HJ

中华人民共和国国家环境保护标准

HJ 729-2014

环境信息系统安全技术规范

Security specification of environmental information system

（发布稿）

本电子版为发布稿。请以中国环境科学出版社出版的正式标准文本为准。

2014-12-25 发布　　2015-03-01 实施

环　境　保　护　部　发布

目　　次

前　　言

为贯彻落实《中华人民共和国环境保护法》，促进环境信息化工作，加强和规范环境信息系统的安全建设与管理，保障环境信息系统安全，制定本标准。

本标准规定了环境信息系统的物理安全、网络安全、主机安全、应用安全、数据安全与备份恢复、系统建设、系统运维、终端与办公安全方面的安全要求。

本标准附录 A、附录 B 为规范性附录，附录 C 为资料性附录。

本标准首次发布。

本标准由环境保护部科技标准司组织制订。

本标准主要起草单位：环境保护部信息中心、北京神州绿盟科技有限公司。

本标准环境保护部 2014 年 12 月 25 日批准。

本标准自 2015 年 3 月 1 日起实施。

本标准由环境保护部解释。

环境信息系统安全技术规范

1 适用范围

本标准规定了环境信息系统的物理安全、网络安全、主机安全、应用安全、数据安全与备份恢复、系统建设、系统运维、终端与办公安全的安全要求。

本标准适用于国家环境保护业务专网内的环境信息系统的规划、设计、开发、运行及维护等各个阶段。

2 规范性引用文件

本标准内容引用了下列文件或其中的条款。凡是不注明日期的引用文件，其有效版本适用于本标准。

GB/T 5271.8-2001 信息技术 词汇

GB/T 17859-1999 计算机信息系统 安全保护等级划分准则

GB/T 20270-2006 信息安全技术 网络基础安全技术要求

GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求

GB/T 20282-2006 信息安全技术 信息系统安全工程管理要求

GB/T 20988-2007 信息系统灾难恢复规范

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 25070-2010 信息安全技术 信息系统等级保护安全设计技术要求

GB/T 50052-2009 供配电系统设计规范

GB/T 50174-2008 电子信息系统机房设计规范

HJ 511-2009 环境信息化标准指南

3 术语和定义

GB/T 5271.8-2001 第八部分 安全 中确立的术语和定义，以及下列术语和定义适用于本标准。

3.1 信息系统 information system

用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员和组件的总和。

3.2 信息系统安全 information system security

使用合理安全措施保护信息系统中的信息在存储、处理或传输等过程中不会被未授权用户访问，并保障授权用户能够正常使用系统。

3.3 机密性 confidentiality

数据所具有的特性，表示数据所达到的未提供或未泄露给未授权的个人、过程或其它实体的程度。

3.4 完整性 integrity

保证信息及信息系统不会被有意地或无意地更改或破坏的特性。

3.5 可用性 availability

保证信息和通信服务能够按预期投入使用的特性。

3.6 安全域 security domain

一个逻辑范围或区域，在同一安全区域中的各信息单元具有相同或相近的安全等级或安全防护需求，安全服务的管理员定义和实施统一的安全策略。它是从安全策略的角度划分的区域。

3.7 威胁 threat

来自于信息系统外部的，能够通过未授权访问、毁坏、泄露、数据修改和/或拒绝服务对信息系统

造成潜在危害的任何环境或事件。

3.8 风险 risk

表现为一种可能性，由威胁发生的可能性、威胁所能导致的不利影响以及影响的严重程度共同决定。

4 保护对象

环境信息系统安全保护的对象包括国家环境保护业务专网范围内的信息网络、业务系统、环境信息及其物理环境、支撑性基础设施与安全设备设施等。

4.1 环境信息网络

环境信息系统安全保护的网络对象是国家环境保护业务专网范围内的各个信息网络，国家环境保护业务专网包括国家、省、地市、县四级，网络结构如图 1 所示。

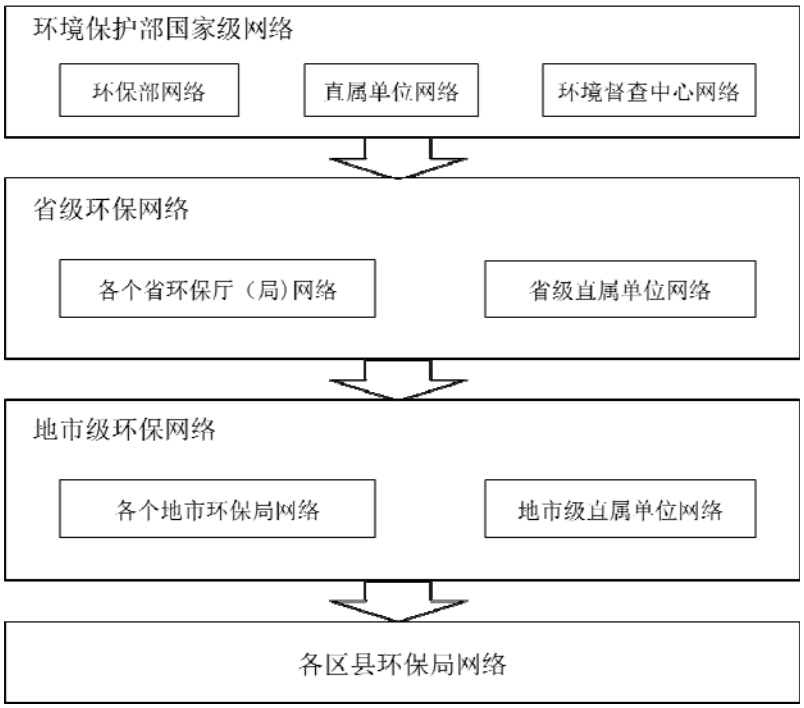

图 1 环境保护业务专网网络结构示意图

4.2 环境信息应用系统

环境信息系统安全保护的业务对象是环境信息系统中运行的各类环境业务应用系统，依据HJ511-2009，环境信息系统按业务应用类型可以分为环境保护核心业务应用系统和综合应用系统两大类，其中：

a) 环境保护核心业务应用系统包括环境监测管理、污染监控管理、生态保护管理、核安全与辐射管理、环境应急管理信息系统。各系统的作用分别为：

1) 环境监测管理信息系统用于实现对全国环境质量数据（包括环境空气、地表水、地下水、声环境、近岸海域、酸雨、沙尘暴等数据）的管理，并覆盖生态监测、污染源监测等业务；

2) 污染监控管理信息系统覆盖污染控制管理、环境监察管理以及环境影响评价和环境统计等业务；

3) 生态保护管理信息系统覆盖区域生态环境管理、农村环境保护管理、生物多样性保护等业务；

4) 核安全与辐射管理信息系统覆盖核设施与材料监督管理、放射源监督管理、辐射环境监测管理；

5) 环境应急管理信息系统覆盖环境应急指挥调度、环境应急监测管理、环境应急决策支持、

环境应急现场处置管理、环境突发事件后评估等业务。

b) 环境保护综合应用系统包括各类行政办公管理信息系统、环境保护政府网站、环境科技管理信息系统、环境政策法规管理信息系统、环境财务与资产管理信息系统和环境外事管理信息系统等综合性的、为核心业务应用系统提供支持与服务的应用系统。

4.3 环境信息

环境信息系统安全保护的信息对象是环境信息系统中的各类业务与办公信息，其中信息类型分为公开信息和部门信息两类，根据不同类别的信息应采取不同的保护措施，其中：

公开信息是在互联网上可以向公众完全开放的环境信息，对公开信息的保护应保证信息的完整性和可用性。

部门信息只限于各级环境保护部门人员访问，主要包括不宜公开的工作信息、政府的商业秘密、个人隐私等。部门信息分为部门公开信息和部门受控信息两种，部门公开信息允许所有各级环境保护部门人员访问，部门受控信需要经授权允许的各级环境保护部门人员才能访问。

5 安全目标

环境信息系统安全目标是保持环境信息系统的持续可用和可靠，为国家环境保护工作正常运行提供有力的支撑，保护环境保护信息系统中的信息网络、业务系统、环境信息及其物理环境、支撑性基础设施与安全设备设施等，防止来自内、外部的非法攻击与损坏。

环境信息系统安全建设应符合国家的信息安全规范的相关要求，遵照国家等级保护的相关规定，参考国际上的安全标准，并且以风险防范为核心加强环境信息安全保护建设。环境信息系统中有关安全保密问题应遵守国家保密相关规定。

6 安全总体架构

环境信息系统安全保障体系在风险评估的基础上，通过安全管理体系、安全技术体系的建设实现不同等级保护对象、不同安全域的安全保护。环境信息系统安全保障体系见图 2。

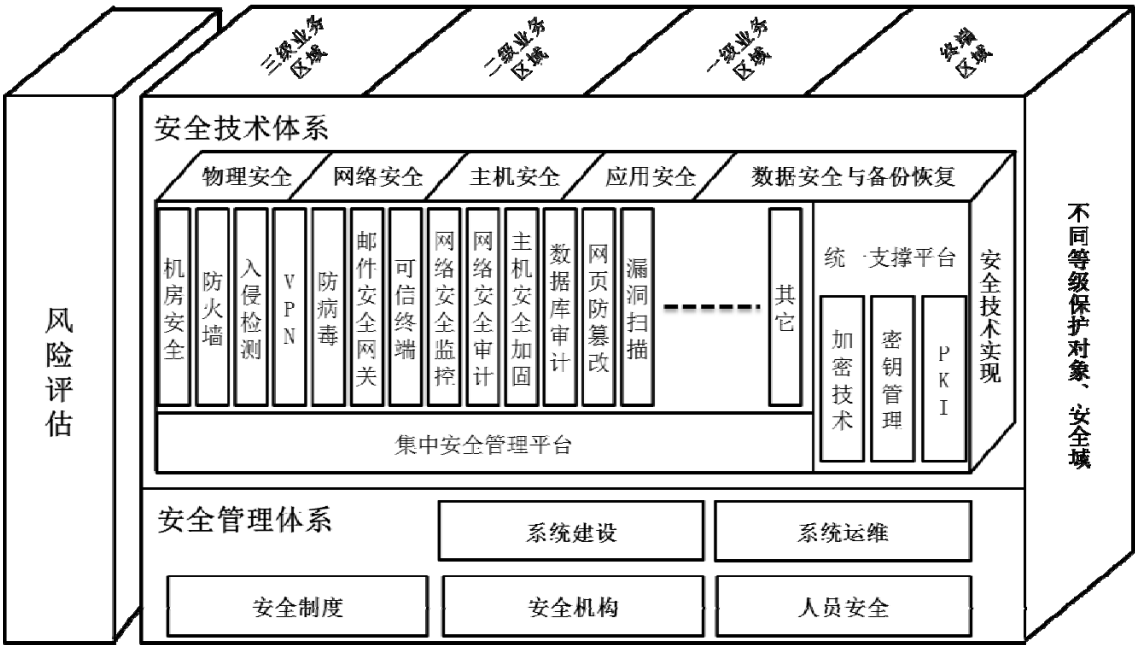

图 2 环境信息系统安全保障体系

安全管理体系建设应在信息系统建设和信息系统运行维护阶段进行，包括安全制度、安全机构、人员安全的建设；安全技术体系应包含物理安全、网络安全、主机安全、应用安全、数据安全与备份恢复，安全技术体系建设应重视发展统一支撑平台、各类安全技术与产品以及集中安全管理平台的建设。

本标准是在国家等级保护基本要求的基础上提出的环境信息系统的安全保障性的技术要求，其中包括物理安全、网络安全、主机安全、应用安全、数据安全与备份与恢复、信息系统建设、信息系统运维的安全要求，其中终端与办公安全按附录 A 执行。各环境信息系统在安全建设过程中按附录 B 中的相应级别的安全要求实施安全保护。

7 信息安全保护方法

7.1 环境信息系统的特点

依据环境保护的工作特点，环境信息系统具有一些特殊安全要求，在安全建设过程中应考虑以下方面的特点：

a） 为满足环境监测、环境统计、生态监测等业务需要，用于环境监测业务的信息网络、系统及设施应考虑移动监测、远程操作及办公等方面的安全要求；

b） 针对环境保护业务中核安全与辐射管理的信息系统，应当实施更加严格的安全技术措施；

c） 处理环境事件的环境应急的应急执法、应急指挥类的信息系统与设施应加强安全保障方面的建设，增强业务可靠性保护；

d） 国家环境保护业务专网依据业务的需要，可能与其它信息系统、网络、应用之间互联互通，应通过严格的安全技术与管理措施保证外部接入的信息系统不会对国家环境保护业务专网造成不良的影响；

e） 包括环境监测、环境统计、环境评价、基础地理信息等在内的环境业务信息是环境保护业务基础，应当对相关的数据实施安全保护，保证数据安全。

对于环境保护业务特有的业务系统的安全保护，在实施国家等级保护的基础上，应通过信息安全风险评估识别风险因素，采取有针对性安全保护措施。

7.2 环境信息系统安全建设要求

环境信息系统建设应符合 GB/T 22240-2008 的要求，正确划分环境信息系统安全等级，并按照等级保护的要求开展设计、建设、运行和维护的工作。

环境信息系统安全建设应遵循 GB/T 17859-1999、GB/T 20271-2006 和 GB/T 22239-2008 的相关规定。

应根据环境信息的重要程度和不同类别，采取不同的保护措施，实施分类防护；根据信息系统和数据的重要程度，进行分域存放，实施分域保护和域间安全交换，实施分域控制。

依据国家等级保护的相关要求，环境信息系统不允许存储、传输、处理国家秘密信息。

7.3 安全建设实施方法

依据等级保护的相关要求，实施环境信息系统安全建设的方法是：

a） 依据信息安全等级保护的定级规则，确定环境信息系统的安全等级；

b） 按照信息安全等级保护要求，确定与信息系统安全等级相对应的基本安全要求；

c） 依据信息系统基本安全要求，并综合环境信息系统安全技术要求、信息系统所面临风险和实施安全保护措施的成本，进行安全保护措施的定制，确定适用于特定环境信息系统的安全保护措施，并依

照本规范相关要求完成规划、设计、实施、验收和运行工作。

7.4 安全建设实施过程

环境信息系统安全建设的实施过程包括定级阶段；规划与设计阶段；实施、等级评估与改进阶段。

7.4.1 第一阶段：定级

定级阶段主要包括两个步骤：

a） 信息系统识别与描述

清晰地了解环境信息系统，根据需要可将复杂的环境信息系统分解为环境信息子系统，描述系统和子系统的组成及边界。

b） 等级确定

环境信息系统的信息安全等级保护工作实行行业指导、属地管理。环境保护部及直属单位、各省级环境保护厅（局）按照国家信息安全等级保护制度有关要求，负责本区域相关信息系统安全等级保护工作的指导和管理。按照“谁主管、谁负责，谁运营、谁负责”的原则确定信息安全责任。

各个单位等级保护对象的确定、受侵害的客体和严重程度的判定、最终等级的认定等定级工作依据GB/T 22240-2008中要求的过程的标准执行。

环境信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。等级保护对象受到破坏时所侵害的客体包括：公民、法人和其他组织的合法权益；社会秩序、公共利益；国家安全三个方面。

对客体的侵害程度由客观方面的不同外在表现综合决定。由于对客体的侵害是通过对等级保护对象的破坏实现的，因此，对客体的侵害外在表现为对等级保护对象的破坏，通过危害方式、危害后果和危害程度加以描述。等级保护对象受到破坏后对客体造成侵害的程度归结为：造成一般损害；造成严重损害；造成特别严重损害的三种情况。

定级要素与环境信息系统安全保护等级的关系如表1所示。

表1 定级要素与安全保护等级的关系

业务信息或系统服务受到破坏时受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

作为定级对象的环境信息系统的安全保护等级由业务信息安全等级和系统服务安全等级的较高者决定。

7.4.2 第二阶段：规划与设计

规划与设计阶段主要包括三个步骤，分别为：

a） 信息系统分域保护框架建立

通过对环境信息系统进行安全域划分、保护对象分类，建立环境信息系统的分域保护框架。

b） 选择和调整安全措施

根据环境信息系统和子系统的安全等级，选择对应等级的基本安全要求，并根据风险评估的结果，综合平衡安全风险和成本，以及各信息系统特定安全要求，选择和调整安全措施，确定出环境信息系统、子系统和各类保护对象的安全措施。

c） 安全规划和方案设计

根据所确定的安全措施，制定安全措施的实施规划，并制定安全技术解决方案和安全管理解决方案。

7.4.3 第三阶段：实施、等级评估与改进

实施、等级评估与改进阶段主要包括三个步骤，分别为：

a） 安全措施的实施

依据安全解决方案建设和实施等级保护的安全技术措施和安全管理措施。

b） 评估与验收

按照等级保护的要求，选择相应的方式来评估信息系统是否满足相应的等级保护要求，并对等级保护建设的最终结果进行验收。

c） 运行监控与改进

运行监控是在实施等级保护的各种安全措施之后的运行期间，监控信息系统的变化和信息系统安全风险的变化，评估信息系统的安全状况。如果经评估发现信息系统及其风险环境已发生重大变化，新的安全保护要求与原有的安全等级已不相适应，则应进行信息系统重新定级。如果信息系统只发生部分变化，例如发现新的系统漏洞，这些改变不涉及信息系统的信息资产和威胁状况的根本改变，则只需要调整和改进相应的安全措施。

对于大型环境信息系统，等级保护过程可以根据实际情况进一步加强和细化，以满足其复杂性的要求。附录 C 给出了大型环境信息系统安全建设实施过程的示例。

7.5 安全建设与信息系统生命周期关系

新建环境信息系统与已经建成的环境信息系统在等级保护工作的切入点是不相同的，它们各自的切入点以及与信息系统生命周期的对应关系如图 3 所示。

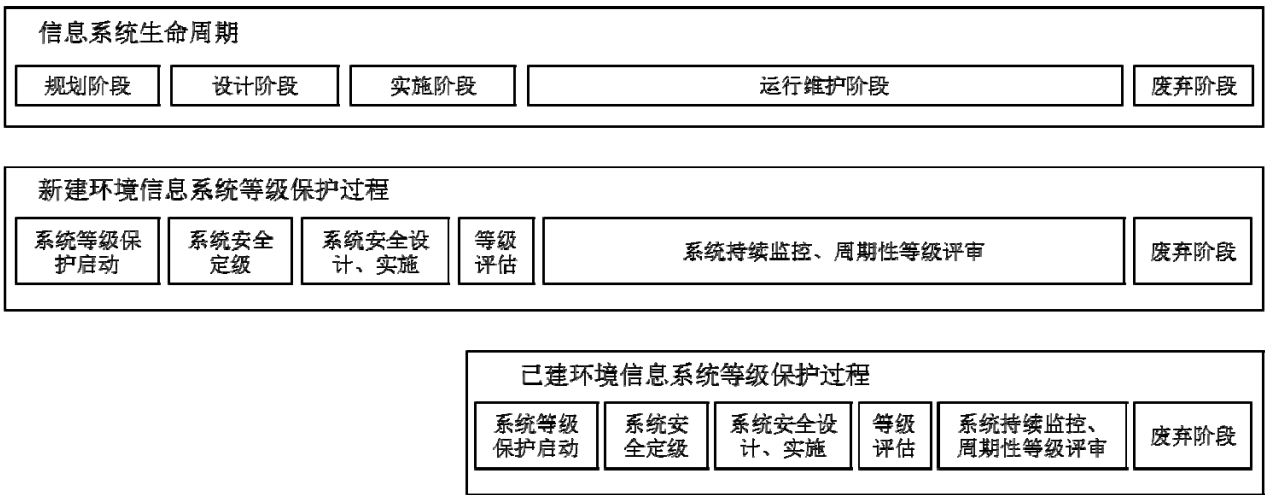

图 3 等级保护过程与新建和已建信息系统生命周期对应关系

对于新建的环境信息系统，等级保护工作的切入点应是信息系统规划阶段。

a） 信息系统规划阶段，应分析并确定所建环境信息系统的安全等级，并在项目建议书中对环境信息系统的安全等级进行论证；

b） 信息系统设计阶段，要根据所确定的信息系统安全等级，设计信息系统的安全保护措施，并在可行性分析中论证安全保护措施；

c） 信息系统实施阶段，要与信息系统建设同步进行信息安全等级保护体系的实施，之后进行等级评估和验收；

d） 信息系统运行维护阶段，要按照所建立的等级保护体系的要求，进行安全维护与安全管理；

e） 信息系统废弃阶段，要按照所建立的等级保护体系的要求，对废弃过程进行有效的安全管理。

对于已建的环境信息系统，等级保护工作的切入点应是信息系统运行维护阶段。

在确定要实施等级保护工作之后，应对环境信息系统进行安全现状分析，对每个信息系统进行定级，之后进行等级保护的安全规划和方案设计，最后进行实施、评估和验收。

7.6 环境信息系统间互联互通

不同安全等级的环境信息系统之间可以根据业务需要进行互联互通。不同安全等级的环境信息系统进行互联互通时，要根据信息系统业务要求和安全保护要求，制定相应的互联互通安全策略，包括访问控制策略和数据交换策略等。要采取相应的边界保护、访问控制等安全措施，防止高等级信息系统的安全性受到低等级信息系统的影响。各环境信息系统间的互联互通应遵循以下要求：

a） 同等级环境信息系统之间的互联互通

由各信息系统的运营单位参照该等级对访问控制的要求，协商确定边界防护措施和数据交换安全措施，保障环境信息系统间互联互通的安全。

b） 不同等级环境信息系统间的互联互通

各信息系统在按照自身安全等级进行相应保护的基础上，协商对相互连接的保护。高安全等级的信息系统要充分考虑引入低安全等级信息系统后带来的风险，采取有效措施进行控制。

c） 环境信息系统互联互通中有关密码的部分，按照国家密码管理部门的要求执行。

8 物理安全

物理安全是环境信息系统安全保护的一个重要方面，应通过安全防护措施使得机房、网络基础设施、信息系统等免受非法的物理访问、自然灾害和环境危害。

8.1 物理安全区域控制

应通过建立物理安全区域并实施相应的控制措施，对机房、网络、信息处理设施进行全面的物理保护。应根据不同的安全保护需求，划分不同的安全区域，实施不同等级的安全管理。

8.1.1 安全区域边界

应通过在边界设置物理隔离装置来实现安全区域的物理保护，装置的位置和强度应适合于安全区域的重要程度。

各个安全区域的边界应有明确标志，如机房、办公区、安全通道等。

只有通过申请和审批流程获得授权的人员才能访问内部安全区域。

安全边界上所有应急通道的出入口平时都应关闭，并设置报警装置。

8.1.2 安全区域出入控制

进入安全区域的外来人员应通过检查并接受监督，进入和离开安全区域的时间应有记录。

机房等重要安全区域应使用电子门禁系统，所有访问活动应事先进行申请和授权，并保存审计记录。

进入重要安全区域的所有内、外部人员都应佩戴明显的、可视的身份识别证明。

机房安全区域的访问权限应定期进行审查和更新。

8.1.3 安全区域物理保护

机房安全区域内物理保护措施的选择和设计应考虑到应对火灾、洪水、雷击、爆炸、骚乱及其它自

然或人为灾害导致的破坏，还应遵照相关的安全标准，如 GB/T 50174-2008，并防范周边的安全威胁。

所有重要的环境信息网络与信息处理设施（例如：通信设备、主机与网络设备等）应置于公众无法进入的场所。

常用的办公设备，如复印机、传真机等，应放置在合适的办公安全区域内，减少无关人员接触，避免信息的泄露。

对于无人值守机房，所有门窗都应关闭，建筑物底层的窗户应设置外部防护。

机房内应安装防盗、防火、监视系统等安全设施，机房内未使用区域的告警装置也应开启。

机房等安全区域应远离危险或易燃物品，安全区域内不应存放大量的、短期内不使用的材料或物品。

备用设备和备份介质应放置在远离主安全区域的备用场所内，以防主安全区域发生灾难时可能造成的破坏。

8.2 物理设施安全

环境信息系统中的网络、基础设施、信息处理设施应妥善放置，加强保护以降低环境因素带来的风险，并且防止非法访问。

8.2.1 设备物理保护

对设备的物理保护应采取以下控制措施：

a) 应对温湿度等有可能对信息处理设施造成不良影响的环境条件进行监控；
b) 需要特殊保护的设备应与其它设备隔离，以降低整个区域内所需的安全保护级别；
c) 处于特殊环境下的设备，应考虑采用特殊的保护方法，如在工业环境里，应采用防爆灯罩、键盘隔膜等。

8.2.2 电力保护

可靠的电力供应是保证网络与信息处理设施可用性的必要条件，应采取以下措施确保供电安全：

a) 电源应符合国家标准 GB/T50052-2009 的要求；
b) 应采用多种供电方式如：多路供电、配备 UPS、备用发电机等方法，避免电源单点故障；
c) 定期维护和检查供电设备，UPS 应有充足容量，发电机应配备充足的燃料；
d) 如进行有计划的停电，停电计划应提前通知有关部门，防止无准备的断电造成不必要的损失。

8.2.3 线缆安全

通信电缆和电力电缆被损坏或信息被截获，会破坏网络与信息资产的机密性和可用性，应采取以下控制措施对线缆进行保护：

a) 应使用电缆管道布放线缆，且避免线缆经过公共区域；
b) 电力电缆应与通信电缆分离，避免互相干扰；
c) 应定期对电缆线路进行维护、检查和测试，及时发现故障隐患。

8.2.4 工作区外设备的安全

环境信息系统中工作区外的设备包括带离工作区的信息处理设备和固定在公共场所的设备，应根据工作区域外设备面临的安全风险，制定相应的保护措施，安全要求如下：

a) 应至少达到工作区内相同用途设备的安全保护级别；
b) 各类在线监测设备应确保 24 小时不间断的安全监控。

9 网络安全

9.1 网络访问控制

应对访问网络的行为进行控制，应确保接入网络的用户不会破坏网络的安全性，其基本要求如下：

a) 在环境保护业务专网与相关企事业单位的网络之间、环境保护业务专网与公共网络之间应设置安全的访问控制设备；

b) 安全访问控制设备应采取有效的用户和设备验证机制。

9.1.1 网络服务安全策略

应防止不安全的网络连接影响环境保护部门网络的安全，因此环境保护业务专网内的内网用户和公网用户都只能使用经过授权的网络服务。应制定有关网络及网络服务的使用策略，并与访问控制策略保持一致。具体策略应规定以下内容：

a) 应明确用户允许访问的网络和网络服务；

b) 应规定对用户访问网络和网络服务进行授权的程序；

c) 应具有对网络连接和网络服务的访问进行保护的管理控制措施和程序；

d) 应保留对网络服务的访问日志，并根据信息的敏感程度确定日志的具体内容。

9.1.2 逻辑安全区域的划分与隔离

应基于访问控制策略和访问需求，根据不同的业务、应用及其所处理信息的敏感性和重要性，并按国家信息安全等级保护要求，将网络与信息系统划分成不同的逻辑安全区域。

应根据保护等级的要求，采取重点防护、边界隔离的办法，重点加强安全域关键边界的安全保护和监控。同时通过隔离措施，过滤域间业务，控制域间通信。

应根据各安全区域的安全风险、防护等级确定不同网络访问控制的安全技术要求和安全管理要求。

9.1.3 外部连接用户的验证

用户通过外部网络访问环境保护业务专网的网络时必须接受验证。各类外部网络连接所需的保护级别应通过风险评估来确定，且不同的环境要求采用不同的验证方式。

无线网络应视作外部网络，用户通过无线网络访问环境保护业务专网时应符合以下标准：

a) 必须采用经过批准的无线接入方式；

b) 必须接受身份验证；

c) 必须使用符合安全标准的通信终端；

d) 传送敏感信息时必须进行加密。

9.1.4 端口保护

应制定并实施有效的安全控制措施，保护网络与信息系统的远程诊断、操作、维护、管理等功能所使用的端口，防止端口被未经授权或非法的访问，并记录各端口的访问日志。

9.1.5 网络接入控制

应基于业务应用的访问策略和要求，采取措施控制网络接入，由于环境数据采集等业务要求的外部网络接入的基本控制要求如下：

a) 网络互联应基于业务需求；

b) 应明确定义允许和禁止接入专网的网络；

c) 应在边界处通过安全网关按照预设的规则过滤网间通信；

d) 在网络边界处应采取限制措施限制电子邮件、文件传输、交互式访问等具体应用；

e) 外部设备接入专网时应部署相应的网络接入控制策略。通过认证的设备可以接入内络，没有通过认证的拒绝接入专网；
f) 通过认证的外部设备在接入专网前必须安装防病毒软件，并定期进行补丁更新。对移动存储设备接入时应开启对病毒、木马的自动查杀的功能；
g) 对需要接入专网的外部设备应进行安全漏洞及风险扫描，并对所出现的问题进行安全加固。

9.1.6 网络路由控制

应实施路由控制，确保网络连接和信息流符合访问控制策略。路由控制应基于源地址和目标地址检查机制，可使用网络地址转换（NAT）来隔离内部与外部网络，应阻止网间传播不必要的路由信息。

9.2 网络操作流程与职责

为确保网络与信息处理设施的正确和安全使用，应建立所有网络与信息处理设施管理与操作的流程和职责，包括制定操作细则和事件处理流程。应落实责任与分工，减少疏忽和蓄意的系统滥用风险。

9.2.1 技术操作要求

应制定网络与信息处理设施的技术操作规范，技术操作规范涵盖以下内容：
a) 应规定对信息的处理和信息载体的处置操作规范；
b) 应规定进行操作的时间和进度的要求，考虑同其它系统的相关性；
c) 应规定操作过程中发生非预期的错误或出现其它异常情况时的指导说明；
d) 应规定意外的操作困难或技术难题出现时的支持人员；
e) 应规定故障情况下系统的重启和恢复程序；
f) 应规定系统维护的相应程序，按操作规范实现主要设备的启动/停止、加电/断电、备份/恢复等操作。

9.2.2 设备维护要求

正确规范地维护网络设备，可以保护设备的可用性和完整性，网络设备维护的安全要求如下：
a) 应根据网络设备原厂商建议的维护周期和规范进行维护；
b) 设备维护人员应具备相应的技术技能；
c) 应储备一定数量的备品备件；
d) 所有日常维护和故障处理工作都应记录在案；
e) 当网络设备送到外部场所进行维护时，应采取控制措施防止信息泄露；
f) 系统关键设备应冗余配置；
g) 关键部件在达到标称的使用期限时，不管其是否正常工作，必须予以更换。

9.2.3 变更控制

网络的变更包括：网络结构、安全策略的调整，硬件的增减与更换等。任何变更必须经过授权，并接受变更测试。变更控制安全要求如下：
a) 识别并记录重大变更；
b) 评估进行变更的潜在影响；
c) 明确变更失败的恢复措施和责任；
d) 保留所有与变更相关信息的日志记录。

9.2.4 开发、测试与运行设备的分离

前期开发调试设备与运行中的设备应实现物理分离或逻辑分离，应设置独立的实验环境。后期在运

行环境中进行测试时，应做好安全防护，并对测试过程进行安全检查。

9.3 网络传输安全

网络传输安全方面应采取以下的安全措施：

a) 应采取 SSL、IPSec 等加密控制措施，保护通过公共网络传输的数据的机密性和完整性；

b) 应对网络安全状态进行持续监控，并对有关错误、故障和补救措施进行记录。

9.4 网络安全审计与监控

应对网络访问和使用情况进行审计和监控，以检测违反访问控制策略的活动，并记录相关证据。网络监控可以提高控制措施的有效性，并保证访问控制策略的执行。

9.4.1 网络安全事件记录

应建立审计日志，记录网络异常情况、身份鉴别失败事件及其它安全事件。审计日志应保留规定的时长，以便支持以后的事件调查和访问控制审核。审计日志应包括以下内容：

a) 用户标识与事件类型；

b) 登录和退出的日期和具体时间；

c) 成功的和被拒绝的系统访问活动的记录；

d) 成功的和被拒绝的数据与其它资源的访问记录。

9.4.2 监控系统

应对网络的使用进行监控。具体监控内容应包括：

a) 授权接入操作；

b) 所有特殊操作；

c) 未经授权的访问尝试；

d) 系统告警或故障。

9.4.3 日志审查

应对日志进行自动筛选以获取有用信息，或使用分析工具进行检索查询。在进行日志审查时，被审查人员不应参与，以维护审计独立性。

9.5 网络设备安全管理

9.5.1 设备安全管理要求

网络设备安全管理应遵循以下基本要求：

a) 设备管理权限除非明确许可，否则必须禁止；

b) 应明确限定设备管理权限的变更，包括系统自动生效的变更和管理员批准生效的变更；

c) 访问控制规则需经管理人员审查批准方可执行；

d) 应依照每个系统的安全要求制定访问控制策略；

e) 应依照与该系统相关的业务信息的类型制定访问控制策略。

9.5.2 设备安全管理措施

应基于以下内容确定环境信息系统及网络设备的安全措施：

a) 在所有的网络与信息设备上，应配备、应用并维护安全控制机制；

b) 系统中的安全产品必须能够提供验证用户身份的手段；应根据不同的系统和应用，提供不同深

度、不同层次及不同强度的认证手段；

c) 安全控制措施必须能够防止对用户认证数据的非法访问；

d) 备份软件、管理工具、数据库自动查询等只能由特殊功能帐户运行的软件，以及能够建立特殊权限帐户的软件，只能由内部专业的授权人员安装、测试和执行，以确保此类软件只能执行授权功能；

e) 应规定可以使用的安全软件和特权的管理工具及使用范围，其使用必须经过批准并记录，在日志中记录其操作过程；

f) 所有系统和安全工具都必须对管理员帐户的口令采取保护措施，管理员帐户的默认口令必须在产品安装过程中进行修改；

g) 所有接入环境保护业务专网的系统必须接受环境保护部门的管理，应对接入网络进行安全的监控和入侵测试。

10 主机安全

10.1 身份鉴别

10.1.1 用户注册

针对多用户使用的网络与信息系统应设定正式的注册和注销程序，对用户的访问权限进行控制。用户注册基本要求包括：

a) 每个用户应使用唯一的用户标识符，用户与其操作相关联，并对其行为负责；

b) 因业务需要时允许使用用户组，但应采取更加严格的控制措施；

c) 授权用户访问的级别应基于业务目的，且符合安全策略，用户授权应遵循最小授权原则；

d) 用户访问权限应得到上级批准；

e) 应及时修改或注销已经转岗或离职用户的访问权限；

f) 定期核查并删除多余、闲置或非法的帐户。

10.1.2 超级权限的管理

超级权限帐户应能进行设置，并可修改口令，超级权限的使用和分配必须受到严格限制。

必须通过正式的授权程序控制超级权限的分配，做好超级权限拥有者无法行使职责时的应急安排，应有角色备份。

10.2 操作系统访问控制

操作系统应提供以下访问控制功能：

a) 验证用户身份；

b) 记录所有系统访问日志；

c) 应限制用户连接时间。

10.2.1 用户识别和验证

所有用户都应具有唯一用户标识符，以便追溯，责任到人。因业务需要时可以共享用户标识，但必须经过授权，并采取其它方法来保证责任到人。

依据不同等级保护的要求，验证方式可以基于口令、令牌、指纹、虹膜等多种因素的身份验证机制。

10.2.2 连接时间限制

应限制终端与主机的网络服务的连接时间，以降低非法接入的风险，具体限制措施如下：

a) 应使用预先定义的时间段进行通信；

b） 应对每次连接的时长进行限制。

10.2.3 日志审核

系统应保留日志记录，分析重复性登录失败、连续的访问尝试等信息以确定可疑事件。日志至少应记录以下内容：

a） 事件发生的日期和起止时间；
b） 用户标识或者计算机帐户；
c） 事件的类型及其结果（成功或失败）；
d） 事件来源（如端口和地址等）。

系统管理员应明确日志审核频率、定义安全事件判断规则、规定安全事件通报流程，对日志进行审核，发现并确定安全事件，应记录重大安全事件。

10.3 主机操作流程与职责

10.3.1 主机操作要求

应制定主机的技术操作规范，技术操作规范涵盖以下内容：

a） 应规定对信息的处理和信息载体的处置操作规范；
b） 应规定进行操作的时间和进度的要求，考虑同其它系统的相关性；
c） 应规定操作过程中发生非预期的错误或出现其它异常情况时的指导说明；
d） 应规定意外的操作困难或技术难题出现时的支持人员；
e） 应规定故障情况下系统的重启和恢复程序；
f） 应规定系统维护的相应程序，按操作规范实现主要设备的启动/停止、加电/断电、备份/恢复等操作。

10.3.2 主机维护要求

正确规范地维护主机设备，可以保护设备的可用性和完整性，主机设备维护的安全要求如下：

a） 应根据主机设备原厂商建议的维护周期和规范进行维护；
b） 设备维护人员应具备相应的技术技能；
c） 应储备一定数量的备品备件；
d） 所有日常维护和故障处理工作都应记录在案；
e） 当主机设备送到外部场所进行维护时，应采取控制措施防止信息泄露；
f） 系统关键设备应冗余配置；
g） 关键部件在达到标称的使用期限时，不管其是否正常工作，必须予以更换。

10.3.3 变更控制

主机的变更包括：全局数据、安全策略、参数的调整，硬件的增减与更换，软件版本与补丁的变更，处理流程的改变等。任何变更必须经过授权，并接受变更测试。变更控制安全要求如下：

a） 识别并记录重大变更；
b） 评估进行变更的潜在影响；
c） 明确变更失败的恢复措施和责任；
d） 变更成功与失败回退操作完成后的验证测试；
e） 保留所有与变更相关信息的日志记录。

10.4 软件及补丁管理

在系统运行过程中应及时维护与更新软件及补丁版本，在软件或补丁的使用方面的安全要求如下：

a) 应选择稳定运行的软件版本，不应立即使用厂商发布的最新版本，但病毒代码库和系统漏洞库例外；
b) 厂商发布的安全补丁应先进行功能测试，通过功能测试后投入应用；
c) 无法按时完成安全补丁修补时，应采取临时应对措施，明确后续工作计划；
d) 所有软件的升级必须按流程执行。

10.5 时钟和时间同步

监测、审计等安全措施需要保证时间同步，因此要求采用统一的时钟服务器和时间源系统，并根据安全策略要求定时进行同步。

10.6 系统安全监控

应对系统访问和使用情况进行监控，以检测违反访问控制策略的活动，并记录相关证据。系统监控可以提高控制措施的有效性，并保证访问控制策略的执行。

10.6.1 系统事件记录

应建立审计日志，记录系统异常情况、身份鉴别失败事件及其它安全事件。审计日志应保留规定的时长，以便支持以后的事件调查和访问控制审核。审计日志应包括以下内容：

a) 用户标识与事件类型；
b) 登录和退出的日期和具体时间；
c) 系统访问活动的记录；
d) 数据与其它资源的访问记录。

10.6.2 监控系统

应对主机系统、数据库系统的使用进行监控。具体监控内容应包括：

a) 授权接入操作；
b) 所有特殊操作；
c) 未经授权的访问尝试；
d) 系统告警或故障。

10.6.3 日志审查

应对日志进行自动筛选以获取有用信息，或使用分析工具进行检索查询。在进行日志审查时，被审查人员不应参与，以维护审计独立性。

10.7 恶意代码的防范

系统运行过程中应防止恶意软件的破坏，主要措施包括：

a) 应制定软件使用政策，遵守软件许可协议，禁止使用非法软件；
b) 通过互联网或不明来源获取的文件和软件，应采取防护措施；
c) 应安装并定期更新防病毒软件和补丁程序；
d) 应定期检查支持关键业务系统的软件和数据，发现任何未经批准的文件或者未经授权的修改，并进行调查；
e) 应检查所有来源不明和来源非法的存储介质上的文件、通过外部网络接收的文件，以确认是否

含有恶意软件；

f) 应检查所有电子邮件的附件及下载内容是否含有恶意软件，应在用户端和电子邮件服务器端进行检查；

g) 应进行用户安全教育和培训，进行恶意软件攻击通报，制定系统恢复的管理程序，落实相关责任；

h) 应从权威发布部门接收恶意软件相关信息，对可疑问题应及时上报。

11 应用安全

11.1 身份鉴别

11.1.1 口令管理

口令管理应符合以下基本要求：

a) 所有口令的信息均为保密信息；

b) 当系统向用户提供临时口令时，应确保提供安全的初始口令，并要求用户限期修改；当用户忘记口令时，系统应在正确识别用户身份后才能向用户提供重置的临时口令；

c) 应以安全方式向用户提供临时口令，禁止使用明文的电子邮件等未经保护的方式传递，并要求用户确认接收到临时口令；

d) 口令应以加密方式存入用户数据库，通过加密、解密方式实现其存储、读取。

11.1.2 用户访问权限审核

应定期审核用户的访问权限并记录，用户访问权限审核的基本要求如下：

a) 用户访问权限应由管理人员、系统责任人及系统维护人员共同确认；

b) 用户帐户、特殊权限帐户、超级权限帐户的访问权限应定期检查；

c) 发生非法入侵事件、发生人员变动后应进行审核；

d) 对审核中发现的问题，应采取必要措施予以纠正。

11.2 应用访问控制

为避免应用系统中的信息受到非法访问，应用系统应具备如下安全功能：

a) 应根据访问控制策略，控制用户访问应用系统和信息；

b) 应防止用户在未经授权的情况下使用能够超越系统或应用控制措施的工具和系统软件；

c) 只有系统所有人和授权用户可以对应用系统中的信息进行访问；

d) 应用系统对共享信息资源的访问不应威胁到其它系统的安全；

e) 应确保处理敏感信息的应用系统只输出必要信息，而无任何多余信息，输出结果只能被发送至授权的终端，并且应定期检查此类输出。

11.3 应用系统交互的完整性

为避免应用系统中的用户数据丢失、修改和误用，应用系统应设计有适当的控制措施、审计跟踪记录或活动日志，应对输入数据、内部处理和输出数据进行验证。针对处理敏感或关键资产的系统还应根据风险评估的结果确定安全要求，并采取增强的控制措施。

11.3.1 输入数据验证

输入到应用系统中的数据应进行验证，以确保其正确性及适用性，避免无效数据对系统造成危害。对输入数据的验证一般通过应用系统本身及其它辅助管理手段来实现，并应在系统开发中实现输入数据验证功能。具体验证方法如下：

a） 在进行口令修改等输入操作时，要求双重输入，并要确认两次输入的口令一致才接受修改；
b） 建立用于响应输入错误的程序；
c） 建立用于测试输入数据真实性的程序。

11.3.2 内部处理控制

已被正确输入的数据可能受到错误处理或者故意破坏，系统应采取有效的验证检查措施来检测此类破坏，并在应用系统设计时引入数据处理控制，尽可能地减小破坏数据完整性的危险。应采取的控制措施如下：

a） 不应在程序或进程中固化帐户和口令；
b） 应具备对口令猜测的防范机制和监控手段；
c） 应避免应用程序以错误的顺序运行，防止出现故障后程序以不正常的流程运行；
d） 采用正确的故障恢复程序，确保正确处理数据；
e） 采取会话控制或批次控制，确保更新前后数据文件状态的一致性；
f） 检查执行操作前后对象是否正常；
g） 验证系统生成的数据；
h） 检查上传、下载的数据或软件的完整性；
i） 检查文件与记录是否被篡改。

11.3.3 输出数据验证

应用系统的输出数据应被验证，以确保数据处理的正确性与合理性。输出数据验证要求如下：

a） 应验证输出数据在规定的赋值范围内；
b） 输出数据应为用户或后续处理系统提供充足的信息，以确定信息的准确性、完整性、精确性和分类级别；
c） 应具有可以用来验证输出数据的测试程序。

11.4 通信加密技术控制措施

加密技术可用来保护信息的机密性和完整性，防止信息被泄露或篡改，也可用于身份验证和防止抵赖。

11.4.1 加密技术使用策略

应在风险评估的基础上制定加密技术使用策略，使加密技术的应用达到有效控制风险的目的，避免不当或错误使用。

应通过风险评估确定是否采用以及采用何种加密技术控制措施、控制目的和控制对象，加密技术使用策略应包含以下内容：

a） 应具有密钥管理方法，在密钥丢失、泄露或损坏时恢复信息原文；
b） 应具有策略实施、密钥管理的相关岗位和职责；
c） 应能正确确定合适的加密保护级别。

11.4.2 使用加密技术

在选择和应用加密技术时，应考虑以下因素：

a） 必须符合国家有关加密技术的使用和进出口限制等方面的法律法规；
b） 根据风险评估确定保护级别，并以此确定加密算法的类型、属性，以及所用密钥的长度；
c） 选择能够提供所需保护的合适的加密产品，加密产品应能实现安全的密钥管理；
d） 一般的数据压缩技术不得代替安全手段。

11.4.3 数字签名

在使用数字签名技术时，应基于以下要求：

a) 应充分保护私钥的机密性，防止窃取者伪造密钥持有人的签名；

b) 应使用公钥证书保护公钥完整性；

c) 用于数字签名的密钥应不同于用来加密内容的密钥；

d) 应符合有关数字签名的法律法规。

11.4.4 抗抵赖服务

应根据加密技术使用策略，明确必须使用抗抵赖服务的业务和情况，及相应的加密和数字签名技术。

11.4.5 密钥管理

应采取加密等安全措施来有效保护密钥，以免密钥被非法修改和破坏；应对生成、存储和归档保存密钥的设备采取物理保护。必须使用经过批准的加密机制进行密钥分发，并记录密钥的分发过程，以便审计跟踪。

为了降低泄露的可能，密钥应指定确切的密钥生存期，使之只在生存期内有效。生存期的长短取决于使用环境及加密技术。

应与外部加密服务提供商签订服务协议或合同，其中应涵盖责任、服务可靠性以及服务响应时间等安全要求。

11.5 应用系统安全管理

11.5.1 应用程序的部署及更新

在操作系统中运行软件应得到有效的控制。为了最大限度地降低操作系统遭受破坏的风险，应考虑采取如下控制措施：

a) 应用程序的软件版本升级或数据更新只能由指定的管理员在获取授权后完成；

b) 运行应用程序的操作系统中应只保留应用程序的可执行代码；

c) 历史版本的软件应予以保留，用作应急措施；

d) 任何应用程序的版本更新都应考虑安全性，应采用软件补丁消除或削弱安全缺陷；

e) 操作系统的软件版本更新，有可能对应用系统带来影响，应对应用系统进行兼容性测试。

11.5.2 测试数据的保护

应对系统测试数据加以保护和控制，并避免使用含有个人隐私或敏感信息的数据去测试系统，确保测试数据的普遍性。可采用如下的控制措施：

a) 用于正式运营系统的访问控制程序，也应用于测试环境；

b) 避免使用实际运营中的真实数据进行测试，测试中应对含有的个人隐私数据进行模糊化处理；

c) 在测试结束后，测试数据应马上从测试系统中删除；

d) 测试数据的加载和使用应进行记录，以便检查跟踪。

11.5.3 应用系统源代码安全

为降低应用系统程序遭受破坏的可能性，应严格控制对应用系统源代码的访问，具体控制措施如下：

a) 应用系统源代码不应保留在操作系统内；

b) 应用系统开发过程中源代码版本应有严格的控制，对源代码的访问权限应实现分级访问控制；

c) 应用系统程序源代码应保存在安全环境中；

d) 对应用程序源代码的所有访问都应保留审计日志；

e) 应用程序源代码的维护和拷贝应遵从严格的变更控制程序。

12 数据安全与备份恢复

12.1 数据备份策略

应根据系统的重要程度，制定数据与软件的备份策略，对备份策略应采用如下控制措施：

a) 备份策略应包含系统和数据的名称、备份的频率和类型（全部备份/增量备份等），以及备份介质类型和所用备份软件、异地存放周期以及制定备份方案的实施原则等；
b) 备份操作应安排在不影响业务的时间段里，严格遵照备份策略执行；
c) 重要的业务系统应至少保留两个版本或两个备份周期的备份信息，备份信息应包含完整的备份记录、备份拷贝、恢复程序文档和清单；
d) 为尽快恢复故障，应在本地保留备份信息，同时为了避免主场所的灾难所导致的破坏，还应进行异地备份；
e) 应定期检查和测试备份信息，保持其可用性和完整性，并确保在规定的时间内完成恢复工作；
f) 应明确规定备份信息的保留时间。

12.2 数据备份内容与频率

应对重要的系统、数据及应用进行备份，备份的范围包括操作系统备份、数据库备份和应用系统备份。

12.2.1 操作系统备份

操作系统备份的要求包括：

a) 应对操作系统和系统运行所产生的登录和操作日志文件进行定期备份；
b) 在操作系统安装系统补丁、进行系统升级、修改系统配置或其它可导致系统改变的情况发生前后宜进行操作系统备份；
c) 所有操作系统的备份完成后均应执行备份介质异地存放，并至少保留两年。

12.2.2 数据库备份

数据库备份的要求包括：

a) 数据库备份的范围包括数据库的日志文件、数据文件和系统程序文件；
b) 数据库日志文件包括归档日志文件、告警日志文件和跟踪文件；
c) 在安装数据库补丁、应用系统补丁、数据库升级或其它导致数据库改变的操作发生前后应备份完整的数据库数据文件和数据库程序文件，备份后应执行备份介质异地存放；
d) 数据库数据文件应定期备份，备份后应执行备份介质异地存放；
e) 当数据库发生故障时，如需进行系统恢复，应先备份故障数据库的数据文件；
f) 所有异地存放的数据库数据文件备份建议保留五年以上；
g) 所有异地存放的数据库日志文件和数据库程序文件备份宜至少保留两年；
h) 所有本地存放的数据库备份宜至少保留一年。

12.2.3 应用系统备份

应用系统备份的要求包括：

a) 应用系统备份包括应用系统程序文件、日志；
b) 应用系统程序文件、日志应定期备份，备份后应执行备份介质异地存放；
c) 在安装应用系统补丁前后应备份应用系统程序文件，备份后应执行备份介质异地存放。

12.3 实施数据备份和恢复

12.3.1 数据备份实施

数据备份的实施要求如下 ：

a) 环境信息系统维护人员应根据业务需要定期进行备份计划的复核，并进行相关修订；
b) 备份操作人员应根据备份计划定期执行备份工作，并检查备份日志，确认备份有效性，最后进行记录；
c) 如果发现备份失败，备份操作人员应检查失败原因，编写故障报告，并尽快安排重新备份；
d) 备份完成后需保存备份介质，备份操作人员应在标签上按要求记录备份信息，并移交备份介质管理人员。

12.3.2 恢复性测试

应按照环境信息系统的实际情况，根据业务需要进行系统恢复方案和恢复性测试计划的复核并进行相关修订。恢复性测试的要求如下：

a) 应定期进行恢复性测试，恢复性测试应不影响生产环境的运行；
b) 在恢复性测试时，应确认备份数据的可读性和完整性，以及恢复方案的可执行性，编写恢复性测试报告，签字确认并存档；
c) 如恢复性测试失败，应检查失败原因，编写故障报告，并尽快安排重新测试；
d) 完成测试后，应及时清除测试环境中的生产数据，并归还测试用备份介质，备份介质管理人员应签字确认接收备份介质。

12.4 数据备份介质管理

12.4.1 备份介质的存放

应专人负责保管备份介质，进行登记并按照规定妥善存放。存有备份数据的备份介质应贴好标签，明确标示：备份介质编号、备份介质有效期截止日期、备份日期、备份操作人员、备份环境名称、备份内容、备份用途、备份数据保存时间。

存有备份数据的备份介质需要进行异地存放的，应存放在安全的备用场所内，应在执行完异地存放后进行记录，并签字确认。

12.4.2 备份介质的访问

对备份介质的访问应进行记录，并由保管人员签字确认；应定期检查备份介质的访问情况，保证备份介质数量完整。

13 系统建设

应在系统的规划、设计、开发与维护阶段，正确识别、确认、批准所有安全需求，并设计、实施满足各项安全需求的安全控制措施。

13.1 系统的规划、设计、建设和验收

13.1.1 系统规划、设计和建设

系统规划应考虑当前系统状况、预测发展趋势，以及新的业务和系统需求；系统规划必须保留一定的余量，特别是关键系统。

系统设计除满足业务功能的需要之外，还必须从软硬件、网络结构、业务逻辑、应急恢复等多方面考虑系统的安全性。

在系统建设的过程中，配套安全系统应与业务系统同步规划、同步建设、同步运行，不能滞后业务系统发展。

系统管理人员应通过预测试得到系统信息，从中分析可能对系统安全或用户服务构成威胁的性能瓶颈数据，并设计相应的补救措施。

13.1.2 系统上线审批

设备入网包括采购、新建或扩容的设备进入环境保护业务专网运行，在新建网络与信息处理设施时，必须建立相应的入网审批规定，严把入网关，系统上线的安全要求如下：

a) 新建或扩容设备入网运行时，应做好验收测试工作，特别要通过安全方面的测试查找已知的安全漏洞；
b) 应定期维护入网设备的清单，新型号设备入网应通过入网测试；
c) 新建网络与信息处理设施必须具备用户管理功能，以防止非授权使用；
d) 入网前应先检查网络与信息处理设施的硬件和软件，确保能够和其它系统兼容。

13.1.3 系统验收

在新建系统、系统扩容、软硬件升级验收之前，应制定相应的验收标准，只有经测试合格的系统方可验收，系统验收过程应满足下列安全要求：

a) 应通过漏洞扫描、配置检查、渗透测试等技术手段，对系统的安全性进行测试，验证系统是否已经达到要求的安全水平；
b) 应具备对错误的恢复和重启程序、安全应急方案；
c) 应具有系统变更对现有系统造成影响的说明，特别是在业务高峰处理时间段内的变更；
d) 系统建设方应提供系统操作手册和相应操作培训；
e) 重要系统应引入第三方权威测评认证机构辅助进行安全验收。

13.2 系统开发的安全需求

当涉及系统开发外包或合作开发时，安全需求应在双方认可的合同或协议中给予明确规定。在进行具体的系统开发和软件维护时，应遵循以下安全要求：

a) 在应用系统开发、修改完成或者投入使用之前，应进行安全风险评估、业务影响评估、制定备份和灾难恢复方案；
b) 按照等级保护的相关要求，确保开发、测试与运行设备的分离；
c) 应标明应用的信息在等级保护中的分类级别，并确保运行应用的系统等级不低于该应用的信息级别；
d) 系统开发过程中应咨询用户的意见，以提高所设计系统的安全性及操作效率。

13.3 开发和支持过程中的安全

13.3.1 变更控制程序

为减少变更对系统安全造成的影响，应在系统开发与运行维护的所有阶段实施严格的变更控制，对变更的申请、审核、测试、批准、执行计划与具体实施提出明确要求，当应用软件的修改可能会影响运营环境时，应用软件和业务运营的变更控制程序应结合起来实施。变更控制程序包括以下内容：

a) 识别所有需要修改的计算机软/硬件、信息、数据库；
b) 选择恰当的变更时间，确保在具体实施过程中最大限度地减少对业务的影响；
c) 确保操作系统的更改不会对应用系统的安全性和完整性造成不良影响；
d) 保留所有变更的审计跟踪记录；
e) 及时更新业务连续性计划。

13.3.2 后门及木马的防范

后门和木马都属于恶意代码范畴，对网络与信息系统有重大的潜在威胁。在软件的采购、开发、使用和维护过程中，应采取如下防范控制措施：

a) 仅从信誉优良的厂商处购买软件；
b) 使用通过权威机构评估测试的软件产品；
c) 一旦安装完毕，控制对源代码的访问和修改；
d) 不得随意运行未经检测的软件；
e) 安装并正确使用检测和查杀后门、木马的工具。

13.3.3 软件开发外包的安全控制

在外包软件开发时，应注意以下几点要求：

a) 应选择信誉好的软件承包商；
b) 应遵从软件许可权协议、国家知识产权规定；
c) 应具有对代码质量、编程标准的合同要求；
d) 在安装之前进行后门和木马检测。

14 系统运维

14.1 日常运维工作

14.1.1 维护作业计划

为保证网络与信息系统维护工作的规范性与准确性，维护人员应遵照系统安全要求，根据实际情况，编制维护作业计划，维护作业计划应明确规定维护活动的内容和周期。

维护人员必须严格执行维护作业计划，未经批准不得随意更改。

维护作业计划的执行情况应记录在案，并接受检查。

14.1.2 操作日志

为了对系统运行进行有效的监控、调查研究安全事件，应记录网络与信息系统操作人员的操作日志，并防止操作日志被未经授权的更改或破坏，按规定的保存期限保存该操作日志，并根据操作程序对其进行定期、独立地审查。

14.1.3 日志审核

系统应保留日志记录，分析重复性登录失败、连续的访问尝试等信息以确定可疑事件。日志至少应记录以下内容：

a) 事件发生的日期和起止时间；
b) 用户标识或者计算机帐户；
c) 事件的类型及其结果（成功或失败）；
d) 事件来源（如端口和地址等）。

系统管理员应明确日志审核频率、定义安全事件判断规则、规定安全事件通报流程，对日志进行审核，发现并确定安全事件，应记录重大安全事件。

14.1.4 故障管理

应进行系统的故障管理，对网络与信息系统的故障进行记录，并采取相应的补救措施。系统的故障报告应包括故障起止时间、故障现象、业务影响、故障原因分析、处理过程及结果、故障恢复证据、事后的补救措施等。对故障管理的安全要求如下：

a） 应审核的系统故障报告，确保故障已被正确解决；
b） 故障处理后，应保证故障对系统安全造成的破坏已得到修复；
c） 应检查补救措施本身不会危及原有系统安全。

14.1.5 安全检查

安全检查应定期进行，并在系统变更后进行安全检查。定期检查应是在日常维护工作中定期安排的检查工作；系统变更安全检查应在网络与信息系统进行调整、变更以后进行，目的是验证系统的变更对网络与信息系统的安全运行与服务质量无不良影响。

应依据系统安全检查流程，从物理安全、系统安全、网络安全、应用安全和数据安全方面进行安全检查。检查网络与信息系统的安全运行情况与服务质量情况，主动发现网络与信息系统的安全隐患。

14.2 应急响应

各级环境保护部门须建立安全事件响应机制，规定在安全事件的发现、报告、分析、处理、总结阶段的相关责任和程序，最大限度地减少安全事件造成的损害。为了能够正确处理事件，应在事件发生后尽快收集相关证据。

14.2.1 及时发现与报告

系统运维的人员应确保及时发现安全事件。应向所有员工和第三方人员提供培训，明确其发现并报告安全事件的义务。

为确保及时、准确地报告安全事件，应建立报告程序，明确如下内容：
a） 受理部门和人员；
b） 报告的方式或途径；
c） 报告的内容应包括安全事件发生的时间、地点、系统名称、现象描述、初步分析等；
d） 对处理情况的反馈要求。

应制定安全预警信息的授权审批发布流程，当有可能出现大规模的安全事件时，网络安全机构应发布安全预警信息，提醒相关人员加强安全巡检并采取相关安全措施。

14.2.2 协调与分析处理

应分析安全事件的现象和影响，制定相应的处理程序，并根据以下因素决定处理的优先次序：
a） 国家安全利益；
b） 人员的生命安全；
c） 业务可用性；
d） 保护敏感信息；
e） 保护网络与信息资产，使遭受的损失降至最小。

安全事件处理分为抑制、消除、恢复等阶段，应基于以下安全要求：
a） 各级环境保护部门的网络安全机构应对安全事件进行分析，并通报有关人员协调处理；
b） 除非经过特殊授权，否则未经各级环境保护部门的网络安全机构的批准，任何人都不得试图证实安全缺陷的存在或者试图进行安全调查，以免破坏系统和证据；
c） 违法犯罪行为的计算机技术分析只能由经过各级环境保护部门的网络安全机构授权的、受过特殊培训的人员予以执行；
d） 安全事件处理人员应收集并记录事件数据，特别是采取处理措施后无法再获得的数据；
e） 跟踪、验证处理效果是否达到可接受的安全水平。

14.3 事件管理

14.3.1 建立事件管理程序

应制定并实施事件管理程序，将风险降至较低的水平，具体内容包括：

a) 在识别关键业务流程并排列优先顺序的基础上，根据风险发生的可能性及其产生的影响来判定环境信息系统所面临的风险；
b) 识别网络与信息处理设施实现的业务目标；
c) 根据单位的业务目标和优先级别制定业务连续性战略和业务连续性计划；
d) 定期测试并更新具体方案和程序；
e) 确保事件管理被纳入单位的管理流程和组织结构，明确分配事件管理的职责，包括部门之间的协调。

参与环境信息系统承建的合作厂商、第三方外包服务提供商也必须负责制订、实施、联合测试业务连续性方案，且该方案必须经过各级环境保护部门的网络安全机构审核。

14.3.2 业务连续性和影响分析

在进行业务连续性和事件影响分析时，应先进行风险评估，识别和分析两个主要因素：一是可能导致业务中断的事件；另一个是中断产生的影响。业务连续性和影响分析应涵盖所有业务流程，而不限于网络与信息处理设施。业务连续性和影响分析应基于以下方面：

a) 应根据风险评估的结果制定业务连续性战略，并据此确定业务连续性的整体方案，在获取上级批准后予以贯彻实施；
b) 进行业务连续性和影响分析过程中，应重点确认关键信息资产；
c) 灾难恢复计划流程的级别和范围应由信息资产损失对单位和业务的影响大小决定；
d) 业务的重要程度应基于客户利益、经济损失、法律影响、声誉等因素进行评估；
e) 业务的重要程度可用来确定恢复时间目标，决定网络与信息资产恢复正常需要的时间。

14.3.3 制定并实施业务连续性方案

在制定和实施业务连续性方案时应考虑以下内容：

a) 每套业务连续性方案都应有指定的责任人；
b) 业务连续性方案应经过上级部门和网络安全机构的审批；
c) 识别业务流程中所有岗位的职责，确定该岗位人员在业务连续性方案中的责任；
d) 确定应急程序，并关注与其它业务的关联性；
e) 记录经过批准的应急程序，并形成正式文件；
f) 向各级环境保护部门的员工及第三方提供业务连续性方案培训；
g) 识别业务连续性方案所需要的服务和资源；
h) 方案应确保满足业务恢复目标，并且业务恢复目标应与业务优先级别相匹配。

14.3.4 维护业务连续性方案

为确保业务连续性方案的有效性，应通过定期测试、评审和更新来维护业务连续性方案，同时确保所有相关人员都正确理解并掌握业务连续性方案。

应制定业务连续性方案的测试计划，明确规定所有业务连续性方案的测试周期和方法。可以采取每年全面演练一次备用系统的恢复测试。

应制定业务连续性方案的评估和变更管理程序，把定期评审每套业务连续性方案的责任分配到人，并定期更新，同时确保更新后的方案得到及时分发。

更新方案的时机一般是在系统出现重大变化时，如新设备的采购或操作系统的升级，还包括下列因

素的变化：

a） 人员及其联系方式；
b） 业务战略；
c） 系统迁移导致的地点、设施和资源的变化；
d） 法律法规；
e） 承包商、供应商以及关键客户；
f） 新的/撤销的流程；
g） 风险（运营风险和财务风险）等。

附录A
（规范性附录）
环境信息系统终端与办公安全要求

A.1 办公设备的安全控制

A.1.1 办公桌面的保护

应制定对日常办公桌面的保护要求，桌面保护的控制措施如下：

a) 纸质文件和可移动存储介质在不使用时，特别是在工作时间以外，应保存在柜子内或其它形式的保险装置内，且应锁闭；

b) 个人电脑、计算机终端在无人看管时，不得处于登录状态；在不使用时，必须通过键盘锁定等控制措施予以保护。

A.1.2 设备的移动控制

应对重要资产建立资产移动（包括单位内部移动和离开单位范围的移动）的审批程序，并定期抽查。

员工借用单位的信息资产应承担保密与保护责任，必须在离职时完好归还。

第三方带入工作区域的资产应履行审批和登记手续，承诺按规定使用和操作，并承担保密与保护责任，离开时应办理登出手续将资产带回。

A.2 日常信息的交换

A.2.1 电子邮件的安全

由于电子邮件存在着信息泄露、携带恶意软件、易受攻击、服务不可靠等安全风险，应对电子邮件的使用实施以下安全控制措施：

a) 包含环境信息的电子邮件应符合保密要求，应使用加密技术保护电子邮件的敏感内容的机密性和完整性；

b) 可疑的、来源不明的、无法被验证的电子邮件应交网络安全机构处理，不得随意打开和传播；

c) 应使用防病毒系统、防垃圾邮件系统等安全技术手段，保护电子邮件系统及终端免受恶意攻击；

d) 用于办公的电子邮件不得进行与工作无关的活动；

e) 应保存可作为证据的电子邮件内容，以便用于可能的举证需要。

A.2.2 办公系统的安全

应分析电子办公系统存在的安全风险，找到其薄弱环节，对办公系统应采取如下安全控制措施：

a) 应明确电子公告栏等环境办公的信息共享要求，并采取有效的控制措施进行管理；

b) 在办公系统中，单位领导日程安排等特殊个人相关的信息应限制访问；

c) 划分第三方使用区域，明确规定办公系统的使用人员和权限，使用访问控制技术限制非法访问；

d) 定期检查办公用户的状态，及时清除失效的用户；

A.2.3 信息的交换协议

在环境信息系统与外部组织通过网络交换环境信息时，应通过签订有关协议保护信息交换的安全，协议内容应说明所涉及信息的保密级别和相关要求。信息交换协议应包含如下内容：

a) 控制、传送和接收的管理职责；

b) 控制、传送和接收的流程及使用的软件；

c) 数据丢失情况下的责任和义务；

d) 定义双方认可的敏感信息或关键信息标记，以便信息能够得到有效保护；

e) 采用加密的方式保护敏感信息。

A.2.4 其它形式信息交换的安全

当通过语音、传真、图像、视频等形式交换环境信息时，有可能导致信息泄露，应明确规定通过这些形式交换信息时的安全要求，提高员工的警惕性。控制措施如下：

a) 不应在公共场合或开放的办公场所谈论用户名、口令等需要保密的内容；
b) 正确使用传真机，避免错误拨号误发信息；
c) 应保护电话、传真机、复印机、视频会议系统等信息处理设备，防止故意修改存储电话号码、非法读取设备内存消息的事件发生。

A.3 移动与远程办公

A.3.1 移动办公

应明确移动办公涉及的物理保护、访问控制措施、加密技术、存储备份以及病毒防护等方面的要求，移动办公包括使用苹果 IOS、安卓、Windows Phone 系统等移动客户端上网办公的方式。

应为使用移动式设备办公的人员提供相应的安全培训，使其清楚认识移动办公导致的额外风险及需要采取的控制措施。

A.3.2 远程办公

员工进行远程办公必须经过管理人员授权，远程办公具体控制措施应包括：

a) 应明确规定远程办公的工作范围、工作时间、允许持有信息的级别、被授权访问的系统与服务；
b) 应通过专用线路、VPN 技术、集中认证授权、日志记录等技术远程安全接入系统；
c) 应保证远程办公设备的物理安全，并由员工承担必要责任；
d) 应对远程办公设备定期审计及实施安全监控；
e) 当远程办公结束时，应立即撤销使用权限和访问权限。

A.4 存储介质管理

A.4.1 可移动存储介质管理

包含重要、敏感或关键信息的移动式存储设备应有专人负责管理，以避免丢失。任何存储介质带入和带出安全区域都需经过授权，并保留相应记录，方便审计跟踪。

A.4.2 存储介质的处置

应制定存储介质的安全处置流程，规定不同类型介质的处置方法、审批程序和处置记录等安全要求，控制措施包括：

a) 包含敏感信息的介质应被安全处置，视不同情况可清空其中的数据后重用，也可以将介质粉碎、焚毁；
b) 当不能确认介质中的信息级别时，应统一按最严格的方式处理所有介质；
c) 当需要外部第三方提供介质收集和处置服务时，应挑选合格的厂商，采取有效控制措施，并签署保密协议；
d) 存储过敏感信息的介质的处置过程应进行记录，以便审计跟踪。

附录B
（规范性附录）
环境信息系统不同等级安全要求对照表

本安全技术规范标准规定了基于环境信息系统特点所提出的一类环境信息系统的安全要求，是国家等级保护基本要求在环境系统的补充与落地方面要求，环境信息系统在安全建设过程中，应依据国家等级保护的基本要求和本规范规定的环境信息系统安全要求的内容进行信息系统的安全规划、设计、建设与运行维护。各级系统的安全要求见表 B.1。

表 B.1 环境信息系统不同等级安全要求对照表

			三级系统	二级系统	一级系统	终端	备 注
物理安全等级保护基本要求	物理位置的选择	a) 防震、防风和防雨	*	*			机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内。
		b)场地选择	*				机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。
	物理访问控制	a)专人值守	*	*	*		机房出入口应安排专人值守，控制、鉴别和记录进入的人员。
		b)审批监控	*	*			需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。
		c)区域划分	*				应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域。
		d)电子门禁	*				重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。
	防盗窃和防破坏	a)设备放置	*	*	*		应将主要设备放置在机房内。
		b)固定标记	*	*	*		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。
		c)线缆铺设	*	*			应将通信线缆铺设在隐蔽处，可铺设在地下或管道中。
		d)标识存储	*	*			应对介质分类标识，存储在介质库或档案室中。
		e)光电报警	*				应利用光、电等技术设置机房防盗报警系统。
		f)监控系统	*				应对机房设置监控报警系统。
	防雷击	a)避雷装置	*	*	*		机房建筑应设置避雷装置。
		b)防雷感应	*				应设置防雷保安器，防止感应雷。
		c)交流地线	*	*			机房应设置交流电源地线。
	防火	a)自动消防	*	*	*		机房应设置火灾自动消防系统，自动检测火情、自动报警，并自动灭火。
		b)耐火材料	*				机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
		c)防火隔离	*				机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。
	防水和防	a)水管安装	*	*			水管安装，不得穿过机房屋顶和活动地板下。

	潮	b)防雨	*	*	*		应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。
		c)防结露	*	*			应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。
		d)防水报警	*				应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。
	防静电	a)接地防静电	*	*			主要设备应采用必要的接地防静电措施。
		b)防静电地板	*				机房应采用防静电地板。
	温湿度控制	a)自动调节	*	*	*		机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。
	电力供应	a)稳压器	*	*	*		应在机房供电线路上配置稳压器和过电压防护设备。
		b)备用电源	*	*			应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求。
		c)冗余	*				应设置冗余或并行的电力电缆线路为计算机系统供电。
		d)备用供电	*				应建立备用供电系统。
	电磁防护	a)防干扰	*				应采用接地方式防止外界电磁干扰和设备寄生耦合干扰。
		b)线缆铺设	*	*			电源线和通信线缆应隔离铺设，避免互相干扰。
		c)电磁屏蔽	*				应对关键设备和磁介质实施电磁屏蔽。
物理安全环境安全技术要求	物理安全区域	安全区域边界	*				参见 8.1.1
		安全区域出入控制	*				参见 8.1.2
		安全区域物理保护	*				参见 8.1.3
	物理设备安全	设备安置及物理保护	*	*			参见 8.2.1
		电力保护	*	*			参见 8.2.2
		线缆安全	*	*	*		参见 8.2.3
		工作区外设备的安全	*				参见 8.2.4
网络安全等级保护基本要求	结构安全	a)设备冗余	*	*	*		应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要。
		b)网络带宽	*	*	*		应保证网络各个部分的带宽满足业务高峰期需要。
		c)安全路径	*				应在业务终端与业务服务器之间进行路由控制建立安全的访问路径。
		d)拓扑图	*	*	*		应绘制与当前运行情况相符的网络拓扑结构图。
		e)子网划分	*	*			应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。
		f)技术隔离	*				应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段。
		g)带宽分配	*				应按照对业务服务的重要次序来指定带宽分配优

							先级别，保证在网络发生拥堵的时候优先保护重要主机。
	访问控制	a)边界控制	*	*	*		应在网络边界部署访问控制设备，启用访问控制功能。
		b)会话控制	*	*			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。
		c)内容过滤	*				应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制。
		d)会话终止	*				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。
		e)限制连接数	*				应限制网络最大流量数及网络连接数。
		f)防地址欺骗	*				重要网段应采取技术手段防止地址欺骗。
		g)用户访问规则	*	*	*		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。
		h)拨号访问	*	*	*		应限制具有拨号访问权限的用户数量。
	安全审计	a)记录日志	*	*			应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。
		b)审计记录	*	*			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。
		c)审计报表	*				应能够根据记录数据进行分析，并生成审计报表。
		d)记录保护	*				应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。
	边界完整性检查	a)行为检查	*				应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。
		b)外联检查	*	*			应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。
	入侵防范	a)监视攻击	*	*			应在网络边界处监视以下攻击行为：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。
		b)检测报警	*				当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。
	恶意代码防范	a)检测清除	*				应在网络边界处对恶意代码进行检测和清除。
		b)代码库更新	*				应维护恶意代码库的升级和检测系统的更新。
	网络设备防护	a)用户鉴别	*	*	*		应对登录网络设备的用户进行身份鉴别。
		b)管理员限制	*	*			应对网络设备的管理员登录地址进行限制。
		c)唯一标识	*	*			网络设备用户的标识应唯一。
		d)双因素	*				主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。
		e)口令复杂度	*	*			身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换。

		f)失败处理	*	*	*		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。
		g)防止窃听	*	*	*		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。
		h)权限分离	*				应实现设备特权用户的权限分离。
网络安全环境安全技术要求	网络访问控制	网络服务安全策略	*				参见 9.1.1
		逻辑安全区域的划分与隔离	*	*			参见 9.1.2
		外部连接用户的验证	*	*	*		参见 9.1.3
		端口保护	*				参见 9.1.4
		网络接入控制	*	*			参见 9.1.5
		网络路由控制	*				参见 9.1.6
	网络操作流程与职责	技术操作要求	*				参见 9.2.1
		设备维护要求	*				参见 9.2.2
		变更控制	*				参见 9.2.3
		开发、测试与运行设备的分离	*				参见 9.2.4
	网络传输安全		*				参见 9.3
	网络安全审计与监控	网络安全事件记录	*				参见 9.4.1
		监控系统	*				参见 9.4.2
		日志审查	*				参见 9.4.3
	网络设备安全管理	设备安全管理要求	*	*	*		参见 9.5.1
		设备安全管理措施	*	*			参见 9.5.2
主机安全等级保护基本要求	身份鉴别	a)标识和鉴别	*	*	*		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。
		b)口令复杂度	*	*			操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。
		c)失败处理	*	*			应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。
		d)防窃听	*	*			当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。
		e)唯一性	*	*			应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。
		f)双因素	*				应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。
	访问控制	a)资源控制	*	*	*		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。
		b)最小权限	*	*			应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。

		c)权限分离	*	*	*		应实现操作系统和数据库系统特权用户的权限分离。
		d)默认口令	*	*	*		应禁用或严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令。
		e)多余帐户	*	*			应及时删除多余的、过期的帐户，避免共享帐户的存在。
		f)敏感标记	*				宜对重要信息资源设置敏感标记。
		g)敏感操作	*				宜依据安全策略严格控制用户对有敏感标记重要信息资源的操作。
	安全审计	a)审计范围	*	*			审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。
		b)审计内容	*	*			审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用、账号的分配、创建与变更、审计策略的调整、审计系统功能的关闭与启动等系统内重要的安全相关事件。
		c)审计记录	*	*			审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。
		d)审计报表	*				应能够根据记录数据进行分析，并生成审计报表。
		e)审计进程	*				应保护审计进程，避免受到未预期的中断。
		f)保护记录	*	*			应保护审计记录，避免受到未预期的删除、修改或覆盖等。
	剩余信息保护	a)鉴别信息保护	*				应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他使用人员前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。
		b)存储空间清理	*				应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他使用人员前得到完全清除。
	入侵防范	a)检测报警	*				应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。
		b)恢复措施	*				应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。
		c)最小安装	*	*	*		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，并通过设置升级服务器等方式保持系统补丁及时得到更新。
	恶意代码防范	a)防护软件	*	*	*		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。
		b)代码库	*				主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。

		c)统一管理	*	*			应支持防恶意代码的统一管理。
	资源控制	a)限制终端登录	*	*			应通过设定终端接入方式、网络地址范围等条件限制终端登录。
		b)超时锁定	*	*			应根据安全策略设置登录终端的操作超时锁定。
		c)监视资源	*				应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况。
		d)资源限制	*	*			应限制单个用户对系统资源的最大或最小使用限度。
		e)服务水平检测	*				应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。
主机安全环境安全技术要求	用户身份鉴别	用户注册	*	*	*		参见 10.1.1
		超级权限的管理	*	*	*		参见 10.1.2
	操作系统访问控制	用户识别和验证	*	*	*		参见 10.2.1
		连接时间限制	*				参见 10.2.2
		日志审核	*	*			参见 10.2.3
	主机操作流程与职责	主机操作要求	*	*			参见 10.3.1
		主机维护要求	*	*			参见 10.3.2
		变更控制	*				参见 10.3.3
	软件及补丁管理		*	*	*		参见 10.4
	时钟和时间同步		*	*			参见 10.5
	系统安全监控	系统事件记录	*				参见 10.6.1
		监控系统	*				参见 10.6.2
		日志审查	*				参见 10.6.3
	恶意代码的防范		*	*	*		参见 10.7
应用安全等级保护基本要求	身份鉴别	a)标识和鉴别	*	*	*		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。
		b)双因素	*				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。
		c)标识检查	*	*			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。
		d)登录失败处理	*	*	*		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。
		e)鉴别策略	*	*	*		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。
	访问控制	a)控制策略	*	*	*		应提供访问控制功能，依据安全策略控制用

							户对文件、数据库表等客体的访问。
		b)覆盖范围	*	*			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。
		c)限制默认帐户	*	*	*		应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限。
		d)最小权限	*	*			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。
		e)敏感标记	*				应具有对重要信息资源设置敏感标记的功能。
		f)敏感信息操作	*				应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。
	安全审计	a)审计功能	*	*			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。
		b)保证审计记录	*	*			应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录。
		c)记录内容	*	*			审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。
		d)审计功能	*				应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。
	剩余信息保护	a)信息清理	*				应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。
		b)存储空间保护	*				应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。
	通信完整性	密码技术	*	*			应采用密码技术保证通信过程中关键数据的完整性。
	通信保密性	a)初始化验证	*	*			在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证。
		b)通信加密	*	*			应对通信过程中的整个报文或会话过程进行加密。
	抗抵赖	a)原发证据	*				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。
		b)接收证据	*				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。
	软件容错	a)有效性检验	*	*	*		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。
		b)自动保护	*	*			应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。
	资源控制	a)自动结束会话	*	*	*		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。

		b)并发限制	*	*			应能够对系统的最大并发会话连接数进行限制。
		c)多重会话	*	*			应能够对单个帐户的多重并发会话进行限制。
		d)并发连接数	*				应能够对一个时间段内可能的并发会话连接数进行限制。
		e)资源限额	*				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。
		f)服务水平检测	*				应能够对系统服务水平降低到预先规定的最小值进行检测和报警。
		g)服务优先级	*				应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。
应用安全环境安全技术要求	用户身份鉴别	口令管理	*	*	*		参见 11.1.1
		用户访问权限审核	*	*			参见 11.1.2
	应用访问控制		*	*			参见 11.2
	应用系统交互的完整性	输入数据验证	*	*			参见 11.3.1
		内部处理控制	*	*			参见 11.3.2
		输出数据验证	*	*			参见 11.3.3
	通信加密技术控制措施	加密技术使用策略	*	*	*		参见 11.4.1
		使用加密技术	*	*			参见 11.4.2
		数字签名	*				参见 11.4.3
		抗抵赖服务	*				参见 11.4.4
		密钥管理	*				参见 11.4.5
	应用系统安全管理	应用程序的部署及更新	*	*	*		参见 11.5.1
		测试数据的保护	*	*			参见 11.5.2
		应用系统源代码安全	*	*			参见 11.5.3
数据安全及备份恢复等级保护基本要求	数据完整性	a)检测完整性	*				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。
		b)错误恢复	*				应能够检测到系统管理数据、鉴别信息和重要业务数据在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。
	数据保密性	a)传输加密措施	*				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保密性。
		b)存储加密措施	*	*			应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。

	备份和恢复	a)本地数据	*	*	*		应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放。
		b)异地备份	*				应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地。
		c)冗余结构	*				应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障。
		d)高可用性	*	*			应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。
数据安全与备份恢复环境安全技术要求	数据备份策略		*	*	*		参见 12.1
	数据备份内容与频率	操作系统备份	*				参见 12.2.1
		数据库备份	*				参见 12.2.2
		应用系统备份	*				参见 12.2.3
	实施数据备份和恢复	数据备份实施	*	*	*		参见 12.3.1
		恢复性测试	*	*			参见 12.3.2
	数据备份介质管理	备份介质的存放	*	*	*		参见 12.4.1
		备份介质的访问	*	*	*		参见 12.4.2
系统建设环境安全技术要求	系统的规划、设计、建设和验收	系统规划、设计和建设	*	*	*		参见 13.1.1
		系统上线审批	*	*			参见 13.1.2
		系统验收	*	*			参见 13.1.3
	系统开发的安全需求		*	*	*		参见 13.2
	开发和支持过程中的安全	变更控制程序	*				参见 13.3.1
		后门及木马的防范	*	*			参见 13.3.2
		软件开发外包的安全控制	*	*	*		参见 13.3.3
系统运维环境安全技术要求	日常运维工作	维护作业计划	*	*	*		参见 14.1.1
		操作日志	*	*			参见 14.1.2
		日志审核	*				参见 14.1.3
		故障管理	*	*			参见 14.1.4
		安全检查	*	*	*		参见 14.1.5
	应急响应	及时发现与报告	*	*	*		参见 14.2.1
		协调与分析处理	*	*			参见 14.2.2
	事件管理	建立事件管理程序	*	*			参见 14.3.1
		业务连续性和影响分析	*	*			参见 14.3.2
		制定并实施业务连续性方案	*	*			参见 14.3.3

		维护业务连续性方案	*	*			参见 14.3.4
终端与办公安全环境安全技术要求	办公设备的安全控制	办公桌面的保护				*	参见附录 A.1.1
		设备的移动控制				*	参见附录 A.1.2
	日常信息的交换	电子邮件的安全				*	参见附录 A.2.1
		办公系统的安全				*	参见附录 A.2.2
		信息的交换协议				*	参见附录 A.2.3
		其它形式信息交换的安全				*	参见附录 A.2.4
	移动与远程办公	移动办公				*	参见附录 A.3.1
		远程办公				*	参见附录 A.3.2
	存储介质管理	可移动存储介质的管理				*	参见附录 A.4.1
		存储介质的处置				*	参见附录 A.4.2

（注：其中等级保护基本要求内容供参照--表中列出等保三级要求，对于等级保护二级和一级的信息系统进行建设时，与三级要求有差别的部分需要按照相应级别基本要求的不同强度执行，本表未一一列出）

附录C
（资料性附录）
大型环境信息系统安全建设示例

C．1　大型环境信息系统概述

本示例中的大型环境信息系统安全建设范围为环境保护部、省级环境保护厅（局）、市、县环境保护局四级机构。建设的主要内容包括建立统一的安全管理体系和管理制度，用以保障大型环境信息系统安全、高效、稳定运行。建立科学的、可行的安全工作制度，在内部建立安全管理规范。建立完备与可行的信息系统安全技术体系，保障信息系统免受各种安全攻击、事故的威胁，实现网络访问控制及加密保护、硬件安全防范、操作系统安全防范、用户统一身份认证控制、数据传输保护、安全审计、病毒防范等。

大型环境信息系统信息安全建设工作目前存在的主要困难包括：

a） 信息安全涵盖内容极为广泛，从物理安全，网络安全，系统安全一直到应用安全，数据安全，安全管理，安全组织等等，凡是涉及到影响系统正常运行和业务连续性的都可以认为是信息安全问题；

b） 安全保障是个系统化的工程，各个要素之间存在紧密联系，互相依赖，牵一发而动全身；

c） 安全保障是个长期性的工作，伴随信息系统的整个生命周期，是一个需要不断实施、检查和改进的过程；

d） 不同业务范围、不同地区信息化发展阶段、不同地域和行政隶属层次的安全要求属性和强度存在较大差异性；

e） 安全保障措施除了耗费人力财力，还会损失易用性，降低效率，所以应该考虑信息安全要求与资金人力投入的平衡,控制安全建设的成本。

C．2　安全建设实施过程

大型环境信息系统的等级保护实施过程应符合等级保护的整体实施过程,但对于这类环境信息系统由于存在系统复杂、庞大、行政级别多以及涉及范围广等特点，因此建议在各阶段增加以下相关工作和实施方法：

第一阶段：定级阶段

本阶段主要的三个步骤包括系统识别与描述、子系统划分以及对于系统总体和子系统进行定级，对于大型环境信息系统建议在进行系统识别和子系统划分的过程中结合“系统分域保护框架”的设计思路进行不同层次划分，可以从整体的角度出发，根据适合的划分方法进行整体性划分（例如行政级别、行政区域以及网络等要素），也可以从各个子系统的角度出发，总结和归类进行合并，最终形成多个层次的保护对象。每个层次的保护对象都能够对应相应的等级，形成“等级系统分域保护框架”。这里建议从整体角度出发进行划分，从子系统的角度出发进行验证，形成从下到上和从上到下的统一和平衡。

第二阶段：规划与设计阶段

本阶段主要的三个步骤包括系统分域保护框架建立、选择和调整五个等级基本安全要求、安全规划和方案设计。对于大型环境信息系统在选择和调整安全措施等级时建议首先根据行业背景、政府职能特征以及相对应的安全特性整体进行安全措施指标的选择，制定相关行业的安全要求，在这个基础上相关的各级部门和环保机构可以根据已经选择的安全等级指标进行进一步的修订和细化,这样可以确保从整体性出发安全措施的有效性和可控性；在进行安全规划与方案设计的过程时，不仅要根据不同安全等级系统选择不同安全措施进行规划和方案设计，这里建议采用“体系化”设计的方法，既能够从整体上进行统一规划，又能够通过安全解决方案解决现有安全问题，同时覆盖安全的各个层面，实现等级化和体系化的相互结合，最终形成等级化的安全体系。

第三阶段：实施阶段

本阶段主要是对等级保护的具体实施，在实施的过程中，针对大型环境信息系统建议采用“安全管

理中心”的安全措施建设方法，结合安全体系的内容对于需要统一规划的基础性工作进行总体性考虑，建立基于网控中心的基础性设施。在具体实施过程中可以考虑建立“安全管控中心”，平台中包括策略体系、组织体系以及运作体系，能够实现安全管理的整体性运作；建立“网络控制中心”，把支撑性基础设施的实现采用基础平台方法，例如统一认证平台、监控和审计平台等。

C．3　系统划分与等级保护定级

C.3.1　定级方法

对于大型环境信息系统，在判断系统的安全等级的过程中，系统自身的重要性对安全属性等级的确定有重要的影响。本过程中，系统等级确定的参考要素可以包括：

a）　系统涉及到的用户数量；

b）　系统涉及到的用户级别；

c）　系统对于业务运作的支撑程度；

d）　系统对于其它系统的影响程度；

e）　系统是否是国家环境保护战略发展的重要组成部分；

f）　系统是否支撑环境保护部门的重点发展工作。

C.3.2　系统分域保护框架

通过对等级保护的对象整体的定级、业务系统的影响、信息与资产影响的判断，可以基本确定各层保护对象汇总及定级（示例）见表C.1。

表C.1 各层保护对象及定级（示例）表

网络区域	功能区	安全等级
国家级网络	Internet服务区	3
	应用服务器区	3
	CA服务器区	3
省级网络	应用服务器区	3
	局域网外网区	3
	RA服务器区	3
地市级网络	局域网外网区	2
县级网络	局域网外网区	2

C．4　安全规划与设计

在安全需求分析的基础上，开展信息系统安全建设整改方案设计，包括总体设计和详细设计，制定工程预算和工程实施计划等，为后续安全建设整改工程实施提供依据。

C.4.1　确定安全技术策略，设计总体技术方案

C.4.1.1　确定安全技术策略

根据安全需求分析，确定安全技术策略，包括业务系统分级策略、数据信息分级策略、区域互连策略和信息流控制策略等，用以指导系统安全技术体系结构设计。

C.4.1.2　设计总体技术方案

在进行信息系统安全建设整改技术方案设计时，应以GB/T 22239-2008为基本目标，可以针对安全现状分析发现的问题进行加固改造；也可以进行总体的安全技术设计，将不同区域、不同层面的安全保护措施形成有机的安全保护体系，落实物理安全、网络安全、主机安全、应用安全和数据安全等方面基本要求，最大程度发挥安全措施的保护能力。在进行安全技术设计时，参考GB/T 25070-2010，从安全计算环境、安全区域边界、安全通信网络和安全管理中心等方面落实安全保护技术要求。

C.4.2　安全技术方案详细设计

C.4.2.1　物理安全设计

从安全技术设施和安全技术措施两方面对环境信息系统所涉及到的主机房、辅助机房和办公环境等进行物理安全设计，设计内容包括防震、防雷、防火、防水、防盗窃、防破坏、温湿度控制、电力供应、电磁防护等方面。物理安全设计是对采用的安全技术设施或安全技术措施的物理部署、物理尺寸、功能指标、性能指标等内容提出具体设计参数。具体依据 GB/T 22239-2008 中的“物理安全”内容、本规范中的“物理与资产安全”部分，同时可以参照 GB/T 21052-2007。

C.4.2.2　通信网络安全设计

对环境信息系统所涉及的通信网络，包括骨干网络、城域网络和其它通信网络（租用线路）等进行安全设计，设计内容包括通信过程数据完整性、数据保密性、保证通信可靠性的设备和线路冗余、通信网络的网络管理等方面。

通信网络安全设计涉及所需采用的安全技术机制或安全技术措施的设计，对技术实现机制、产品形态、具体部署形式、功能指标、性能指标和配置参数等提出具体设计细节。具体依据 GB/T 22239-2008 中“网络安全”内容、本规范中的“通信与操作安全”部分，同时可以参照 GB/T 20270-2006。

C.4.2.3　区域边界安全设计

对环境信息系统所涉及的区域网络边界进行安全设计，内容包括对区域网络的边界保护、区域划分、身份认证、访问控制、安全审计、入侵防范、恶意代码防范和网络设备自身保护等方面。

区域边界安全设计涉及所需采用的安全技术机制或安全技术措施的设计，对技术实现机制、产品形态、具体部署形式、功能指标、性能指标和配置策略和参数等提出具体设计细节。具体依据 GB/T 22239-2008 中的“网络安全”内容、本规范中的“通信与操作安全”部分，同时可以参照 GB/T 25070-2010、GB/T 20270-2006。

C.4.2.4　主机系统安全设计

对环境信息系统涉及到的服务器和工作站进行主机系统安全设计，内容包括操作系统或数据库管理系统的选择、安装和安全配置，主机入侵防范、恶意代码防范、资源使用情况监控等。其中，安全配置细分为身份鉴别、访问控制、安全审计等方面的配置内容。具体依据 GB/T 22239-2008 中的“主机安全”内容、本规范中的“系统及网络的访问控制”部分，同时可以参照 GB/T 25070-2010、GB/T 20271-2006。

C.4.2.5　应用系统安全设计

对环境信息系统涉及到的应用系统软件（含应用/中间件平台）进行安全设计，设计内容包括身份鉴别、访问控制、安全标记、可信路径、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错和资源控制等。具体依据 GB/T 22239-2008 中的“应用安全”内容、本规范中的“应用开发与维护安全”部分，同时可以参照 GB/T 25070-2010、GB/T 20271-2006。

C.4.2.6　备份和恢复安全设计

针对环境信息系统的业务数据安全和系统服务连续性进行安全设计，设计内容包括数据备份系统、备用基础设施以及相关技术设施。针对业务数据安全的数据备份系统可考虑数据备份的范围、时间间隔、实现技术与介质以及数据备份线路的速率以及相关通信设备的规格和要求；针对环境信息系统服务连续性的安全设计可考虑连续性保证方式（设备冗余、系统级冗余直至远程集群支持）与实现细节，包括相关的基础设施支持、冗余/集群机制的选择、硬件设备的功能/性能指标以及软硬件的部署形式与参数配置等。具体依据 GB/T 22239-2008 中的“数据安全和备份恢复”内容、本规范中的“备份与恢复”部分、“应急响应与事件管理”部分，同时可以参照 GB/T 20988-2007。

C. 5　安全措施的实施

C.5.1　工程实施和管理

安全建设整改工程实施的组织管理工作包括落实安全建设整改的责任部门和人员，保证建设资金足额到位，选择符合要求的安全建设整改服务商，采购符合要求的信息安全产品，管理和控制安全功能开发、集成过程的质量等方面。

按照 GB/T 20282-2006 中有关资格保障和组织保障等要求组织管理等级保护安全建设整改工程。实施流程管理、进度规划控制和工程质量控制可参照 GB/T 20282-2006 中第 8、9、10 章提出的工程实施、项目实施和安全工程流程控制要求，实现相应等级的工程目标和要求。

C.5.2 工程监理和验收

为保证建设工程的安全和质量，第二级（含）以上信息系统安全建设整改工程可以实施监理。监理内容包括对工程实施前期安全性、采购外包安全性、工程实施过程安全性、系统环境安全性等方面的核查。

工程验收的内容包括全面检验工程项目所实现的安全功能、设备部署、安全配置等是否满足设计要求，工程施工质量是否达到预期指标，工程档案资料是否齐全等方面。在通过安全测评或测试的基础上，组织相应信息安全专家进行工程验收。具体参照 GB/T 20282-2006。

C.5.3 安全等级测评

环境信息系统安全建设整改完成后要进行等级测评。对第三级（含）以上信息系统每年要进行等级测评。

在公安部备案的信息系统，备案单位应选择国家信息安全等级保护工作协调小组办公室推荐的等级测评机构实施等级测评；在省（区、市）、地市级公安机关备案的信息系统，备案单位应选择本省（区、市）信息安全等级保护工作协调小组办公室或国家信息安全等级保护工作协调小组办公室推荐的等级测评机构实施等级测评。