附件二：

HJ

# 中华人民共和国国家环境保护标准

HJ□□-201□

# 环境信息系统安全技术规范

**Security specification of environmental information system**

（征求意见稿）

201□-□□-□□发布　　201□-□□-□实施

**环　境　保　护　部**　发布

# 目　　次

# 前　　言

为贯彻《中华人民共和国环境保护法》、《国家信息化领导小组关于加强信息安全保障工作的意见》的相关要求，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、通信与运营、系统及网络的访问控制、数据的备份与恢复、应用开发与维护、应急响应与事件管理的安全要求。

本标准为首次发布。

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 2□□□年□□月□□日批准。

本标准自 2□□□年□□月□□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、通信与运营、系统及网络的访问控制、数据的备份与恢复、应用开发与维护、应急响应与事件管理的安全要求。

本标准适用于国家环境保护相关的各级、各类信息系统在规划、设计、开发、运行及维护实施中的各个阶段。

## 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/T17859-1999 计算机信息系统 安全保护等级划分准则

GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求

GB/T20984-2007 信息安全风险评估规范

GB/T 22080-2008 信息技术 安全技术 信息安全管理体系要求

GB/T 22081-2008 信息技术 安全技术 信息安全管理实用规则

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 24363-2009 信息安全技术 信息安全应急响应计划规范

GB/Z 24294-2009 信息安全技术 基于互联网电子政务信息安全实施指南

## 3 术语和定义

下列术语和定义适用于本标准。

### 3.1 可用性

保证信息和通信服务能够按预期投入使用的特性。

### 3.2 机密性

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、过程或其他实体的程度。

### 3.3 信息保障

保护信息及信息系统的机密性、完整性、可用性、可核查性、真实性、抗抵赖性，通常包括信息系统的保护、检测和恢复能力。

### 3.4 信息系统

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。

### 3.5 信息系统安全

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。

3.6 完整性

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。

3.7 风险

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。

3.8 安全域

指一个逻辑范围或区域，在同一安全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。

3.9 威胁

来自于信息系统外部的，能够通过未授权访问、毁坏、揭露、数据修改和/或拒绝服务对系统造成潜在危害的任何环境或事件。

3.10 脆弱性

存在于信息系统、系统安全程序、管理控制、物理设计、内部控制或实现中的，可能被攻击者利用来获得未授权的信息或破坏关键处理的弱点。

## 4 安全建设总体要求

环境信息系统应符合国家的信息安全规范，并且以风险防范为核心加强环境信息安全保护建设。

### 4.1 信息保密、严格管理

环境信息系统不得传输、处理、存储涉及国家秘密的信息。有关安全保密问题要严格遵守国家保密有关规定。

### 4.2 适度安全、综合防范

环境信息安全建设应当根据应用系统的安全需求，合理配置信息安全资源，采取适当的安全措施，进行有效的安全管理，从管理、技术等各个方面进行综合防范。

### 4.3 分级管理、分类防护

实施分级的边界防护和系统间访问控制，保证信息的安全隔离和安全交换；针对不同级别的信息采用不同的安全防护措施。

### 4.4 明确工作、各负其责

按照谁主管谁负责、谁运行谁负责的要求，各部门各单位全面负责所属省、市、县环境信息系统的安全管理工作。要明确建设单位、运行维护单位、用户单位的安全责任，并切实落实。

## 5 安全总体架构

### 5.1 环境信息系统安全目标

环境信息系统的安全目标是保持环境信息的持续可用和安全保密，保障国家环境保护工作正常运行。

### 5.2 环境信息网络结构

国家环境保护业务专网包括国家、省、地市、县四级，结构图见图 1：

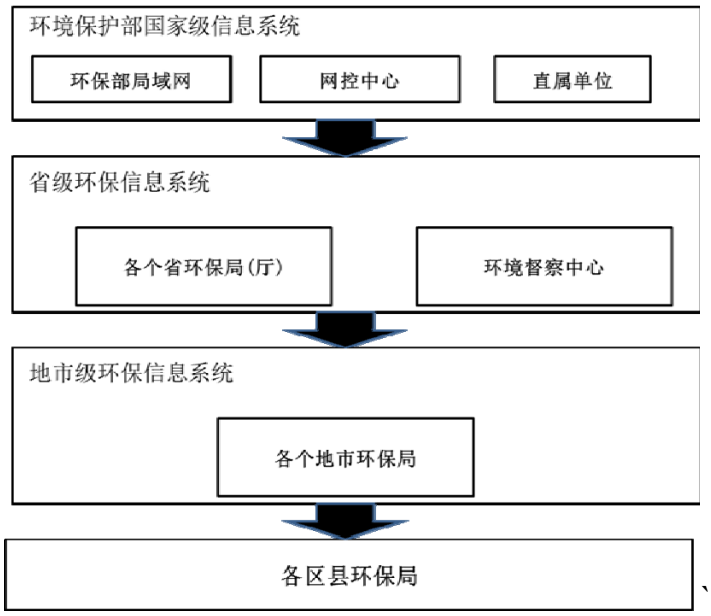


图 1 环境保护网络结构示意图

### 5.3 环境信息系统安全保障体系

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、安全技术系统的建设实现不同等级保护对象、不同安全域的安全保护，环境信息系统的安全保障体系见图 2。

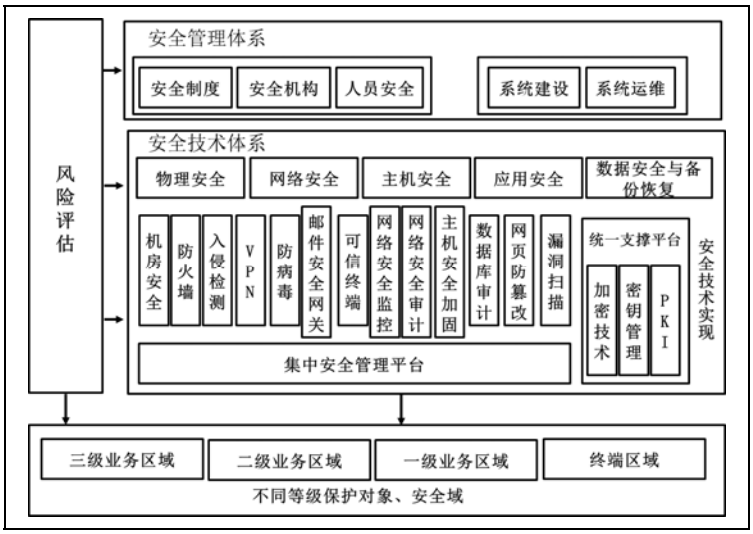


图 2 环境信息系统安全保障体系

安全管理体系建设应在系统建设和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的建设，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。

## 6 安全防护机制

环境信息系统应依据 GB/T 22240 的要求正确划分环境信息系统安全等级，按照等级保护的要求开展设计、建设、运行和维护的工作。

环境信息系统保护应遵循 GB 17859、GB/T 20271 和 GB/T 22239 的规定。

应根据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。

### 6.1 环境信息系统和应用分类

环保系统的业务应用主要分为环保办公、公共服务等。

a）环保办公

环保部门内部的业务处理，如环保部门间的公文流转、公文交换、公文处理、办公管理和数据共享等。安全防护的重点主要包括对环保系统人员的身份认证、环保资源的授权访问和数据传输保护等方面。

b）公共服务

面向社会公众提供信息公开、在线办事、互动交流等服务。安全防护的重点应放在系统和信息的完整性和可用性方面，特别要防范对数据的非法修改。

根据 HJ511-2009《环境信息化标准指南》的要求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：

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。

环境监测管理信息系统用于实现对全国环境质量数据（包括地表水、大气、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；

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；

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；

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；

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。

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。

### 6.2 信息分类防护措施

#### 6.2.1 环境信息系统的分类防护

各级、各类环境信息系统应进行安全等级划分，对信息系统实施等级保护的相关工作，信息系统的安全等级划分参照表 1：

**表 1 信息系统安全等级划分**

| 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 |
| | 局域网外网区 | 3 |
| | 数据库服务器区 | 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 |
| | 数据库服务器区 | 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 |

6.2.2 环境信息的分类防护

信息分类防护是指系统的防护措施应面向它所处理的信息，根据不同类别的信息采取不同的保护措施。

环境信息系统中信息分为公开信息和部门信息两类。

a）公开信息

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。

b）部门信息

部门信息限于环保系统人员访问，主要包括不宜公开的工作信息、政府（企业）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，部门公开信息是允许所有环保系统人员访问的信息，部门受控信息是经授权允许的环保系统人员才能访问的信息。

1)部门公开信息防护

对于部门公开信息的保护可采用口令或数字证书进行身份鉴别等手段，允许系统内环保系统人员通过身份鉴别访问部门公开信息，防止系统内非环保系统人员的非法访问。

2)部门受控信息防护

对于部门受控信息的保护应采用数字证书认证、自主访问控制和加密等手段，防止非授权人员的访问和数据泄漏。

## 7 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，应通过物理安全防护措施使得网络基础设施、信息系统及存储媒介等免受非法的物理访问、自然灾害和环境危害。

### 7.1 物理安全区域

应通过建立物理安全区域并实施相应的控制措施，对网络与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。例如：

机房区域、办公区域、第三方访问区域、公共/会客区域等。

7.1.1 安全区域边界

1) 安全区域的物理保护应通过在其边界周围设置若干隔离屏障来实现。安全边界的位置和强度应适用于安全区域的重要程度。
2) 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；
3) 机房应设有人工接待处或采取门禁限制出入；
4) 访问内部安全区域应仅限于经过授权的人员；
5) 安全边界上的所有应急通道出入口应设置报警装置，并且平时都应关闭。

7.1.2 安全区域出入控制

1) 进入安全区域的外来人员应当通过检查并进行监督，进入和离开安全区域的时间应有记录；
2) 机房等重要安全区域应使用身份识别技术（例如门禁卡、个人识别码等），所有访问活动应事先进行授权和验证，并保存审计记录；
3) 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；
4) 机房安全区域的访问权限应定期进行审查和更新。

7.1.3 安全区域物理保护

1) 机房安全区域内物理保护措施的选择和设计应考虑火灾、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及防范周边的安全威胁。
2) 所有重要的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；
3) 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；
4) 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；
5) 机房内应安装防盗入侵检测系统、防火探测警报系统、电视监视系统等安全设施。机房内未被使用的区域的告警装置也应开启；
6) 机房等安全区域应远离危险或易燃物品。不应存放大量的、短期内不使用的材料或物品；
7) 备用设备和备份媒介应放置在远离主安全区域的备用场所内，以防主场所发生灾难时可能造成的破坏。

**7.2 设备设施安全**

7.2.1 设备安置及物理保护

环境网络与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，对设备的物理保护应采取以下控制措施：

1) 重要的网络与信息处理设施的放置应尽量降低使用中的过失风险；
2) 采取相应的控制措施，尽量降低环境因素带来的潜在威胁。例如：盗窃、火灾、爆炸、烟雾、水、灰尘、震动、化学作用、电力故障、电磁辐射等；
3) 监控有可能对信息处理设施造成不良影响的环境条件。例如：温湿度；

4) 需要特殊保护的设备应与其他设备隔离，以降低整个区域内所需的安全保护级别；
5) 特殊环境下的设备，应考虑采用特殊的保护方法。例如：在工业环境里，采用防爆灯罩、键盘隔膜等。

7.2.2 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：

1) 电源应符合国家统一的技术规范；
2) 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；
3) 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；
4) 已知的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。

7.2.3 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：

1) 线缆布放应使用电缆管道或避免线路经过公共区域；
2) 电力电缆应与通信电缆分离，避免互相干扰；
3) 定期对电缆线路进行维护、检查和测试，及时发现故障隐患。

7.2.4 工作区外设备的安全

工作区外的设备分为两类：一类是带离工作区的信息处理设备，如笔记本电脑、测试仪表、移动硬盘等；另一类是固定在公共场所的设备，如监测基站、天线等。应根据工作区域外设备的安全风险，制定相应的保护措施，应至少达到工作区内相同用途设备的安全保护级别。

**7.3 存储介质的安全**

7.3.1 可移动存储介质的管理

1) 包含重要、敏感或关键信息的移动式存储设备应有人值守，以避免丢失。
2) 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。

7.3.2 存储介质的处置

为最大限度地降低信息泄露的风险，应制定存储媒介的安全处置流程，规定不同类型媒介的处置方法、审批程序和处置记录等安全要求，其中处置方法应与信息分级相一致。控制措施包括：

1) 包含敏感信息的介质应被安全地处置，如粉碎、焚毁，或清空其中的数据，以便重用；
2) 当无法确认介质中的信息级别，或确认信息级别的代价较高时，应统一按最严格的方式处理所有介质；
3) 当需要外界提供的介质收集和处置服务时，应挑选合适的承包商，并采取有效控制措施，如签署保密协议、抽查等；
4) 敏感介质的处置过程应当记录在案，以便审计跟踪。

7.3.3 系统文档的安全

系统文档可能包含一系列敏感信息，比如应用流程、程序、数据结构、授权流程的说明。应当考虑安全保存系统文档，避免系统非法访问。

### 7.4 通用控制措施

7.4.1 屏幕与桌面的清理

制定的屏幕与桌面的清理要求，应与信息分级原则相一致。措施如下：

1) 纸质文件和计算机设备在不使用时，特别是在工作时间以外，应保存在锁闭柜子内或其他形式的保险装置内；
2) 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、密码或其他控制措施予以保护。

7.4.2 资产的移动控制

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）的审批程序，并定期抽查。

员工借用的单位信息资产，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登记手续，以便离开时方便带回。

## 8 设备与运行安全

### 8.1 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的管理与操作的流程和职责，包括指定操作细则和事件响应流程。应落实责任的分工，减少疏忽的风险和蓄意的系统滥用。

8.1.1 技术操作规范

应制定网络与信息处理设施的技术操作规范，技术操作应涵盖以下内容：

1) 应规定对信息的处理和信息载体的处置操作规范；
2) 应规定时间进度的要求，包括同其他系统的相关性、最早的开始时间与最晚的结束时间等；
3) 操作过程中发生非预期的错误或其他异常情况下的指导说明；
4) 规定意外的操作困难或技术难题出现时的支持联系人；
5) 应规定特殊输出处置的说明。例如：特殊设备的使用，或输出机密内容的管理，包括如何安全处置失败的任务输出的程序；
6) 应有故障情况下系统的重启和恢复程序；
7) 应规定系统维护的相应程序。例如：计算机启动和关闭、备份、设备维护等。

8.1.2 IT 设备维护

正确规范地维护 IT 设备，可以保护设备的可用性和完整性。设备维护的基本要求如下：

1) 应根据 IT 设备供应商建议的维护周期和规范进行维护；
2) 设备维护人员必须具备相应的技术技能；
3) 必须储备一定数量的备品备件；
4) 所有日常维护和故障处理都应记录在案；

5) 当 IT 设备送到外部场所进行维护时，应当采取有效的控制措施防止信息泄露；
6) 系统关键设备应冗余配置；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；

8.1.3 变更控制

网络与信息系统的任何变更必须受到严格控制，包括：网络结构/全局数据/安全策略/系统参数的调整、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，记录在案并接受测试。操作环境的变化可能会影响应用系统，因此操作和应用的变更控制程序应尽可能相互衔接。变更控制基本要求如下：

1) 识别并记录重大变更；
2) 评估此类变更的潜在影响；
3) 变更失败的恢复措施和责任；
4) 变更成功与失败回退后的验证测试；
5) 保留所有与变更相关信息的审核日志；

8.1.4 开发、测试与运行设备的分离

1) 前期开发调试工作与运行中的设备应尽可能实现物理分离或逻辑分离，例如：独立的实验环境、不同的计算机或不同的域、目录等；
2) 后期在运行环境中进行测试时，应做好必要的安全防护措施，并对其进行安全检查。

**8.2 系统的规划设计、建设和验收**

8.2.1 系统规划和设计

管理人员应通过预测试得到的信息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，并对应设计合适的补救措施。系统规划应考虑现有发展情况和预测趋势，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。

系统设计在满足业务功能的同时，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。例如：冗余备份、多链路、严密的业务流程、紧急情况优先保证关键功能等。

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，以避免安全漏洞。

8.2.2 入网审批

在新建网络与信息处理设施时，必须建立网络与信息处理设施的入网审批规定，严把入网关。

1) 设备入网包括设备进入环境信息网络使用、新建或扩容的设备进入现网运行。
2) 新建或扩容设备入网运行时，应做好验收测试工作，特别是安全方面的测试，如查找已知漏洞。
3) 应建立入网设备清单并定期维护，对新型号设备应组织测试，并执行审批程序。
4) 新建的网络与信息处理设施必须符合相应的安全管理规定，并满足相应的安全技术要求；
5) 新的网络与信息处理设施必须具备适当的用户管理功能，以控制非授权使用；
6) 应事先检查网络与信息处理设施的硬件和软件，确保能够和其他系统兼容。未使用

过的设备或系统应进行全面测试；

7) 进行环境信息处理时，所采取的安全控制措施必须经过审批。

8.2.3 系统验收

应在新建系统、系统扩容、软硬件升级验收之前，制定相应的验收标准。验收要求和标准应能够被清楚定义、记录和测试。只有测试合格的系统方可验收。系统验收应满足下列要求：

1) 应通过技术手段，对系统的安全性进行测试，并验证达到要求的安全水平。例如：漏洞扫描，主机加固等；
2) 应有错误恢复和重启程序以及应急方案（包括自动化程序失效时的手工的替代方法）；
3) 应有业务连续性安排；
4) 系统更改对现有系统造成影响的说明（例如测试报告、承诺等），特别是在高峰处理时间；
5) 实施方需要提供有效的系统操作手册和相应培训；
6) 应确保验收测试中产生的信息和结果应注意保密，以免泄露影响系统安全性；
7) 重要系统应当引入第三方权威机构的测评认证，辅助进行安全验收。

8.3 恶意软件的防护

1) 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；
2) 针对通过外部网络或任何其他介质获取的文件和软件，应采取相关的防护措施；
3) 应安装并定期更新防病毒软件和补丁程序，以保护计算机和存储介质；
4) 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，都应进行正式调查；
5) 应检查所有来源不明/来源非法的存储介质上的文件或通过不可靠网络接收的文件，以确认是否含有恶意软件；
6) 检查所有电子邮件的附件及下载内容是否含有恶意软件。检查应在用户端或电子邮件服务器端进行；
7) 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；
8) 管理人员应采用可信的信息来源和权威发布，有效区分真假病毒；
9) 只从权威发布部门接收恶意软件相关信息，不要接收和传播未经确认的信息，对可疑问题应及时上报。

8.4 软件及补丁管理

在系统运行过程中应对软件及补丁版本进行维护与及时更新。在安全软件或补丁的使用方面的基本要求如下：

1) 所有安全软件（如：安全访问控制软件、病毒防护软件、入侵检测软件等）应尽可能选择经实践验证稳定运行的版本，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；
2) 厂商发布的安全补丁应进行功能测试，并在规定期限内投入应用。功能测试应确保

安全服务、安全机制的完善性和有效性，同时还应确保其变化不会影响其他安全控制措施；

3) 无法按时完成安全补丁时，应采取临时应对措施，明确后续工作计划，并得到安全组织的批准；

4) 所有安全软件的升级必须按标准的流程执行。

### 8.5 时钟和时间同步

为保证系统的完整性和可用性应当对系统时钟进行同步，为进行监测、审计等重要工作的需要应当保证时间同步，应采用统一的时钟服务器和时间源系统。

### 8.6 日常工作

#### 8.6.1 维护作业计划

为保证网络与信息系统维护的规范性与准确性，系统责任人与维护人员应遵照系统安全要求，结合实际情况，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。

维护人必须严格执行维护作业计划，未经责任人批准不得随意更改。

维护作业计划的执行情况应记录在案，并接受责任人的检查。

#### 8.6.2 数据与软件备份

应根据系统的重要程度，制定数据与软件的备份策略，明确备份周期和方法，并提供充足的备份设施。

应采用如下控制措施：

1) 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），以及备份媒介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；

2) 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；

3) 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；

4) 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；

5) 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恢复系统；

6) 应明确规定必要信息的保留时间。

#### 8.6.3 操作日志

为对系统运作进行有效的监控和调查研究安全事件，网络与信息系统操作人员（如系统管理员）应记录自己的活动，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。

操作日志应至少包含如下信息：

1) 系统的启动和关闭时间；

2) 系统错误及所采取的纠正措施；

3) 对正确处置数据文件和网络与信息处理设备输出结果的确认；

4) 日志编写人员姓名。

8.6.4 日志审核

系统必须保留日志及一切必要信息，用以分析确定可疑事件（例如重复性登录失败，连续的访问尝试）。

审计跟踪记录至少应包含以下内容：

1) 事件发生的日期和起止时间；
2) 用户 ID 或者计算机账户；
3) 事件的类型及其结果（成功或失败）；
4) 事件来源（比如终端端口和节点等）；
5) 密钥的使用。

责任人应明确审核频率、定义安全事件判断规则、规定安全事件通报流程，用以审核日志，发现并确定安全事件。

重大安全事件应有记录，安全事件包括：

1) 多次失败登录；
2) 异常时间的接入或者异常地点的接入；
3) 信息流量的突然增加；
4) 针对系统资源的异常和/或饱和性尝试；
5) 重大网络与信息系统事件（比如配置更新以及系统崩溃等等）；
6) 安全属性变化。

应设置使系统日志能记录单个用户或对象的活动，以便进行审查，特别是超级特权用户。

8.6.5 故障管理

应进行系统的故障管理，将网络与信息系统的故障记录在案，并采取相应的补救措施。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。对故障管理的基本要求如下：

1) 应定期审核故障报告，确保故障已被正确解决；
2) 故障处理后应确保故障对系统安全造成的破坏已得到修补和恢复；
3) 应检查补救措施本身不会危及原有系统安全；
4) 应检查补救措施是否已得到有效实施。

8.6.6 安全测评

安全测评应定期进行例行测评并进行系统变更测评。定期例行测评应是在日常维护工作中定期安排的测评，测评周期可根据业务情况确定；系统变更测评应在对网络与信息系统进行了调整、变更，如对软件、局数据、硬件设备等进行了调整以后安排的安全测评，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。

应依据系统安全测评制度，从系统功能、安全状况、业务表现等方面进行测评。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。

8.7 **网络安全控制**

网络安全方面应采取以下的安全措施：

1) 应采取相应的控制措施，保护通过公共网络传输的数据的机密性和完整性，如采用 SSL、IPSec 等加密协议；

2) 整个网络的安全控制措施应协调一致，以便优化网络运营；

3) 应对网络安全状态进行持续监控，保存有关错误、故障和补救措施的记录。

## 8.8 信息与软件的交换

### 8.8.1 信息与软件交换协议

应通过签订有关协议保护对其它组织间的信息与软件交换的安全，包括交由第三方保管的软件。协议内容应说明所涉及信息与软件的保密级别和相关要求。协议应包含如下具体内容：

1) 控制、传送和接收的管理职责；

2) 控制、传送和接收的流程及使用的软件；

3) 数据丢失情况下的责任和义务；

4) 采用双方一致同意的标签制度来标记敏感信息或关键信息，确保标签含义容易理解，以便信息能够得到有效保护；

5) 保护敏感信息所必需的特殊控制措施，比如密钥等。

### 8.8.2 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、不确定性等安全风险，应制定电子邮件使用规定，实施以下控制措施：

1) 电子邮件应符合信息资产保密要求，必要时使用加密技术保护电子邮件内容的机密性和完整性；

2) 除非采取额外的控制措施，例如数字签名或可记录的人工确认等，否则电子邮件不得用于处理不可否认信息。例如：合同审批；

3) 可疑的、来源不明的、无法被验证的电子邮件应交安全部门处理，不得随意打开和传播；

4) 使用反病毒系统、入侵检测、漏洞扫描等安全技术手段，保护电子邮件系统及终端免受恶意攻击；

5) 规范员工使用电子邮件的行为，不得进行与工作无关或损害单位利益的活动；

6) 保存可作为证据的相关电子邮件内容，以便用于可能的举证需要。

### 8.8.3 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，采取如下控制措施：

1) 明确信息共享的要求，并采取有效的控制措施进行管理；例如电子公告栏；

2) 如果系统无法提供充分的安全保护，则不得处理敏感的环保信息；

3) 限制访问与某些特殊个人相关的信息，例如单位领导日程安排；

4) 明确规定系统的使用人员和权限，使用访问控制技术限制非法访问，例如划分第三方使用区域等；

5) 定期检查账户的状态，并进行清除工作；

6) 备份与业务连续性要求。

### 8.8.4 其他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，提高员工的警惕意识。例如：

1) 当电话存在被偷听或窃听的可能时，不应谈论敏感信息；
2) 不应在公共场合或开放的办公室以及墙壁较薄的会议场所谈论保密内容；
3) 正确使用传真机，避免错误拨号或使用存储的错误号码误发信息；
4) 有效保护信息处理设备，防止非法访问或有意设置的恶意陷阱。例如，故意修改存储号码、非法读取内存消息等。

## 9 系统及网络的访问控制

环境信息系统应基于各自业务的安全需求对系统和数据的访问进行控制，包括限制访问权限与能力，限制物理访问，限制使用网络与信息处理系统及存储数据。

### 9.1 访问控制策略

应根据以下内容确定访问控制策略的基本要求：

1) 访问权限除非明确许可，否则必须禁止；
2) 应明确限定信息标签的变更，包括系统自动生效的和用户决定的；
3) 应明确限定涉及用户权限的变更，包括系统自动生效的和管理员批准生效的；访问规则需经管理人员审查批准方可执行。
4) 应依照每个系统的安全要求制定访问控制策略；
5) 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；
6) 不同系统间，访问控制与信息等级应具有一致性；
7) 访问控制策略应当符合相关法律法规及合同义务的约束要求；
8) 访问控制策略应遵从信息发布和授权的管理，如根据工作需要确定信息发布和授权范围，并明确信息的安全级别；

安全访问控制措施如下：

1) 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；
2) 软硬件安全产品必须能够提供验证用户身份的手段，如口令、加密令牌、生物统计特征等；应根据不同的系统和应用，提供不同深度、不同层次、不同强度的认证手段；
3) 安全控制措施必须能够防止对用户认证数据（如密码、加密令牌、生物数据等）的非法访问；
4) 能够通过特殊功能账号在系统保护区域运行的软件，或者能够建立特殊权限账号的软件，必须只能由少数专业的、可信赖的授权人员予以安装、测试和执行，以确保此类软件只能执行授权功能，如备份软件、管理工具、数据库自动查询等；
5) 明文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案，同时在日志中记录其使用过程；
6) 所有系统和安全工具都必须采取管理账户密码保护措施，如默认的管理账户密码必须在产品安装过程中进行修改；
7) 连接到环境信息网络的系统必须接受环保系统的管理，包括监控和入侵测试。

## 9.2 用户访问管理

### 9.2.1 用户注册

针对多用户网络与信息系统应制定正式的注册和注销程序，对用户的访问权限进行控制。基本要求包括以下内容：

1) 使用唯一的用户标识符（用户 ID），使用户与其操作相关联，并对其行为负责；确实必要时，作为例外情况，才允许使用用户组账号，并采取额外的控制措施；
2) 检查授权访问的级别是否基于业务目的，且符合单位的安全策略，用户授权不得违反职责分离原则；
3) 用户访问权限应得到上级领导和责任人的批准；
4) 马上修改或注销已经更换岗位或离开单位的用户的访问权限；
5) 定期核查并删除多余、闲置或非法的用户 ID 和账户。

### 9.2.2 超级权限的管理

特殊权限账户应能灵活设置，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，如角色备份。

### 9.2.3 口令管理

口令作为鉴别用户身份的通用方法，口令的管理应符合以下的基本要求：

1) 口令的信息均为保密的信息；
2) 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，否则应关闭该账户；当用户忘记口令时，系统必须正确识别用户身份，否则不得向用户提供重置的临时口令；
3) 应以安全方式向用户提供临时口令，禁止使用未经保护的方式传递（如使用明文的电子邮件），并要求用户确认口令的接收；
4) 口令不得以未经保护的方式存储。

根据不同等级的安全要求应当选择使用其他的用户识别和验证技术，如指纹验证、签名验证、智能卡等。

### 9.2.4 用户访问权限审核

应采取措施定期审核用户的访问权限并记录。审核的基本要求如下：

1) 用户访问权限应由管理人员、系统责任人及系统维护人共同确认；
2) 用户账户、特殊功能账户、超级账户的访问权限应定期检查，周期至少每年检查一次；
3) 任何变化发生后应进行审核，如：发生非法入侵、人员变动等；
4) 对审核中发现的问题，应督促相关人员采取必要措施予以纠正。

## 9.3 用户职责

用户口令的应从安全角度选择和使用，并符合以下基本要求：

1) 口令必须保密；
2) 不得将口令记录在纸张等一切可视介质上；
3) 口令至少应有 6 个字符，必须是大小写字母、数字、特殊字符的组合，且不能包含

连续的相同字符，也不得基于个人信息，如姓名、电话号码以及出生日期等；

4) 定期修改口令，或根据访问次数修改口令，避免重复或循环使用旧口令；

5) 在第一次登录时修改系统分配的临时口令；

6) 不得在任何自动登录程序中包含口令，也不得将口令保存在宏或者功能键中；

7) 不得共享个人用户口令。

### 9.4 网络访问控制

访问内部和外部网络服务应当受到控制。应确保接入网络和网络服务的用户不会破坏网络服务的安全，其基本要求如下：

1) 在网络与其他企事业单位的网络，或者公共网络之间应设置安全的接口；

2) 安全边界采取有效的用户和设备验证机制；

3) 控制用户访问信息服务。

#### 9.4.1 网络服务使用策略

应防止不安全的网络服务连接影响整个单位的安全，因此内部网和公网的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：

1) 应明确用户允许访问的网络和网络服务；

2) 应规定对用户访问网络和网络服务进行授权的程序；

3) 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。

#### 9.4.2 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，同时综合考虑网络性能和成本，将网络与信息系统划分成不同的逻辑安全区域。

应根据该安全域内网络与信息系统的价值和安全风险等级，确定各安全域不同的保护等级。

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。

还需根据该安全区域的安全风险，防护等级，确定不同的安全管理要求和技术要求。

#### 9.4.3 外部连接用户的验证

用户通过外部网络访问内部网时必须接受验证。特定网络连接所需的保护级别应当通过风险评估来确定，且不同的环境可以采用不同的验证方式。

无线网络应被视作外部网络，用户通过无线网络访问内部网时应符合以下标准：

1) 必须采用经过批准的无线接入方式；

2) 必须接受身份验证；

3) 必须使用符合安全标准的通信终端；

4) 当传送敏感信息时必须进行加密。

#### 9.4.4 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、管理等端口，防止未经授权或非法的访问，并记录访问日志。

9.4.5 网络互联控制

应基于业务应用的访问策略和要求，采取适当措施，从技术和管理两方面控制网络互联。网络互联的基本控制要求如下：

1) 网络互联应基于业务需求；
2) 应制订互联接口规范和标准。例如：双层异构防火墙等；
3) 应明确定义允许和禁止互联的网络；
4) 限制边界处的网络互联能力，如通过安全网关，按照预设的规则过滤网间通信等；
5) 应在网络边界处采取限制措施限制具体应用，例如：电子邮件、文件传输、交互式访问及限定日期/时段的网络访问等。

9.4.6 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。路由控制应当基于源地址和目标地址检查机制，并使用网络地址转换（NAT）来隔离内部网络，并阻止网间传播不必要的路由信息。

9.4.7 网络服务的安全

应只允许提供必需的、经过批准的、“可确保安全”的网络服务。所有网络服务都应有清晰的安全属性描述，并明确对应的值，例如：WEB 中的 HTTP 协议是否采用 SSL 加密。

必须保留对网络服务的访问日志，并根据信息的密级确定日志的具体内容，针对低密级信息，可只保留失败访问记录，而针对高密级信息时，必须同时保留失败访问记录和成功访问记录。

**9.5 操作系统的访问控制**

操作系统应利用自身安全工具提供以下访问控制功能：

1) 验证用户身份，还应进行终端或物理地点识别；
2) 记录所有系统访问日志；
3) 应能限制用户连接时间；或其他任何特定情况下必须的访问控制方式，如查询-应答（challenge-response）等。

9.5.1 用户识别和验证

所有用户都应具有唯一的个人标识符（即用户 ID），以便追溯，责任到人。在特定情况下可以使用共享的用户 ID，但必须经过授权，并采取额外的控制措施来保证责任到人。

用户 ID 不得体现用户的权限级别。

验证方式可以基于密码、令牌、指纹、虹膜或数字签名等。

9.5.2 终端超时关闭

位于单位安全管理范围之外的公共区域或外部区域的终端，应当在规定的空闲时间之后清除屏幕并关闭应用和网络会话，从而阻止非授权访问，如个人电脑上带密码的屏幕保护程序，但此工具可以清除屏幕但不会关闭应用或者网络会话。

应根据该区域以及用户终端存在的安全风险，确定终端超时关闭的等待时长。

9.5.3 连接时间限制

应限制终端与网络服务的连接时间可以降低非法接入的风险。具体限制措施例如：

1) 应使用预先定义的时间段进行通信；
2) 正常情况下，应将连接时间限制在正常办公时间内；
3) 应对每次连接的时长进行限制。

## 9.6 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：

1) 应根据访问控制策略，控制用户访问应用系统和信息；
2) 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；
3) 不应威胁到共享信息资源的其他系统的安全；
4) 应仅向系统所有人和其他指定的授权用户提供信息访问。

### 9.6.1 信息访问限制

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，并且输出结果只能被发送至经过授权的终端和位置。同时，应定期检查此类输出，以确保冗余信息被删除。

### 9.6.2 隔离敏感应用

应为敏感应用提供隔离的运行环境，如运行在专用计算机上，或只与可信赖的应用系统共享资源。基本安全要求如下：

1) 应用系统的敏感级别应由责任人确定，并记录在案；
2) 与敏感应用共享资源的其他应用系统，应由敏感应用的所有人审查并批准。

## 9.7 系统安全监控

应对系统访问和使用进行监控，以检测违背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。

### 9.7.1 事件记录

应建立审计日志，记录系统异常情况及其他安全事件。审计日志应保留规定的时长，以便支持日后的事件调查和访问控制监控。审计日志应包括以下内容：

1) 用户 ID；
2) 登录和退出的日期和具体时间；
3) 成功的和被拒绝的系统访问活动的记录；
4) 成功的和被拒绝的数据与其他资源的访问记录。

### 9.7.2 监控系统使用情况

#### 9.7.2.1 监控流程

应对网络与信息系统的使用建立监控流程。监控流程应包括监控级别、监控内容、监控手段与工具、监控结果审查与措施、记录保存等方面的规定。

具体监控内容应包括：

1) 授权接入，包括：用户 ID、关键事件的日期和具体时间、事件的类型、被访问的文件、所用的程序/工具等；
2) 所有特殊操作，例如：主管账户的使用、系统的启动和终止、I/O 设备的连接/分离等；
3) 未经授权的访问尝试，例如：失败尝试、网络网关和防火墙的违反访问政策及通知、

专有入侵检测系统的发出的告警等；

4) 系统告警或故障，例如：控制台告警或消息、系统日志异常、网络管理告警等。

9.7.2.2 监控结果审查

应定期检查监控的结果，具体检查内容包括：

1) 检查应用进程的重要性；

2) 检查所涉及信息的价值、敏感程度和重要程度；

3) 应从曾经发生的安全事件中得到的经验；

9.7.2.3 日志审查

应对日志进行自动筛选以获取有用信息，或使用适当的分析工具进行检索查询。

在进行日志审查时，应区分审查人员与被审查人员，维护审计独立性。

### 9.8 移动与远程工作

9.8.1 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。

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。

9.8.2 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：

1) 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；

2) 应具备远程安全接入的技术方法，例如：专用线路、VPN 技术、集中认证授权、日志记录等；

3) 应保证远程办公设备的物理安全，并由员工承担必要责任；

4) 应定期审计及安全监控；

5) 当远程办公结束时，应立即撤销权限和访问权，并收回设备。如：员工出差租借密码令牌，返还后必须撤销权限。

当涉及第三方进行移动或远程办公时，应参照以上内容和相关的要求，明确规定双方应采取的安全控制措施。

## 10 数据备份与恢复

### 10.1 数据备份要求

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。

10.1.1 操作系统备份要求

操作系统层备份的要求包括：

1) 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备份；

2) 操作系统宜每半年备份一次；

3) 操作系统运行所产生的登录和操作日志文件宜每月备份一次；
4) 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；
5) 操作系统层的备份由主机管理员负责实施；
6) 所有操作系统层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。

10.1.2 数据库备份要求

数据库备份的要求包括：

1) 数据库层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；
2) 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；
3) 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；
4) 数据库数据文件宜每周备份一次，备份后建议执行备份介质异地存放；
5) 数据库归档日志宜每天进行增量备份；
6) 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；
7) 数据库层备份由数据库管理员负责实施；
8) 所有异地存放的数据库数据文件备份建议保留五年以上；
9) 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；
10) 所有本地存放的数据库备份宜至少保留一年。

10.1.3 应用系统备份要求

应用系统层备份的要求包括：

1) 应用系统层备份包括应用系统程序文件、日志；
2) 应用系统程序文件、日志宜每月至少备份 1 次，备份后应执行备份介质异地存放；
3) 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；
4) 应用系统日志宜每天进行增量备份，可在本地保存备份介质；
5) 应用系统备份由数据库管理员负责实施；
6) 所有的异地存放应用系统备份宜至少保留两年；
7) 所有本地存放的应用系统备份宜至少保留一年。

**10.2 实施数据备份和恢复**

10.2.1 备份方式

系统的数据备份方式分为全备份和增量备份：

1) 全备份是指在停止应用系统和数据库后进行数据文件的完整备份；
2) 增量备份指在不停止应用系统和数据库时只备份前次备份后发生变动或新产生的文件。

系统的数据备份方式又可以分为定期备份和临时备份：

1) 定期备份可采用定期运行的批处理脚本的方式；
2) 临时备份一般采用手工操作的方式。

除数据库归档日志文件、应用系统日志文件采用增量备份方式外，其它文件应采用全备份的方式。

10.2.2 数据备份

各单位应按照环境信息系统的实际情况制定详细的定期备份计划，包括日备份、周备份、月备份、年备份和可预见的临时备份。

环境信息系统维护人员应根据业务需要每季度进行备份计划的复核并进行相关修订。

备份操作人员应每日检查备份日志，确认备份有效性，并进行记录。

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。

备份完成后如需保存备份介质，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员。

10.2.3 恢复性测试

应按照环境信息系统的实际情况制定详细的系统恢复方案和恢复性测试计划。

环境信息系统应根据业务需要每年进行系统恢复方案和恢复测试计划的复核并进行相关修订。

恢复性测试宜每半年进行一次，恢复性测试应不影响生产环境的运行。

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；

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。

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，备份介质管理员应签字确认接收备份介质。

**10.3 数据备份介质管理**

10.3.1 备份介质的购买和报废

应根据日常备份的需要提前估算并购买备份介质的数量，并及时检查备份介质的可用量，避免备份介质写满或者容量不足的情况发生。

备份介质达到使用年限后，应对备份介质上保存的数据进行审核，如需继续保存，则应由备份操作人员将数据装移到新的备份介质上，并做恢复性测试，并签字确认。

在完成恢复性测试后应将新旧备份介质和记录移交备份介质管理员，备份介质管理员宜在 1 个月后销毁旧备份介质，记录更换信息，并签字确认。

10.3.2 备份介质的存放

应专人负责随时接收备份操作人员交来的备份介质，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，明确写明：

1) 备份介质编号
2) 备份介质有效期截止日
3) 备份日期
4) 备份操作人员
5) 备份环境名称
6) 备份内容

7) 备份用途

8) 备份数据保存时间

存有备份数据的备份介质应进行异地存放，存放地点需具备以下要求：

1) 和数据源的距离在 1 公里以上；

2) 符合防潮、防火和防震和温、湿度的要求。

应在执行完异地存放后应及时记录，并签字确认。

10.3.3 备份介质的访问

所有备份介质应由专人负责保管。

如需访问备份介质，必须填写申请表，由维护主管签字确认。

异地备份介质应保存在有环境监控及保安保卫的异地专用库房中，由负责管理异地存放备份介质的备份介质人员进行管理。

宜每月检查一次备份介质的访问情况，保证备份介质数量完整。

## 11 应用开发与维护的安全

应在网络基础设施、应用系统的开发与维护阶段，正确识别、确认、批准所有安全需求，并将之文档化。

### 11.1 系统的安全需求

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。

可采用通过公正的第三方独立评估和认证的产品。

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：

1) 必须在应用系统开发、修改或者投入使用之前指定应用系统责任人；

2) 在应用系统开发、修改或者投入使用之前，必须完成风险评估、业务影响评估、备份和灾难恢复方案；

3) 参照相关的要求，确保开发、测试与运行设备的分离；

4) 应用系统责任人负责标明应用的信息分类级别，并确保运行应用的系统的信息分类级别不低于该应用的信息分类级别；

5) 系统开发过程中应不断咨询操作部门及用户的意见，以提高所设计系统的操作效率。

### 11.2 应用系统的安全

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，如对输入数据、内部处理和输出数据的验证。针对用以处理敏感、脆弱或关键资产的系统，或者对此类资产有影响的系统，还应根据风险评估的结果确定安全要求，并采取额外的控制措施。

11.2.1 输入数据验证

输入到应用系统中的数据应当被验证，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和其他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：

1) 双重输入，如密码修改；

2) 定期检查关键字段或数据文件内容，确认其有效性和完整性；
3) 建立用于响应输入错误的程序；
4) 建立用于测试输入数据真实性的程序，如身份证号码末位数的奇偶性。

11.2.2 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。可以采用的控制措施如下：

1) 应用系统不应在程序或进程中固化账户和口令；
2) 系统应具备对口令猜测的防范机制和监控手段；
3) 避免应用程序以错误的顺序运行，或者防止出现故障时后续程序以不正常的流程运行；
4) 采用正确的故障恢复程序，确保正确处理数据；
5) 采取会话控制或批次控制，确保更新前后数据文件的一致性，例如：检查操作前后文件打开和关闭的数目是否一致；
6) 检查执行操作前后对象的差额是否正常，如：句柄处理，堆栈等系统资源的占用与释放等；
7) 验证系统生成的数据；
8) 在中央计算机和远程计算机之间，检查下载/上传的数据或软件的完整性；
9) 检查文件与记录是否被篡改。例如通过计算哈希值（HASH）进行对比；
10) 建立检查措施，确保应用程序在正确时间，按先后顺序运行。

11.2.3 输出数据验证

应用系统的输出数据应当被验证，以确保数据处理的正确性与合理性。输出验证包括：

1) 用以测试输出数据是否合理的真实性检查；例如：输出数据应在规定的赋值范围内；
2) 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；例如：在输出数据时提供帮助信息；
3) 可以用来验证输出数据的测试程序。

**11.3 系统文件的安全**

访问系统文件应当得到有效的控制。保证系统的完整性由拥有应用系统或软件的用户职能部门或者开发小组负责。

11.3.1 操作系统软件的控制

在操作系统中运行软件应当得到有效的控制。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：

1) 程序运行库的升级只能由指定的程序库管理员在获取授权后予以完成；
2) 操作系统应尽可能只保留应用程序的可执行代码；
3) 在系统测试、用户验收结束之前，及相应的程序源代码库升级之前，可执行代码不得在操作系统中运行；
4) 程序运行库的所有更新记录都应当予以保留；
5) 历史版本的软件应当予以保留，用作应急措施；

6) 任何版本更新都应考虑安全性，即应根据新版本具有的新型安全功能及带来的安全问题的数量和严重程度，确定是否更新版本。如果软件补丁有助于消除或削弱安全缺陷，则应采用软件补丁；

7) 操作系统的软件版本更新，有可能对应用系统带来影响。应与应用系统厂商签订合同，由其提供合适的支持与维护，例如兼容性测试、配合修改、技术支持等。

11.3.2 系统测试数据的保护

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。可采用的控制措施如：

1) 用于正式运营系统的访问控制程序，也应用于测试环境；
2) 每当将测试数据加载到测试系统时，应进行独立授权；
3) 在测试结束后，测试数据应当马上从测试系统中删除；
4) 测试数据的加载和使用应当被记录在案，以便检查跟踪。

11.3.3 系统源代码的访问控制

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

1) 源代码尽量不要保留在操作系统内；
2) 为每个系统指定程序库管理员；
3) 控制系统支持人员对程序源代码库的访问；
4) 处于开发和维护阶段的程序不得保留于运行程序源代码库中；
5) 程序源代码库的更新及发布只能由指定的程序库管理员在经过该应用的主管领导授权后实施；
6) 程序清单应当保存在安全环境中；
7) 对程序源代码库的所有访问都应保留审计日志；
8) 老版本的源程序应当归档，并清楚记录其被正式使用的确切日期和具体时间，及所有相关的支持软件、功能说明、数据定义和程序（如流程图）等；
9) 程序源代码库的维护和拷贝应当遵从严格的变更控制程序。

**11.4 开发和支持过程中的安全**

11.4.1 变更控制程序

为减少变更对系统安全造成的风险，应在系统开发与运行维护的所有阶段（如：计划需求、设计、编码、测试、运行和维护）强制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，确保系统安全性与控制措施不被损害，系统管理人员只能访问其工作必需的系统部分。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当结合起来实施。变更控制程序包括以下内容：

1) 保留变更的授权级别记录；
2) 确保由授权用户提交变更申请；
3) 审查变更控制措施和流程的完整性，确保未被修改和破坏；
4) 识别所有要求修改的计算机软/硬件、信息、数据库实体；
5) 及时发布操作系统的变更通知；
6) 在实施之前，详细的变更方案必须获得正式批准；

7) 选择恰当的变更时间，确保在具体实施过程中最大限度地减少业务影响；

8) 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；

9) 确保系统文档在每次修改后得到及时更新，并确保旧文档被正确归档和处置；

10) 做好软件升级的版本控制，如保存历史版本；

11) 保留所有变更的审计跟踪记录；

12) 确保及时更新业务连续性计划。

11.4.2 后门及木马的防范

后门和木码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。在软件的原始采购、开发、使用和维护过程中，应采取如下防范控制措施：

1) 仅从信誉卓著的厂商处购买软件；

2) 应购买提供源代码的软件，以便进行检验；

3) 使用通过权威机构评估测试的软件产品；

4) 在投入使用之前检查所有源代码；

5) 一旦安装完毕，控制对源代码的访问和修改；

6) 使用可靠人员操作关键系统；

7) 不得随意运行未经检测的软件，如电子邮件附件；

8) 安装并正确使用有关后门、木码的检测和查杀工具。

11.4.3 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：

1) 应选择信誉与质量保证能力好的软件承包商；

2) 应遵从软件许可权协议、代码所有关系以及知识产权；

3) 进行对外包工作质量和准确性的检验，并保留检查权利；

4) 制定在承包方违约时的处置措施；

5) 对代码质量的合同要求，如对编程标准的要求；

6) 在安装之前进行测试，以检测后门和木马。

**11.5 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。

加密技术通常被用来保护处于风险威胁中的信息，以及使用其它控制措施无法充分保护的信息。

11.5.1 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，力求使加密技术的应用达到“有效控制风险”，并避免不当或错误使用。

加密方案的评判是风险评估和控制措施选择流程的一部分。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：

1) 应具有密钥管理方法，包括在密钥丢失、泄露或损坏时恢复信息原文的方法；

2) 应具有相关岗位和职责，例如：策略实施、密钥管理等；

3) 应确定合适的加密保护级别的方法；

11.5.2 使用加密技术

在选择和应用加密技术时，应考虑以下因素：

1) 必须符合国家有关加密技术的法律法规，包括使用和进出口限制；
2) 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；
3) 应听取专家的建议，确定合适的保护级别，选择能够提供所需保护的合适的产品，该产品应能实现安全的密钥管理。另外，还应听取与加密技术法律法规相关的法律建议；
4) 一般的数据压缩技术（例如 ZIP 等）不得代替安全手段。

11.5.3 数字签名

在使用数据签名技术时，应基于以下的要求：

1) 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；
2) 应采取保护公钥完整性的安全措施，例如使用公钥证书；
3) 应确定签名算法的类型、属性以及所用密钥长度；
4) 用于数字签名的密钥应不同于用来加密内容的密钥；
5) 应符合有关数字签名的法律法规。

11.5.4 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，及相应的加密和数据签名技术。

11.5.5 密钥管理

应采取加密技术等措施来有效保护密钥，以免密钥被非法修改和破坏；还应对生成、存储和归档保存密钥的设备采取物理保护。此外，必须使用经过安全部门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。

密钥管理系统应当基于一致同意的标准、程序和安全方法：

1) 密钥产生：为不同的密码系统和不同的应用生成密钥；
2) 密钥证书：生成并获取公钥证书；
3) 密钥分发：向目标用户分发密钥，包括在收到密钥时如何将之激活；
4) 密钥存储：为当前或近期使用的密钥或备份密钥提供安全存储，包括授权用户如何访问密钥；
5) 密钥变更：包括密钥变更时机及变更规则。

11.5.6 处置被泄露的密钥

1) 密钥撤销：包括如何收回或者去激活密钥，如在密钥已被泄露时或者用户离开单位时；
2) 密钥恢复：作为业务连续性管理的一部分，对丢失或破坏的密钥进行恢复，如恢复加密信息；
3) 密钥归档：归档密钥，以用于归档或备份的信息；
4) 密钥销毁：密钥销毁将删除该密钥管理信息客体的所有记录，将无法恢复，因此，

在密钥销毁前，应确认由此密钥保护的文件不再需要；

5) 记录并审核与密钥管理相关的所有活动。

为了降低泄露的可能，密钥应当指定确切的激活和去激活日期，即密钥生存期，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。

除了安全地保管私钥之外，也应考虑对公钥的保护，如采用值得信赖的、得到公认的认证中心来发布公钥证书，并且控制证书的发布和使用范围。

应在与外部加密服务提供商（如认证中心）之间的服务协议或合同中，涵盖责任、服务可靠性以及服务响应时间等内容。

## 12 应急响应与事件管理

与安全事件的被动响应不同，环境安全事件管理是主动的预防手段，它从单纯事件的层次上升到网络与业务高度，从多方面保证预防措施落实到位，以及出现安全事件时正确有序的响应。

### 12.1 应急响应

各级环境保护单位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。

#### 12.1.1 及时发现与报告

应不断提高维护水平，并提供必要的技术手段，确保及时发现安全事件。还应向所有员工和承包商提供培训，使之认识到发现并报告安全事件是其应尽的义务。

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：

1) 受理部门和人员；

2) 报告的方式或途径，如电话、短信、电子邮件、传真等；

3) 报告的内容，如安全事件发生的时间、地点、系统名称、现象描述、初步分析等；

4) 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，信息安全机构应发布安全预警信息，提醒相关系统责任人和维护人加强安全巡检并采取相关安全措施。

#### 12.1.2 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：

1) 国家安全利益；

2) 人员的生命安全；

3) 业务可用性；

4) 保护敏感信息；

5) 保护网络与信息资产，使遭受的损失降至最小。

安全事件处理可分为抑制、消除、恢复等阶段，并应遵循以下标准：

1) 环保信息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；

2) 除非经过特殊授权，否则未经环保信息安全机构的批准，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；
3) 未经人事部门、法律部门、安全机构的授权，任何人不得对环保员工和相关单位个体进行安全调查，也不得向任何人提供任何支持调查的数据；
4) 违法犯罪行为的计算机技术分析只能由经过环保信息安全机构授权的、受过特殊培训的人员予以执行；
5) 安全事件处理人员应在不延长业务中断时间的前提下，尽量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。例如：内存数据、进程状态、连接等；
6) 跟踪、验证处理效果是否达到可接受的水平。

## 12.2 事件管理

### 12.2.1 建立事件管理程序

应当制定并实施事件管理程序，将风险降至可以接受的水平。具体内容包括：

1) 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；
2) 识别网络与信息处理设施实现的业务目标；
3) 根据单位的业务目标和优先级别制定业务连续性战略；
4) 根据业务连续性战略制定业务连续性计划；
5) 定期测试并更新具体方案和程序；
6) 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。

已成为环保业务流程一部分的合作方（如 SP）、外包服务的承包商也必须负责制订、实施、联合测试业务连续性方案，且该方案必须经过环境信息安全部门审核。

### 12.2.2 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，首先应进行风险评估，识别和分析两个主要因素：一是可能导致业务中断的事件，如设备故障、自然灾害等；另一个是中断产生的影响，如破坏规模以及恢复时间等。业务连续性和影响分析应当涵盖所有业务流程，而不仅仅限于网络与信息处理设施。业务资源和流程的责任人必须参与到风险评估活动中。

应当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，在获取管理人员批准后予以贯彻实施。

进行业务连续性和影响分析过程中，重要的一步是确认关键信息资产，

灾难恢复计划流程的级别和范围从总体上由业务影响评估所确定的特定信息资产损失对单位和业务的影响予以决定。

业务的重要程度基于若干评估范围：客户利益、经济损失、法律影响、声誉。

该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，并以此作为重要程度的主要度量。同时，必须评审恢复时间，并且应由受影响的业务和信息系统的相关各方协商一致，记录在案。

### 12.2.3 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：

1) 每套业务连续性方案都应指定责任人，系统责任人、维护人必须负责制定并实施业务连续性方案；
2) 业务连续性方案应经过领导层和信息安全部门的审批；
3) 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；
4) 确定并实施应急程序，并特别关注外部业务的关联性；
5) 记录经过批准的程序，并形成正式文件；
6) 向环保员工及第三方提供不同内容的业务连续性方案培训；
7) 所需的服务和资源，包括物业、水电、人员配备、非信息处理资源以及信息处理设施的备用安排等；
8) 业务连续性方案的密级应与业务系统的信息敏感性的最高级别相匹配；
9) 确保满足业务恢复目标，并与业务优先级别相匹配；
10) 确保业务连续性方案和其他备份数据、软件包等必需资源被安全地保存，如异地存放。

12.2.4 业务连续性方案框架

应制定一套业务连续性方案框架，以确保所有方案的连贯性、一致性，具体内容应包括：

1) 详细列出各种措施的触发条件和激活程序（包括涉及的人员）；
2) 应急程序，规定在发生危及业务可用性的事件后应采取的各种措施。当危及生命安全时，还应包括与相关政府部门的联系安排，如公安局、消防局等；
3) 备用程序，规定各种临时性的、尽快提供业务的替代措施，如：启用异地备份系统，用手工方式临时替代自动方式等；
4) 恢复程序，规定在恢复正常业务流程时所应采取的措施，如：用备份数据恢复原有系统，备用倒回主用等；
5) 维护计划，规定测试业务连续性方案的时间和方式，以及维护流程；
6) 提出教育和培训的具体要求，如：培训周期、培训对象等；
7) 明确相关人员在方案执行过程中的角色和职责，并根据实际情况指定主备用人员。

另外，现有的应急预案是业务连续性方案的一部分。

12.2.5 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，该计划应包括测试规模、测试时间和测试方式。业务连续性方案的各个组成部分也可以单独测试，并根据其重要程度采用不同的测试频率。在具体测试中，应结合实际情况，采用恰当的测试方式，如：

1) 仿真，即通过模拟环境和流程进行测试；
2) 系统恢复测试，侧重技术和操作；
3) 备用系统或场所的恢复测试；
4) 第三方提供的设施和服务测试，确保其符合合同要求；
5) 全面演练，检验环保部门、人员、设备、设施以及流程能否做出正确响应。

在具体测试中，应首先确保本地测试，再尽可能地实现异地恢复测试，同时尽量由不熟

悉被测场所的人员完成测试，以检验恢复程序的细节和完整性。在测试结束后，还应保留测试日志，包括时间、问题以及建议等，以利于问题的跟踪和解决。

应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等。

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