据传输完整性保护。应采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护，并在发现完整性被破坏时进行恢复。
- 通信网络数据传输保密性保护。应采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。
- 通信网络可信接入保护。应采用由密码等技术支持的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，确保接入通信网络的设备真实可信，防止设备的非法接入。

4) 终端区：终端区是各部门办公人员终端计算机部署的区域。依据终端区计算机设备使用目标的不同，终端区的计算机设备可以分为两类（1）管理终端：办公人员需要使用此类终端进行应用系统进行配置、管理。（2）普通终端：办公人员需要使用此类终端进行登录应用系统处理业务。管理终端纳入相应信息系统应用服务区进行安全保

护，普通终端纳入终端区进行安全防护。依据各工作人员工作职责的不同，使用的终端可能需要同时访问多个级别信息系统，每个终端按照访问的最高级别的系统，实施相应的安全防护措施，不同防护等级的终端应进行逻辑隔离。

5) 核心交换区：核心交换区主要实现各区域之间的数据交换，本身不提供安全防护能力，配合安全互联提供各区域之间的访问控制。

6) 安全管理区：建立集中的安全管理中心，实现统一的安全策略管理、资源管理及安全审计。

7) 公众服务区：公众服务区主要部署为公众服务的信息系统，水利部公众服务区含第二级信息系统和第三级信息系统，按照最高级别防护采取第三级应用服务区的防护措施。

8) 物理安全环境：物理安全环境主要是为网络与信息系统提供机房、电力环境保障以及设备、设施、介质的防盗、防破坏等防护。根据网络与信息系统的位置不同，每个节点物理安全环境可以分为多个部分，每部分按照该环境内承载的信息系统的最高安全等级来确定防护级别。

安全互联要求：应对节点内不同安全保护区之间及节点之间的信息系统互联、互通及互操作进行安全保护。

3.2 省、流域级节点安全系统建设要求

依据 GB 17859-1999《计算机信息系统安全防护等级划分准则》以及《信息安全技术　信息系统等级保护安全设计技术要求》等信息安全标准规范，各省、流域机构信息系统定级情况及网络与信息系统状况，将省、流域机构政务外网网络与信息系统划分为 6 个安全保护区和 1 个物理安全环境，6 个安全保护区分别为：第二级应用服务区、

第三级应用服务区、终端区、安全管理区、核心交换区、公众服务区。省、流域机构网络与信息安全系统结构如图 3-2 所示。

根据各单位的实际需求，在省、流域级节点新建第四级的信息系统时可以参照部机关安全系统建设要求中第四级应用服务区的要求进行安全系统建设。

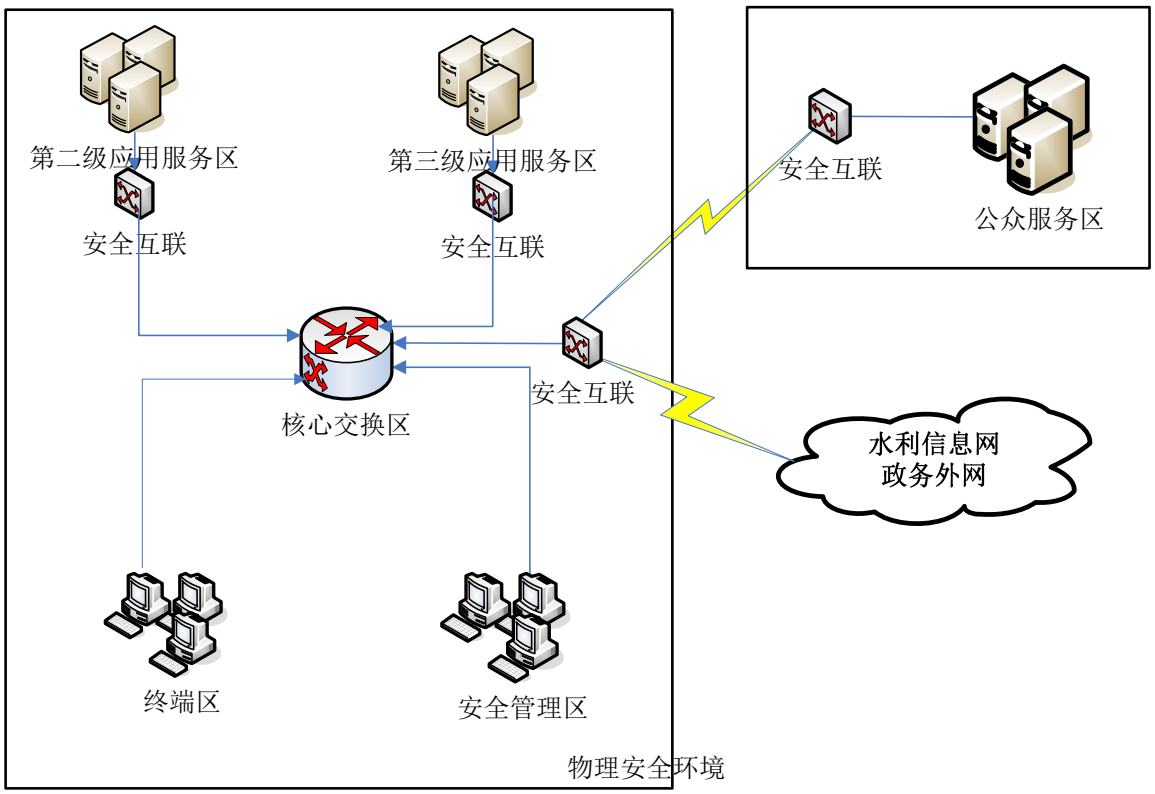

图 3-2 省、流域机构网络与信息安全系统结构图

图 3-2 中各区域功能及要求与部机关安全系统中相应区域一致，省、流域机构公众服务区可能是由第二级信息系统组成或第二级信息系统与第三级信息系统共同组成，按照最高级别的信息系统进行防护。

3.3 市级节点安全系统建设要求

依据 GB 17859-1999《计算机信息系统安全防护等级划分准则》以及《信息安全技术　信息系统等级保护安全设计技术要求》等信息

安全标准规范，各地市级单位信息系统定级情况及网络与信息系统状况，将地市级单位政务外网网络与信息系统划分为 6 个安全保护区和 1 个物理安全环境，6 个安全保护区分别为：第二级应用服务区、第三级应用服务区、终端区、安全管理区、核心交换区、公众服务区。地市级单位网络与信息安全系统结构如图 3-3 所示。

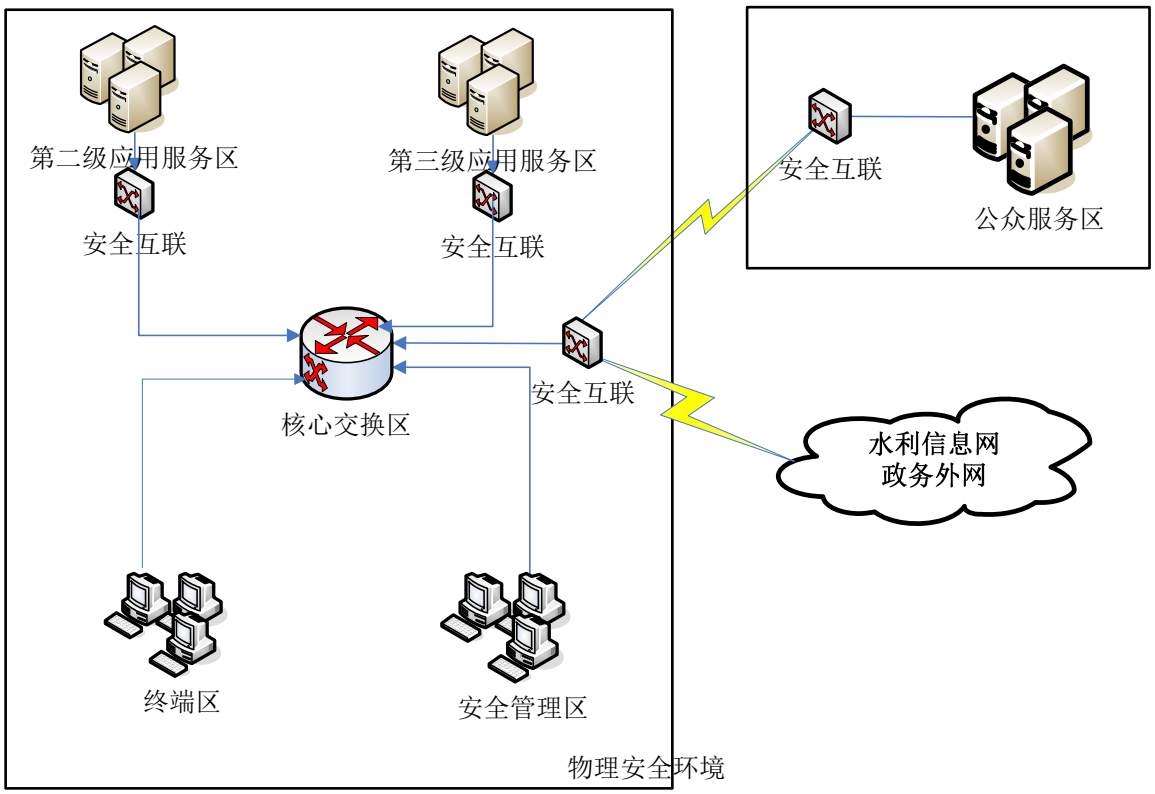

图 3-3 地市级节点网络与信息安全系统结构图

图 3-3 中各区域功能及要求与部机关安全系统中相应区域一致。市级节点公众服务区一般由第二级信息系统组成，按照第二级信息系统进行防护。

3.4 县级节点安全系统建设要求

依据 GB 17859-1999《计算机信息系统安全防护等级划分准则》以及《信息安全技术　信息系统等级保护安全设计技术要求》等信息安全标准规范，各县级单位信息系统定级情况及网络与信息系统状

况，将县级单位政务外网网络与信息系统划分为 5 个安全保护区和 1 个物理安全环境，5 个安全保护区分别为：第二级应用服务区、终端区、安全管理区、核心交换区、公众服务区。县级单位网络与信息安全系统结构如图 3-4 所示。

根据各单位的实际需求，在县级节点新建第三级信息系统时可以参照部机关安全系统建设要求中第三级应用服务区的要求进行安全系统建设。

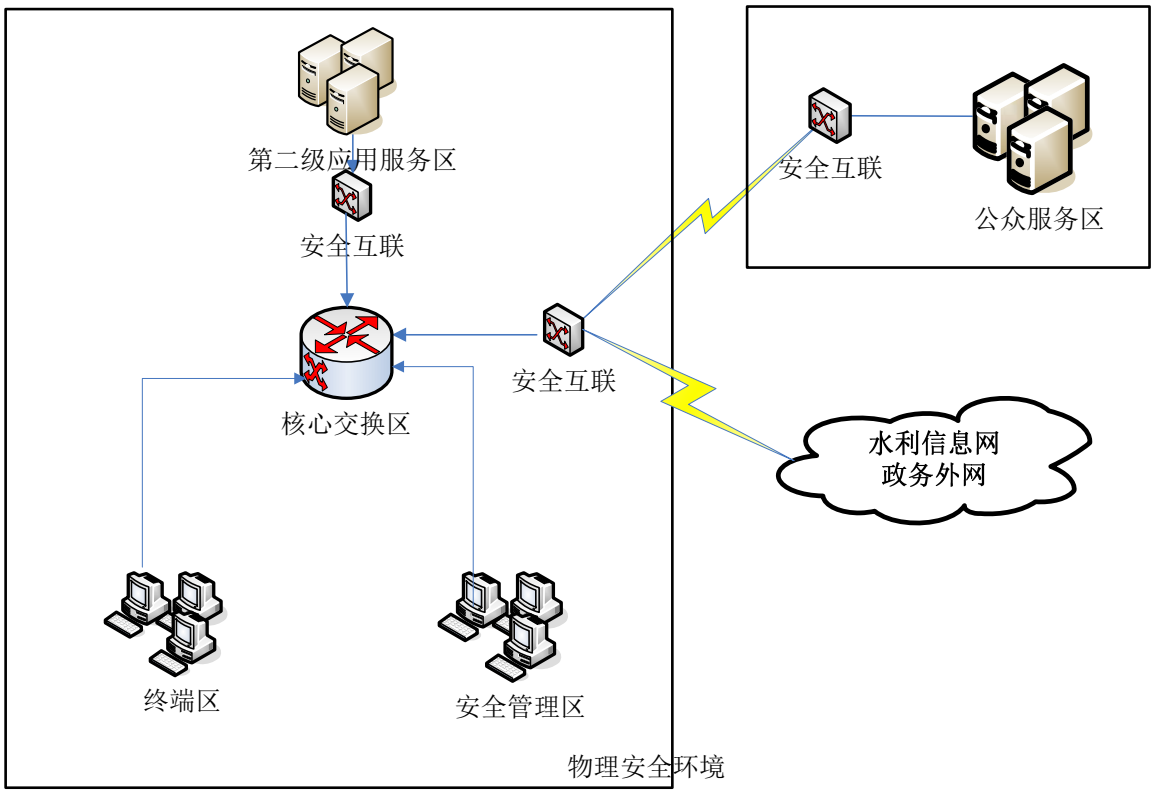

图 3-4 地市级节点网络与信息安全系统结构图

图 3-4 中各区域功能及要求与部机关安全系统中相应区域一致。县级节点公众服务区一般由第二级信息系统组成，按照第二级信息系统进行防护。对于规模较小的节点，安全管理区可以并入第二级应用服务区。

4 安全要素建设要求

各单位在进行网络与信息安全体系设计时，可根据第 2、3 章要求进行安全分区的基础上，参考本章进行各安全保护区设计。

4.1 物理安全环境建设要求

物理安全主要是为网络与信息系统提供机房、电力环境保障以及设备、设施、介质的防盗、防破坏等防护。根据各节点网络与信息系统的位置分布不同，物理安全环境可以分为多个部分，每部分按照该部分承载的信息系统的最高安全等级来确定防护级别。

4.1.1 第二级安全防护物理安全要求

4.1.1.1环境安全

1. 场地选择

机房场地选择应满足:

1) 基本要求：按一般建筑物的要求进行机房场地选择;

2) 防火要求：避开易发生火灾和危险程度高的地区，如油库和其他易燃物附近的区域;

3) 防污染要求：避开尘埃、有毒气体、腐蚀性气体、盐雾腐蚀等环境污染的区域;

4) 防潮及防雷要求：避开低洼、潮湿及落雷区域;

5) 防震动和噪声要求：避开强震动源和强噪声源区域;

6) 防强电场、磁场要求：避开强电场和强磁场区域;

7) 防地震、水灾要求：避开有地震、水灾危害的区域;

8) 防公众干扰要求：避免靠近公共区域，如运输通道、停车场或餐厅等。

2. 机房内部安全防护

机房内部安全防护应满足:

1) 机房出入：机房应只设一个出入口，并有专人负责，未经允许的人员不准进入机房;另设若干紧急疏散出口,标明疏散线路和方向;

2) 机房物品：没有管理人员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房,磁铁、私人电子计算机或电设备、食品及饮料、香烟、吸烟用具等均不准带入机房。

3. 机房防火

机房防火应满足:

1) 建筑材料防火：机房和记录介质存放间，其建筑材料的耐火等级，应符合 TJ16-1974 中规定的第二级耐火等级;机房相关的其余基本工作房间和辅助房,其建筑材料的耐火等级应不低于 TJ16-1974 中规定的第三级耐火等级;

2) 报警和灭火系统：设置火灾报警系统，由人来操作灭火设备，并对灭火设备的效率、毒性、用量和损害性有一定的要求;

3) 区域隔离防火：机房布局应将脆弱区和危险区进行隔离，防止外部火灾进入机房，特别是重要设备地区，应安装防火门、使用阻燃材料装修等。

4. 机房供、配电

机房供、配电应满足:

1) 分开供电：机房供电系统应将计算机系统供电与其他供电分开，并配备应急照明装置;

2) 紧急供电：配置抵抗电压不足的基本设备，如 UPS;

3) 备用供电：建立备用的供电系统，以备常用供电系统停电时启用，完成对运行系统必要的保留;

4) 稳压供电：采用线路稳压器，防止电压波动对计算机系统的影响;

5) 电源保护：设置电源保护装置，如金属氧化物可变电阻、硅雪崩二极管、气体放电管、滤波器、电压调整变压器和浪涌滤波器等，防止/减少电源发生故障。

5. 机房温度、湿度调节

应有必要的空调设备，使机房温度、湿度达到所需设备运行允许的范围。

6. 机房防水与防潮

机房防水与防潮应满足:

1) 水管安装要求：水管安装，不得穿过屋顶和活动地板下，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;

2) 水害防护：采取一定措施，防止雨水通过屋顶和墙壁渗透、室内水蒸气结露和地下积水的转移与渗透。

7. 机房防静电

机房防静电应满足:

1) 接地与屏蔽：采用必要的措施，使计算机系统有一套合理的防静电接地与屏蔽系统;

2) 服装防静电：人员服装采用不易产生静电的衣料，工作鞋选用低阻值材料制作;

3) 温、湿度防静电：控制机房温湿度，使其保持在不易产生静电的范围内;

4) 地板防静电：机房地板从表面到接地系统的阻值，应在不易产生静电的范围;

5) 材料防静电：机房中使用的各种家具，工作台、柜等，应选择产生静电小的材料。

8. 机房接地与防雷击

机房接地与防雷击应满足:

1) 接地要求：采用地桩、水平栅网、金属板、建筑物基础钢筋构建接地系统等，确保接地体的良好接地;

2) 去耦、滤波要求：设置信号地与直流电源地，并注意不造成额外耦合，保障去耦、滤波等的良好效果;

3) 避雷要求：设置避雷地，以深埋地下、与大地良好相通的金属板作为接地点；至避雷针的引线则应采用粗大的紫铜条，或使整个建筑的钢筋自地基以下焊连成钢筋网作为“大地”与避雷针相连。

9. 机房电磁防护

机房电磁防护应满足:

1) 不电源线和通信线缆应隔离，避免相互干扰;

10. 通信线路的安全

确保线路畅通：采取必要措施，保证通信线路畅通。

4.1.1.2设备安全

1. 设备的防盗和防毁

设备的标记、防盗应满足:

1） 设备标记要求：计算机系统的设备和部件应有明显的无法除去的标记，以防更换和方便查找赃物;

2） 计算中心防盗：计算中心应安装防盗报警装置，防止夜间

从门窗进入的盗窃行为。

2. 设备的安全可用

基本运行支持：信息系统的所有设备应提供基本的运行支持，并有必要的容错和故障恢复能力。

4.1.1.3记录介质安全

记录介质安全应满足：

1） 用户公开数据介质保护：存放用户公开数据的各类记录介质，如纸介质、磁介质、半导体介质和光介质等，应采取一定措施防止被毁和受损；

2） 用户内部数据介质保护：存放用户内部数据的各类记录介质，如纸介质、磁介质、半导体介质和光介质等，应采取一定措施，防止被盗、被毁和受损；需要删除和销毁的内部数据，应有一定措施，防止被非法拷贝。

4.1.2 第三级安全防护物理安全要求

在达到第二级安全防护物理安全要求的基础上达到以下物理安全要求。

4.1.2.1环境安全

1 机房场地选择

1) 位置要求：避免在建筑物的高层以及用水设备的下层或隔壁；

2 机房内部安全防护

1) 机房人员：获准进入机房的来访人员，其活动范围应受到限制，并有接待人员陪同；

2)机房分区：机房内部应分区管理，一般分为主机区、操作区、辅助区等，并根据每个工作人员的实际工作需要，确定其能进入的区域；

3)机房门禁：设置机房电子门禁系统，进入机房的人员，通过门禁系统的鉴别，方可进入。

3 机房防火

1)建筑材料防火：机房和重要的记录介质存放间，其建筑材料的耐火等级，应符合 GBJ45-1982 中规定的第二级耐火等级；机房相关的其余基本工作房间和辅助房，其建筑材料的耐火等级应不低于 TJ16-1974 中规定的第二级耐火等级；

2)报警和灭火系统：设置火灾自动报警系统，包括火灾自动探测器、区域报警器、集中报警器和控制器等，能对火灾发生的部位以声、光或电的形式发出报警信号，并启动自动灭火设备，切断电源、关闭空调设备等；

4 机房供、配电

1)紧急供电：配置抵抗电压不足的改进设备，如基本 UPS、改进 UPS、多级 UPS；

2)不间断供电：采用不间断供电电源，防止电压波动、电器干扰、断电等对计算机系统的影响。

5 机房防水与防潮

防水检测：安装对水敏感的检测仪表或元件，对机房进行防水检测，发现水害，及时报警。

6 机房接地与防雷击

防护地与屏蔽地要求：设置安全防护地与屏蔽地，采用阻抗尽可能小的良导体的粗线，以减小各种地之间的电位差；应采用焊接方法，

并经常检查接地的良好，检测接地电阻，确保人身、设备和运行的安全。

7 通信线路的安全防护

及时发现线路截获：采取必要措施，及时发现线路截获事件并报警。

4.1.2.2设备安全

1 设备的防盗和防毁

1）计算中心防盗：计算中心应利用光、电、无源红外等技术设置机房报警系统，并有专人值守，防止夜间从门窗进入的盗窃行为；

2）机房外部设备防盗：机房外部的设备，应采取加固防护等措施，必要时安排专人看管，以防止盗窃和破坏。

2 设备的安全可用

设备安全可用：支持信息系统运行的所有设备，包括计算机主机、外部设备、网络设备及其他辅助设备等均应安全可用。

4.1.2.3记录介质安全

用户重要数据介质保护：存放用户重要数据的各类记录介质，如纸介质、磁介质、半导体介质和光介质等，应采取较严格的保护措施，防止被盗、被毁和受损；应该删除和销毁的重要数据，要有有效的管理和审批手续，防止被非法拷贝。

4.1.3 第四级安全防护物理安全要求

在达到第三级安全防护物理安全要求的基础上达到以下物理安全要求。

4.1.3.1环境安全

1 机房供、配电

1) 电器噪声防护：采取有效措施，减少机房中电器噪声干扰，保证计算机系统正常运行;

2) 突然事件防护：采取有效措施，防止/减少供电中断、异常状态供电（指连续电压过载或低电压）、电压瞬变、噪声（电磁干扰）以及由于雷击等引起的设备突然失效事件。

2 机房防水与防潮

排水要求：机房应设有排水口，并安装水泵，以便迅速排出积水。

3 机房防静电

1) 维修 MOS 电路保护：在硬件维修时，应采用金属板台面的专用维修台，以保护 MOS 电路;

2) 静电消除要求：在机房中使用静电消除剂和静电消除器等，以进一步减少静电的产生。

4 机房接地与防雷击

交流电源地线要求：设置交流电源地线；交流供电线应有规范连接位置的三芯线，即相线、中线和地线，并将该“地线”连通机房的地线网，以确保其安全保护作用。

5 机房电磁防护

电磁屏蔽：关键区域应采用必要措施，防止计算机设备产生的电磁泄漏发射造成信息泄露。

6 通信线路的安全防护

防止线路截获：采取必要措施，防止线路截获事件发生。

4.1.3.2设备安全

1 设备的安全可用

设备不间断运行：提供可靠的运行支持，并通过容错和故障恢复等措施，支持信息系统实现不间断运行。

4.2 第二级应用服务区建设要求

第二级应用服务区通过建设第二级的安全计算环境、安全区域边界、安全通信网络及安全管理中心实现第二级系统安全保护环境，为第二级信息系统提供安全防护。

4.2.1 安全计算环境建设

安全计算环境子系统通过使用安全操作系统或对操作系统进行安全加固并进行功能扩充，加入身份认证、自主访问控制、系统安全审计、客体安全重用、系统恶意代码查杀等功能。

4.2.1.1用户身份鉴别（S2）

通过使用符合第二级安全保护要求的安全操作系统或相应的系统加固软件实现用户身份鉴别，安全操作系统或系统加固软件需具备以下功能：

- 宜支持数字证书进行身份认证。
- 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；
- 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;

- 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。
- 在每次用户登录系统时，采用强化管理的口令或具有相应安全强度的其他机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护。

4.2.1.2自主访问控制（S2）

自主访问控制是使用户在安全策略控制范围内，对自己创建的客体具有各种访问操作权限，并能将这些权限的部分或全部授予其他用户。

通过使用符合第二级安全保护要求的安全操作系统或相应的系统加固软件进行系统加固实现自主访问控制安全要求。安全操作系统或系统加固软件需具备以下功能:

- 策略控制: 能接收到管理中心下发的安全策略，并能依据此策略对登录用户的操作权限进行控制;
- 客体创建: 用户可以在管理中心下发的安全策略控制范围内创建客体，并拥有对客体的各种访问操作（读、写、修改和删除等）权限;
- 授权管理: 用户可以将自己创建的客体的访问权限（读、写、修改和删除等）的部分或全部授予其他用户;
- 访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。

4.2.1.3系统安全审计（G2）

通过部署审计系统，探测、记录、相关安全事件，并将审计记录转换为标准格式，上报安全管理中心实现系统安全审计。审计系统需具备以下功能:

- 对系统相关安全事件进行审计、记录;
- 可以直接或通过审计代理，将安全事件上报安全管理中心;
- 对审计记录应包括安全事件的主体、客体、时间、类型和结果等内容。

4.2.1.4客体安全重用（S2）

在客体安全重用要求能对于动态管理和使用的客体资源，应在客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄漏。客体安全重用可以通过操作系统加固，利用系统加固时建立的客体安全重用机制实现; 也可以通过部署客体安全重用系统，对客体资源进行监控、管理，并记录相关审计信息。对建立的客体安全重用系统，需能对使用的客体资源（文件存储、内存使用）进行监控、管理，在该客体资源重新分配前对其原使用者的信息进行清除，以确保系统的重要信息不被泄漏。

4.2.1.5恶意代码防范（G2）

通过部署病毒防护系统或配置具有相应功能的安全操作系统，实现安全计算环境的病毒防护以及恶意代码防范。病毒防护系统需具备以下功能:

- 远程控制与管理
- 全网查杀毒

- 防毒策略的定制与分发
- 实时监控客户端防毒状况
- 病毒与事件报警
- 病毒日志查询与统计
- 集中式授权管理
- 全面监控邮件客户端

4.2.1.6备份和恢复（A2）

建立数据备份措施,建立备份管理制度，制定数据备份策略，对重要信息进行备份以及对依据备份记录进行数据恢复。

关键网络设备、线路和数据处理设备硬件冗余。

4.2.2 安全区域边界建设

4.2.2.1区域边界协议过滤（G2）

在系统区域边界，部署防火墙或其他访问控制设备，通过访问控制策略,实现边界协议过滤。访问控制设备需具备以下功能:

- 实现基于源/目的 IP 地址、源 MAC 地址、服务/端口、用户、时间、组（网络，服务，用户，时间）的精细粒度的访问控制;
- 能对连接、攻击、认证和配置等行为进行审计，并且可以对审计事件提供的告警;
- 实现日志的本地存储、远端存储、备份等存储方式。

4.2.2.2区域边界恶意代码防范（G2）

在区域边界部署防恶意代码设备实现区域边界的病毒防护以及

恶意代码防范。区域边界防恶意代码设备需具备以下功能:

- 应具有恶意代码库;
- 恶意代码的识别与及时清除能力及清除失败的补救能力;
- 应提供管理界面对恶意代码库的升级和检测系统的更新进行维护;
- 能通过管理中心对防恶意代码设备进行管理。

4.2.2.3区域边界安全审计（G2）

在区域边界部署审计系统,收集、记录区域边界的相关安全事件,并将审计记录转换为标准格式,上报审计管理中心。区域边界审计系统需具备以下功能:

- 收集、记录区域边界的各项安全日志信息;
- 并使用标准通讯协议将探测到的各种审计信息上报安全管理中心;
- 审计记录应包括事件的日期和时间、主体、事件类型、事件是否成功,及其他与审计相关的信息。

4.2.2.4区域边界完整性保护（G2）

在区域边界部署检测设备实现探测非法外联和入侵等行为,完成对区域边界的完整性保护。检测设备需具备以下功能:

- 能通过监视端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等攻击行为;
- 能检测内部网络中用户私自联到外部网络的行为;
- 探测结果需上报到安全审计系统。

4.2.3 安全通信网络建设

4.2.3.1通信网络安全审计（G2）

部署网络审计系统或使用安全网络设备等，收集、记录通信网络的相关安全事件，并将审计记录转换为标准格式，上报审计管理中心。通信网络审计系统需具备以下功能：

- 探测、记录通信网络中的网络设备配置、网络流量、用户网络行为等安全事件；
- 将探测到的各种审计信息上报安全管理中心；
- 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息。

4.2.3.2通信网络数据传输完整性保护（G2）

通过密码技术或其他数据校验机制，对鉴别信息和重要业务数据在传输过程中完整性进行保护。

4.3 第三级应用服务区建设要求

4.3.1 安全计算环境建设

4.3.1.1用户身份鉴别（S3）

通过使用符合第三级安全保护要求的安全操作系统或相应的系统加固软件实现用户身份鉴别，安全操作系统或系统加固软件除具备4.2.1.1用户身份鉴别的要求外，还需具备以下功能：

- 在每次用户登录系统时，采用强化管理的口令、基于生物特征、

基于数字证书以及其他具有相应安全强度的两种或两种以上机制的组合进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护。

4.3.1.2自主访问控制（S3）

通过使用符合第三级安全保护要求的安全操作系统或相应的系统加固软件进行系统加固，并结合安全管理中心的安全管理功能实现自主访问控制安全要求。安全操作系统或系统加固软件除满足4.2.1.2中的要求外，还需具备以下功能：

- 访问控制客体的粒度为文件或数据库表级和（或）记录及字段级。

4.3.1.3标记和强制访问控制（S3）

通过采用符合第三级安全保护要求的安全操作系统或通过采用相应的系统加固软件对系统进行加固，通过其提供的标记和强制访问控制系统，实现标记和强制访问控制功能。安全操作系统或系统加固软件需具备以下功能：

- 在对安全管理员进行严格的身份鉴别和权限控制基础上，由安全管理员通过特定操作界面对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制；
- 强制访问控制主体的粒度应为用户级，客体的粒度应为文件或数据库表级；应确保系统安全计算环境内所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。

4.3.1.4系统安全审计（G3）

通过部署审计系统，探测、记录、相关安全事件，并将审计记录转换为标准格式，上报安全管理中心实现系统安全审计。审计系统除满足 4.2.1.3 的要求外，还需具备以下功能:

- 要求审计系统能接收由安全管理中心下发的安全事件报警策略;
- 审计系统依据预定义的报警策略对特定安全事件进行报警。

4.3.1.5用户数据完整性保护（G3）

通过密码技术支持的完整性保护机制和数据备份系统，共同实现用户数据完整性保护。

密码技术支持的完整性保护机制需具备以下功能:

- 能对系统管理数据、鉴别信息和重要业务数据通过密码算法提供的验证机制，对存储的数据进行完整性验证;
- 能对发现的数据破坏事件进行记录。

要求数据备份系统包含以下基本功能:

- 能根据备份管理策略，自动进行数据备份;
- 用户可以通过备份记录进行数据恢复。

4.3.1.6用户数据保密性保护（G3）

用户数据保密性保护要求提供系统管理数据、鉴别信息、重要用户数据存储过程的保密性。可采用以下方法中的任意一种进行实现:

1) 通过部署符合第三级信息系统安全要求的安全操作系统或部署具备强制访问控制功能的系统加固软件，实现对存储数据的保密性保护;

2）通过建立数据加密系统实现对存储数据的保密性保护。

4.3.1.7客体安全重用（S3）

同 4.2.1.4 要求。

4.3.1.8恶意代码防范（G3）

同 4.2.1.5 要求。

4.3.1.9备份和恢复(A3)

在满足 4.2.1.6 要求的基础上，还需具备以下功能:

- 部署备份管理系统，并且要求备份管理系统能设置定时备份，能通过网络将备份数据传送到备用场地，进行备份数据存储。
- 对关键网络设备提供双机热备，进行网络双回路设计，对重要信息系统采用集群或双机器热（冷）备。

4.3.2 安全区域边界建设

4.3.2.1区域边界访问控制（S3）

在网络区域边界部署访问控制设备，实现对区域边界的访问控制。访问控制设备需具备以下功能:

- 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级;
- 应在会话处于非活跃一定时间或会话结束后终止网络连接;

- 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。

4.3.2.2区域边界协议过滤（G3）

在系统区域边界，部署防火墙或其他访问控制设备，通过访问控制策略，实现边界协议过滤，防火墙或其他访问控制设备除满足4.2.2.1的要求外，还需具备以下功能：

- 能实现网络流量控制，依照义务的优先级别分配带宽，确保业务的连续服务；
- 具备对ARP攻击等地址欺骗手段攻击的防御能力；

4.3.2.3区域边界安全审计（G3）

在区域边界部署审计系统，收集、记录区域边界的相关安全事件，并将审计记录转换为标准格式，上报审计管理中心。对于区域边界审计系统除需满足4.2.2.3的要求外，还需具备以下功能：

- 在发现违规行为时能进行及时报警功能。

4.3.2.4区域边界恶意代码防范（G3）

同4.2.2.2要求。

4.3.2.5区域边界完整性保护（G3）

在区域边界部署检测设备实现探测非法外联和入侵等行为，完成对区域边界的完整性保护。除满足4.2.2.4的要求外，还需具备以下功能：

- 部署内网安全管理系统，对接入内网的设备进行认证，并对接

入内网的设备网络资源访问权限进行严格控制;

4.3.3 安全通信网络建设

4.3.3.1通信网络安全审计（G3）

部署网络审计系统，收集、记录通信网络的相关安全事件，并将审计记录转换为标准格式，上报审计管理中心。通信网络审计系统除满足 4.2.3.1 的要求外，还需具备以下功能:

- 对确认的违规行为及时报警。

4.3.3.2通信网络数据传输完整性保护（G3）

通过等密码技术或其他数据校验机制，对系统管理数据、鉴别信息和重要业务数据在传输过程中完整性进行保护，发现数据破坏的同时，对被破坏的数据进行修复或自动抛弃被破坏的数据，向数据发送端重新请求被抛弃的数据。

4.3.3.3通信网络数据传输保密性保护（G3）

通信网络数据传输保密性要求提供系统管理数据、鉴别信息、重要用户数据传输的保密性保护。可采用以下方法中的任意一种进行实现:

1) 通过建立 VPN 为数据传输提供数据保密性保护;
2) 通过采用加密传输设备为数据传输提供数据保密性保护;
3) 通过部署符合第三级信息系统安全要求的安全操作系统或部署具数据加密传输功能的系统加固软件，为数据传输提供数据保密性保护。

4.4 第四级应用服务区建设要求

4.4.1 安全计算环境建设

4.4.1.1用户身份鉴别（S4）

通过使用符合第四级安全保护要求的安全操作系统或相应的系统加固软件实现用户身份鉴别，安全操作系统或系统加固软件除具备4.3.1.1的要求外，还需具备以下功能:

- 在每次用户登录和重新连接系统时，采用强化管理的口令、基于生物特征数据、基于数字证书以及其他具有相应安全强度的两种或两种以上机制的组合进行用户身份鉴别;
- 其中一种鉴别技术产生的鉴别数据是不可替代的，并对鉴别数据进行保密性和完整性保护。

4.4.1.2自主访问控制（S4）

同4.3.1.2中的要求。

4.4.1.3标记和强制访问控制（S4）

通过采用符合第四级安全保护要求的安全操作系统或通过采用相应的系统加固软件对服务器以及终端进行系统加固，通过其提供的标记和强制访问控制系统，实现标记和强制访问控制功能。符合第四级安全保护要求的安全操作系统或系统加固软件在满足4.3.1.3的要求外，还需具备以下功能:

- 能将强制访问控制扩展到所有主体与客体;
- 应按安全标记和强制访问控制规则，对确定主体访问客体的操

作进行控制。

4.4.1.4系统安全审计（G4）

通过部署审计系统，探测、记录、相关安全事件，并将审计记录转换为标准格式，上报安全管理中心实现系统安全审计。审计系统除满足 4.3.1.4 的要求外，还需具备以下功能:

- 能对特定安全事件进行报警和相应的处置，终止违例进程等;确保审计记录不被破坏或非授权访问以及防止审计记录丢失等;
- 应为安全管理中心提供接口;对不能由系统独立处理的安全事件，应提供可由授权主体调用的接口。

4.4.1.5用户数据完整性保护（G4）

同 4.3.1.5 要求。

4.4.1.6用户数据保密性保护（G4）

同 4.3.1.6 要求。

4.4.1.7客体安全重用（S4）

同 4.3.1.7 要求。

4.4.1.8程序可信执行保护（G4）

通过采用符合第四级安全保护要求的安全操作系统或通过采用相应的系统加固软件对服务器以及终端进行系统加固，构建从操作系统到上层应用的信任链，其中可采用可信计算技术，以实现系统运行

过程中可执行程序的完整性检验，防范恶意代码等攻击，并在检测到其完整性受到破坏时，应采取有效的恢复措施。

4.4.1.9备份和恢复(A4)

除满足 4.3.1.9 的要求外，还需具备以下功能:

- 在异地建立数据备份中心，进行数据实时备份;
- 为建立异地灾难备份中心配备应急通信线路、网络设备和数据处理设备，提供业务应用的实时无缝切换;
- 主要网络设备和数据处理硬件系统需提供冗余，通信线路提供双回路。

4.4.2 安全区域边界建设

4.4.2.1区域边界访问控制（S4）

同 4.3.2.1 要求。

4.4.2.2区域边界协议过滤（G4）

同 4.3.2.2 要求。

4.4.2.3区域边界安全审计（G4）

在区域边界部署审计系统，收集、记录区域边界的相关安全事件，并将审计记录转换为标准格式，上报审计管理中心。区域边界审计系统除需满足 4.3.2.3 的要求外，还需具备以下功能:

- 在发现违规行为时能进行及时报警和并做出相应的处置。

4.4.2.4区域边界完整性保护（G4）

同 4.3.2.5 要求。

4.4.3 安全通信网络建设

4.4.3.1通信网络安全审计（G4）

部署网络审计系统，收集、记录通信网络的相关安全事件，并将审计记录转换为标准格式，上报审计管理中心。通信网络审计系统除需满足 4.3.3.1 的要求外，还需具备以下功能：

- 对确认的违规行为及时报警并做出相应处置。

4.4.3.2网络数据传输完整性保护（G4）

同 4.3.3.2 要求。

4.4.3.3网络数据传输保密性保护（G4）

同 4.3.3.3 要求。

4.4.3.4网络可信接入（G4）

在网络区域边界部署可信网络接入设备或采用可信接入技术，依据安全管理中心制定的安全策略，对接入网络的设备进行验证，实现对区域边界保护。

4.5安全管理区建设要求

各级节点应建立集中安全管理中心，对本节点内安全设施进行集

中管理，根据需要可以在各应用服务区建设本区的安全管理中心，负责本区内的安全集中管理。

安全管理中心包括：包括系统/安全管理和审计管理，系统/安全管理对信息系统安全保护环境中的计算节点、区域边界、通信网络实施管理和维护，包括用户身份管理、资源管理、应急处理、授权管理和策略管理。审计管理对安全保护环境中的计算节点、区域边界、通信网络、系统/安全管理依据制定的审计策略统一实施安全审计，记录确定的系统安全相关事件并对其分析；提供受保护的审计踪迹存储和审计记录的保护；为系统不能独立分辨的审计事件提供可由授权主体调用的审计接口。

4.5.1 第二级安全管理中心建设

4.5.1.1系统管理要求

应对系统管理员进行身份鉴别，只允许使用特定的命令和操作界面进行系统管理操作，并对管理操作进行审计。

4.5.1.2审计管理要求

应对安全审计员进行身份鉴别，只允许使用特定的命令和操作界面进行安全审计操作。

4.5.2 第三级安全管理中心建设

4.5.2.1系统管理中心要求

系统管理中心除需满足 4.5.1.1 的要求外，还需具备以下功能：

- 用户身份管理，系统资源配置，系统加载和启动，系统运行的

异常处理，以及支持管理本地和/或异地灾难备份与恢复等;

- 及时发现发生的安全事件，并采取相应措施。

4.5.2.2安全管理中心要求

建立安全管理中心对主\客体进行统一标记，用户授权、策略等进行集中管理。对安全管理员进行身份鉴别，只允许使用特定的命令和操作界面进行安全管理操作，并对管理操作进行审计。安全管理中心功能要求如下:

1) 标记管理功能要求如下:

- 提供主体标记管理功能，为系统中的所有用户配置安全级别和安全范畴。
- 提供客体标记管理功能，为系统与安全业务相关的客体设定安全标记。安全标识包括与文件名直接相关的安全标识、目录安全标识、通配符格式的安全标识等类型。同时提供安全标识中安全级别的修改接口，供人工参与安全级别的制定和更改。

2) 授权管理功能要求如下:

- 提供授权管理界面，安全管理子系统提供授权模板维护强制访问控制表和自主访问控制表，将对特定客体的读、写执行等权限赋予相应的用户。对应用流程的特定位置进行授权，制定级别调整策略、网络访问控制策略等。
- 提供策略批准功能，接收并查看来自系统管理员以及各节点上报的策略申请信息，依据安全管理规则和主客体的安全标识信息，对合法的申请内容予以批准。

3) 策略管理功能要求如下:

- 生成访问策略库。访问策略库是将用户与用户能够访问的客体

资源结合起来所形成的一个访问控制策略表，安全管理子系统根据应用的安全策略配置，生成访问策略设置，并将访问策略设置与策略配置功能所生成的用户身份配置、文件标识配置以及可信接入策略和可信进程名单等组装发送到各安全部件中。

- 策略请求处理和下发。策略请求和处理是将设定客体安全级别的特权和该特权所授予的用户身份结合起来所形成的一个权限列表，该列表项目来源于各用户提出的主客体安全级别修改请求和自主访问控制策略申请，反应客体资源属性和主体的权限范围，并将该列表发送给相应主体所在的平台。
- 策略的维护。策略的维护功能为安全管理员的策略查找、策略更新等操作提供支持，并能够实现策略文件的导入和导出操作，支持离线状态下的策略管理，提高安全管理员的策略管理操作的方便性和易用性。

4.5.2.3审计管理中心要求

审计管理中心除需满足 4.5.1.2 的要求外，还需具备以下功能：

- 对分散到系统各部分的安全审计机制进行集中的管理，对审计记录进行分类，并将这些记录转换为标准格式进行记录，对各类审计记录进行存储、管理和查询；
- 实现自动对采集的审计信息进行分析，对违规行为进行报警，并能进行报警方式的设置。

4.5.3 第四级安全管理中心建设

4.5.3.1系统管理中心要求

同 4.5.2.1 要求。

4.5.3.2安全管理中心要求

安全管理管理中心除需满足 4.5.2.2 的要求外，还需具备以下功能:

- 确保标记、授权合安全策略的数据完整性。

4.5.3.3审计管理中心要求

审计管理中心除需满足 4.5.2.3 的要求外，还需具备以下功能:

- 对违规行为进行及时处理。

4.6 核心交换区建设要求

核心交换区主要工作是数据交换，各级系统安全保护环境及终端区通过安全互联到核心交换区实现数据交换处理;

核心交换区汇聚所有数据的集合，核心交换区应提供高速转发通信，可靠的骨干传输结构，因此核心交换区应拥有更高的交换性能和吞吐量。

4.7终端区建设要求

4.7.1 第二级终端安全要求

终端访问安全保护等级为第二级的信息系统需通过使用安全操

作系统或对操作系统进行安全加固并进行功能扩充满足以下要求:

- 用户身份鉴别：详细参照 4.2.1.1 要求;
- 自主访问控制：详细参照 4.2.1.2 要求;
- 系统安全审计：提供对用户登录审计、文件访问审计、进程启动审计、移动存储设备使用审计、网络访问审计。
- 恶意代码防范：详细参照 4.2.1.5 要求。

4.7.2 第三级终端安全要求

终端访问安全保护等级为第三级的信息系统需通过使用安全操作系统或对操作系统进行安全加固并进行功能扩充满足以下要求:

- 用户身份鉴别：详细参照 4.3.1.1 要求;
- 自主访问控制：详细参照 4.3.1.2 要求;
- 强制访问控制：提供控制文件操作（读、写、改名和删除）、文件的特权访问，粒度为文件或文件夹。
- 系统安全审计：提供对用户登录审计、文件访问审计、进程启动审计、移动存储设备使用审计、网络访问审计。
- 数据保密性保护：提供信息进行加密保护，加密粒度为文件或目录;
- 恶意代码防范：详细参照 4.3.1.8 要求。

4.7.3 第四级终端安全要求

终端访问安全保护等级为第四级的信息系统需通过使用安全操作系统或对操作系统进行安全加固并进行功能扩充满足以下要求:

- 用户身份鉴别：详细参照 4.4.1.1 要求;
- 自主访问控制：详细参照 4.4.1.2 要求;

- 强制访问控制：提供控制文件操作（读、写、改名和删除）、文件的特权访问，粒度为文件或文件夹。
- 系统安全审计：提供对用户登录审计、文件访问审计、进程启动审计、移动存储设备使用审计、网络访问审计。
- 数据保密性保护：提供信息进行加密保护，加密粒度为文件或目录;
- 恶意代码防范：详细参照 4.4.1.9 要求;
- 程序可信执行保护：提供程序保护，非授权程序无法获得执行权限，被篡改的授权程序无法启动，授权程序无法被写篡改。

4.8 公众服务区建设要求

4.8.1 部级节点

水利部公众服务区按照第三级应用服务区的相关要求建设。

4.8.2 省、流域级节点

在水利行业省、流域级单位的公众服务区，一般包含有已定级为第二级、第三级的公众服务系统。公众服务区根据包含的公众服务系统最高等级按照相应等级应用服务区的相关要求建设。

4.8.3 市级节点

在水利行业市级单位的公众服务区，一般包含有已定级为第二级的公众服务系统，公众服务区按照第二级应用服务区的相关要求建设。当市级单位的公众服务区中包含有已定级为第三级的信息系统时，需要按照第三级应用服务区的相关要求进行设计、建设或整改。

4.8.4 县级节点

在水利行业县级单位的公众服务区，一般包含有已定级为第二级的信息系统。公众服务区按照第二级应用服务区的相关要求建设。当县级单位的公众服务区中包含有已定级为第三级的信息系统时，需要按照第三级应用服务区的相关要求进行设计、建设或整改。

4.9安全互联部件建设要求

安全互联部件遵循 GB 17859-1999 对各级系统的安全保护要求，以各定级系统的计算环境安全、区域边界安全和通信网络安全为基础，通过安全管理中心增加相应的安全互联策略，保持用户身份、主/客体标记、访问控制策略等安全要素的一致性，对互联系统之间的互操作和数据交换进行安全保护。

1、系统间互操作安全要求

各级系统之间的互操作安全防护包括访问控制部分和数据传输保护部分。对于访问控制部分，需要对全系统中的主体、客体进行统一标记，并设置统一的访问规则。对于数据传输保护部分由相关的通信网络来实现。

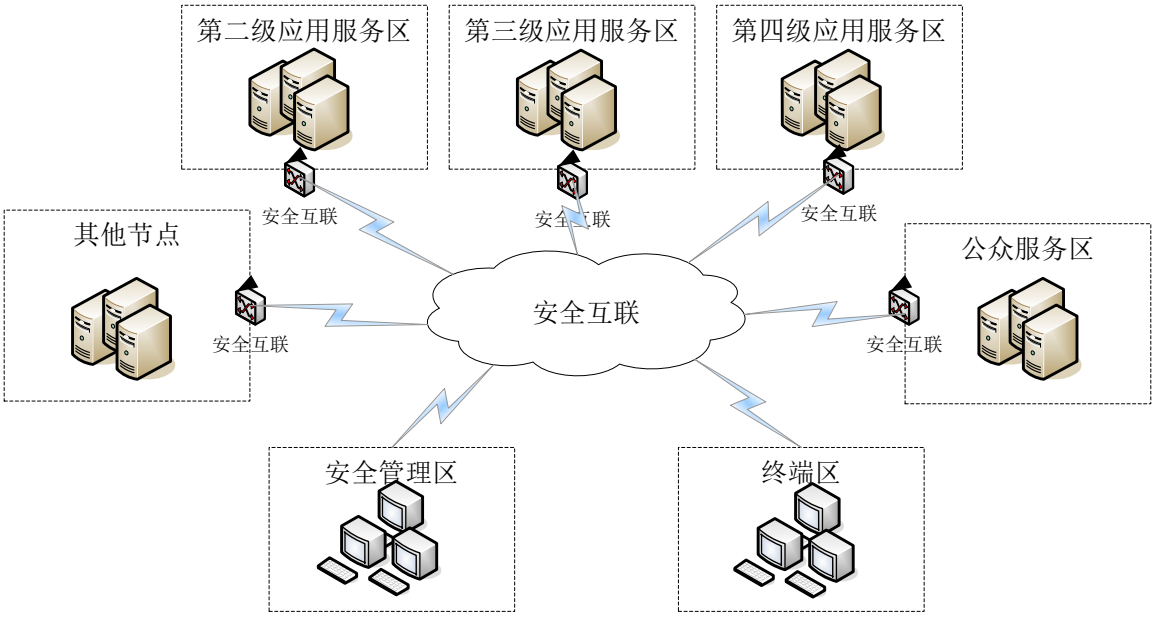

图 4-1 安全互联系统结构示意图

2、系统间数据交换安全要求

各级系统之间的数据交换安全防护主要是确保通过跨系统通信网络进行数据交换的参与者双方身份的真实性和交换数据的真实性及抗抵赖等。实现通信网络数据交换的参与者双方身份的真实性和交换数据的真实性及抗抵赖等，可以采用以 PKI 为基础的 CA 系统实现或采用具有相当安全性的其他安全机制实现。

5 应用安全建设要求

新建应用系统或对已有应用系统升级改造时，可以参照本要求进行应用系统安全建设。

5.1 第二级应用安全建设

5.1.1 身份鉴别(S2)

1) 宜支持 CA 数字证书进行身份认证;

2) 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;

3) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用;

4) 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。

5.1.2 访问控制(S2)

1) 应提供访问控制功能，依据安全策略控制用户对应用资源的访问;

2) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作;

3) 应由授权主体配置访问控制策略;

4) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

5.1.3 安全审计(G2)

1) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计;

2) 应保证无法删除、修改审计记录,应将审计记录上传至安全管理中心;

3) 审计记录的内容至少应包括事件日期、时间、发起者信息、类型、描述和结果等。

5.1.4 软件容错（A2）

1) 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。

5.1.5 资源控制（A2）

1) 当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话;

2) 应能够对系统的最大并发会话连接数进行限制;

3) 应能够对单个帐户的多重并发会话进行限制。

5.2 第三级应用安全建设

5.2.1 身份鉴别(S3)

在实现 5.1.1 要求的基础上，还需实现以下要求:

1) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别;

2) 可提供身份鉴别策略管理接口，由安全管理中心统一管理策略。

5.2.2 访问控制(S3)

在实现 5.1.2 要求的基础上，还需实现以下要求:

1) 应具有对重要应用资源设置敏感标记的功能;

2) 应依据安全策略严格控制用户对有敏感标记重要应用资源的操作;

3) 可提供访问控制策略管理接口，由安全管理中心统一管理策略。

5.2.3 安全审计（G3）

在实现 5.1.3 要求的基础上，还需实现以下要求:

1) 应保证无法单独中断审计进程;

2) 可提供审计策略管理接口，由安全管理中心统一管理策略。

5.2.4 客体安全重用（S3）

1) 可保证用户鉴别信息所在的存储空间被释放前得到完全清除，无论这些信息是存放在硬盘上还是在内存中;

2) 可保证应用数据的存储空间被释放前得到完全清除。

5.2.5 抗抵赖(G3)

1) 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的功能;

2) 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

5.2.6 软件容错（A3）

同 5.1.4 的要求。

5.2.7 资源控制（A3）

在实现 5.1.5 要求的基础上，还需实现以下要求:

1) 应能够对一个时间段内可能的并发会话连接数进行限制;

2) 应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额。

5.3 第四级应用安全建设

5.3.1 身份鉴别(S4)

在实现 5.2.1 要求的基础上，还需实现以下要求:

1) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别，其中一种是不可伪造的。

5.3.2 访问控制（S4）

在实现 5.2.2 要求的基础上，还需实现以下要求:

1) 应通过比较安全标记来确定是授予还是拒绝主体对客体的访问。

5.3.3 可信路径（S4）

1) 在应用系统对用户进行身份鉴别时，应能够建立一条安全的信息传输路径；

2) 在用户通过应用系统对资源进行访问时，应用系统应保证在被访问的资源与用户之间应能够建立一条安全的信息传输路径。

5.3.4 安全审计(G4)

同 5.2.3 要求。

5.3.5 客体安全重用（S4）

同 5.2.6 要求。

5.3.6 抗抵赖（G4）

同 5.2.7 要求。

5.3.7 软件容错（A4）

同 5.2.6 要求。

5.3.8 资源控制（A4）

同 5.2.9 要求。