

---

# 重点用能单位能耗在线监测系统技术规范

## 第 8 部分 系统安全规范

(试行)

---

## 目 次

前 言.....	II
1 适用范围.....	1
2 规范性文件.....	1
3 术语和定义.....	1
4 系统信息安全保护概述.....	2
5 安全设计规范.....	7

# 前 言

为贯彻落实《国家发展改革委 质检总局关于印发重点用能单位能耗在线监测系统推广建设工作方案的通知》（发改环资〔2017〕1711号），规范和指导重点用能单位能耗在线监测系统建设，按照统一标准、互联互通、信息共享的建设原则，特制定《重点用能单位能耗在线监测系统技术规范》。

本部分为《重点用能单位能耗在线监测系统技术规范》的第8部分。

本部分参照 GB/T1.1-2009 给出的规则起草。

本部分起草指导单位为国家发展改革委环资司、市场监管总局计量司。

本部分主要起草单位：国家节能中心、国家信息中心、北京卫星信息工程研究院、太极计算机有限公司、中通服咨询设计研究院有限公司、中国电子技术标准化研究院、上海市计量测试技术研究院、北京华电众信技术股份有限公司。

# 重点用能单位能耗在线监测系统技术规范

## 第 8 部分 系统安全规范

### 1 适用范围

本规范规定了能耗在线监测系统信息安全体系架构的具体要求。

本规范用于指导重点用能单位能耗在线监测系统的国家平台和省级平台开展系统安全防护规划及设计，也可作为对能耗在线监测系统安全防护情况的监督、检查和指导的依据。

### 2 规范性文件

下列文件中的条款通过本标准的引用而成为本标准的条款，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859	计算机信息系统安全保护等级划分准则
GB/T 20984	信息安全技术信息安全风险评估规范
GB/T 22239	信息系统安全等级保护基本要求
GB/T 22240	信息系统安全保护等级定级指南
GB/T 25058	信息安全技术信息系统安全等级保护实施指南
GB/T 25070	信息系统等级保护安全设计技术要求
GB/T 28449	信息安全技术信息系统安全等级保护测评过程指南
GB/T 30976.1	工业控制系统信息安全 第 1 部分：评估规范
GB/T 30976.2	工业控制系统信息安全 第 2 部分：验收规范

### 3 术语和定义

GB 17859、GB/T 22239 和 GB/T 25070 确立以及下列术语和定义适用于本标准。

#### 3.1 敏感数据

敏感数据是指一旦泄露可能会对用户造成损失的数据，包括但不限于：

- a) 用户敏感数据，如用户口令、密钥等；
- b) 系统敏感数据，如系统的密钥、关键的系统管理数据；
- c) 其他需要保密的敏感业务数据；
- d) 关键性的操作指令；
- e) 系统主要配置文件；
- f) 其他需要保密的数据。

### 3.2 风险

某种威胁存在利用一种资产或若干资产的脆弱性使这些资产损失或破坏的可能性。

### 3.3 安全策略

主要指为信息系统安全管理制定的行动方针、路线、工作方式、指导原则或程序。

### 3.4 安全需求

为使设备、信息、应用及设施符合安全策略的要求而需要采取的保护类型及保护等级。

### 3.5 完整性

包括数据完整性和系统完整性。数据完整性表征数据所具有的特征，即无论数据形式作何变化，数据的准确性和一致性均保持不变的程度；系统完整性表征系统在防止非授权用户修改或采用资源和防止授权用户不正确地修改或采用资源的情况下，系统能履行其操作目的的品质。

### 3.6 可用性

表征数据或系统根据授权实体的请求可被访问与采用程度的安全属性。

### 3.7 弱口令

指在计算机采用过程中，设置的过于简单或非常容易被破解的口令或密码。

### 3.8 国家平台

国家平台指设立在国家节能主管部门，接收、存储、汇总、分析全国重点用能单位能源相关数据的国家数据中心，为相关政府部门、用能单位、社会公众提供应用服务，也称“国家数据中心”。

### 3.9 省级平台

省级平台是部署在省（区、市）相关部门，接收、存储、汇总、分析本地区内重点用能单位能耗在线监测数据，为本地相关政府部门、用能单位提供应用服务，也称“区域数据中心”。

### 3.10 能耗监测端设备

指放置在重点用能单位，用于采集、分析、汇总用能单位能耗数据并将数据上传到系统平台的设备总称。

## 4 系统信息安全保护概述

### 4.1 系统总体结构

重点用能单位能耗在线监测系统的国家平台和省级平台通过政务外网实现互通，各重点用能单位通过安装能耗监测端设备对自身能源数据进行采集、汇总，经互联网上传至系统平

台。

系统建成后，将为部委、节能管理部门和重点用能单位等各级用户，提供不同层次的服务。其中，部委级用户包括国家发展改革委、教育部、工业和信息化部、财政部等十二部委；节能管理部门用户包括国家节能中心和各省、区、市节能主管部门。

省级节能主管部门如已建有类似能源在线监测系统，可将已有系统中存储的各重点用能单位能耗数据上传至系统平台，省级节能主管部门在系统建成后，可根据自身需求，扩展其接入用能单位、接入数据范围或应用功能。

重点用能单位需按照《用能单位能源计量器具配置和管理通则》（GB 17167-2006）安装计量仪表，按照所属行业相应的能耗数据采集指南向系统平台传输数据。同时，系统平台向重点用能单位提供能耗水平统计分析服务。

国家部委级用户及国家节能中心通过政务外网访问国家平台，省、市级节能主管部门用户通过政务外网访问省级平台，重点用能单位通过互联网访问系统平台。系统总体网络架构如图 1 所示。

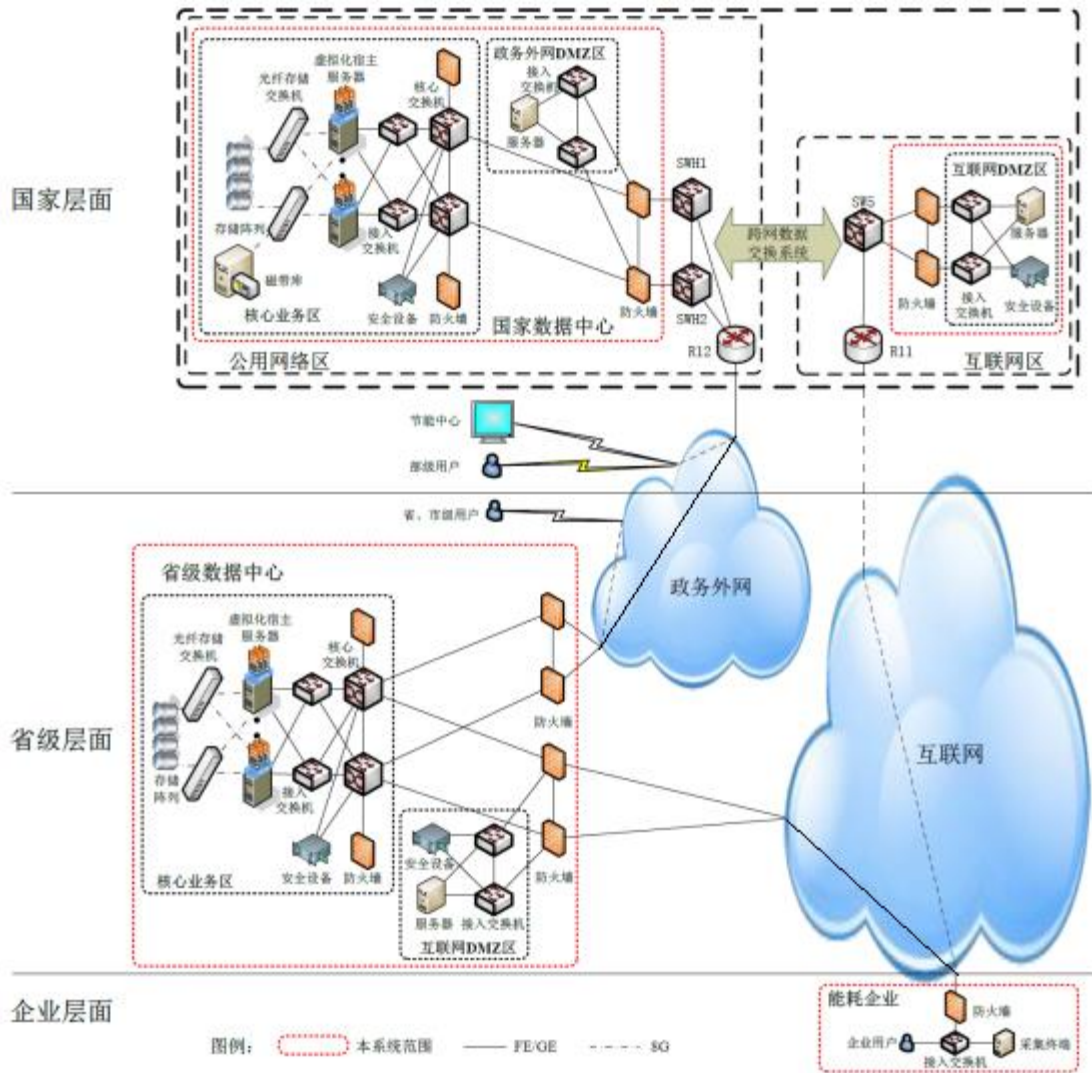


图 1 系统总体网络架构图

在图 1 总体架构图中，安置在重点用能单位的能耗监测端设备接收、采集本单位的在线能耗数据，每日定时向系统平台传送数据。传送数据采取可靠数据传送机制，即要求系统平台的数据接收服务器在接收到能耗监测端设备传送的一批数据之后，向能耗监测端设备反馈数据安全收到的反馈消息，能耗监测端设备接收到数据反馈之后，本次数据传送过程结束。如果接收到失败反馈，或者由于网络原因在规定时间内没有收到反馈，则自动进行数据重发，直至上述过程完成。系统平台的数据接收服务器在保证能耗监测端设备上数据完整、正确的情况下，接收上传数据并入库。

#### 4.2 安全防护设计框架

能耗在线监测系统安全规范设计以国家等级保护要求为原则，以能耗在线监测系统业务特点为基础，以《基本要求》为根本、参照《设计要求》提出信息安全保障总体框架。国家平台系统安全保护等级为第三级，省级平台安全保护等级为第二级。因此，能耗在线监测系

统安全防护设计应根据自身系统等级情况，完成在国家平台、省级平台及能耗监测端设备保护设计及跨级之间安全互联设计。

能耗在线监测系统信息安全防护总体框架如图 2 所示：



图 2 总体安全防护框架图

能耗在线监测系统安全防护设计应采用“安全域纵深防护”、“多层次立体防御”及“信息安全等级保护”相结合，从系统（或设备）所在的计算环境、区域边界、通信网络、安全管理以及物理安全等多层面部署安全保障措施，满足不同等级系统在技术、管理各层面防护要求，通过建立安全管理中心，实现数据、系统、网络等安全交换和关联分析管理，保障同级系统内部、跨级系统区域安全互联的安全。

#### 4.2.1 计算环境

计算环境是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，计算环境安全是信息系统安全保护的核心与基础。计算环境安全指保障终端、服务器操作系统、数据库、上层应用系统以及应用业务处理全过程的安全。通过在操作系统核心层设置以访问控制为主体的系统安全机制，形成严密的安全保护环境，从而有效防止非授权用户访问和授权用户越权访问，确保信息和信息系统的保密性和完整性，为业务应用系统的正常运行、免遭恶意破坏提供支撑和保障。计算环境防护主要针对信息系统的主机安全、应用安全及数据安全。计



算环境包含接入域，交换域和服务域。

### 1) 接入域

根据能耗在线监测系统的业务特点和接入关系而细分出的安全域，是应用系统防范的第一道屏障。根据接入的不同可分为对内系统接入子域、对外系统接入子域和用户接入子域三个部分。

- 对内系统接入子域——部署与能耗在线监测业务相关的互联网络设施以及相关的应用服务设施且不对外提供服务。该子域物理上分布在国家平台、省级平台。
- 对外系统接入子域——部署与能耗在线监测系统相关互联的网络设施以及相关应用服务设施。该子域物理上分布在国家平台、省级平台、企业端。
- 用户接入子域——各类桌面终端，该子域物理上分布在国家平台、省级平台。

### 2) 交换域

是由通信设施构成，主要是国家平台、省级平台及能耗监测端设备之间进行安全域数据的交换。

### 3) 服务域

服务域将应用系统层次架构与服务设施类别相结合，服务域划分为以下两个子域：

- 对外服务子域——部署为能耗在线监测系统用来对向自身平台外来提供接收、发送数据信息的业务服务设施，包括操作系统平台、基础架构平台和业务基础平台、数据库服务器等。
- 对内服务子域——部署为能耗在线监测系统为所在单位内部自身提供服务的信息系统业务服务设施。包括提供服务的数据库服务器、存储系统及网络互连设施。

## 4.2.2 区域边界

区域边界是定级系统的安全计算环境边界，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。区域边界包括互联网区域边界、外部区域边界和内部区域边界，分别与互联网、外部机构和内部机构相连，并包含一系列针对互联网、内外机构不同威胁、风险而采用的安全策略。

区域边界安全指通过对进入和流出应用环境的信息流进行安全检查和访问控制，确保不会有违背系统安全策略的信息流经过边界。区域边界是物理网络分区与边界整合的分析依据，同时还是用户或各级平台应用接入计算环境域前重要的应用接入点，区域边界暴露在安全体系框架的最外面，是风险点集中的环节，是安全防护的重点。区域边界防护主要针对信息系统的网络安全。

区域边界作为定级系统的安全计算环境边界，必须确保具有不同级别系统之间的可信互连机制。互连机制的建立必须基于较高级别系统或安全域的安全防护要求设置访问控制策略以及其他安全策略，可采用网络安全隔离技术或部署信息交换系统(比如前置系统等)实现，通过对不同级别的系统之间的可信互联进行严格约束来保证不会出现因高级别系统与低级别系统之间防护差异而导致的安全漏洞。

#### 4.2.3 通信网络

通信网络是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，通信网络安全指通信网络设备通过对通信双方进行可信鉴别验证，建立安全通道，并实施数据传输保护，确保数据在传输过程中不会被窃听、篡改和破坏。通信网络防护主要针对信息系统的网络安全。

#### 4.2.4 安全管理中心

实现对计算环境、区域边界和通信网络实施统一安全策略管理区域，确保系统配置完整可信，用户操作权限严格划分和审计全程追踪。从功能上可细分为系统管理、安全管理、综合审计管理以及物理支撑实施管理，各管理员职责和权利明确，三权分立，相互制约。

#### 4.2.5 管理体系

能耗在线监测系统应建完善的安全管理体系，首先根据能耗在线监测系统建设进程的实际需求，逐步建立起安全管理机构、各项安全管理制度及人员配置；其次通过专职安全机构、人员对制度的执行，提高信息安全保障能力；后续根据执行结果检查各项制度存在的问题和缺陷；最后依据检查结果对制度进行改进。从而形成建立、实施和执行、监控和审计、保持和改进的循环过程，形成完善的管理体系。

### 5 安全设计规范

#### 5.1 国家平台

国家平台安全设计应参照国家信息安全等级保护第三级基本要求加以设计。

##### 5.1.1 物理安全

国家平台在物理安全防护设计要求如下：

##### 1) 物理位置的选择

- a) 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) 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。

##### 2) 物理访问控制

- a) 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) 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) 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) 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。

### 3) 防盗窃和防破坏

- a) 应将主要设备放置在机房内；
- b) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；
- c) 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；
- d) 应对介质分类标识，存储在介质库或档案室中；
- e) 应利用光、电等技术设置机房防盗报警系统；
- f) 应对机房设置监控报警系统。

### 4) 防雷击

- a) 机房建筑应设置避雷装置；
- b) 应设置防雷保安器，防止感应雷；
- c) 机房应设置交流电源地线。

### 5) 防火

- a) 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) 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) 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。

### 6) 防水和防潮

- a) 水管安装，不得穿过机房屋顶和活动地板下；
- b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
- c) 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) 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。

### 7) 防静电

- a) 主要设备应采用必要的接地防静电措施；
- b) 机房应采用防静电地板。

### 8) 温湿度控制

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。

## 9) 电力供应

- a) 应在机房供电线路上配置稳压器和过电压防护设备；
- b) 应提供短期备用电力供应，至少满足断电情况下的关键设备4小时或以上的不间断运行保护；
- c) 应设置冗余或并行的电力电缆线路为计算机系统供电；
- d) 应建立备用供电系统。

## 10) 电磁防护

- a) 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) 电源线和通信线缆应隔离铺设，避免互相干扰；
- c) 应对关键设备和磁介质实施电磁屏蔽。

### 5.1.2 计算环境安全

#### 5.1.2.1 安全域划分

安全域是由一组具有相同安全保障需求、并相互信任的系统组成的逻辑区域，同一安全域的系统共享相同的安全保障策略。国家平台安全域划分应根据能耗在线监测系统的数据传输流程及网络位置，对其进行安全域划分，并按照这些安全功能需求设计和实现相应的安全隔离与保护措施。

国家平台安全域总体划分情况如下：

- 政务网外网 DMZ 区：包括连接国家电子政务外网的接入的边界防火墙、交换机等。该区域内部放置与各省级平台基于政务外网数据交换的前置机、数据库服务器、交换机等；
- 互联网 DMZ 区：包括连接互联网的接入的边界防火墙、交换机及等。该区域内部放置与各省级平台及企业端通过互联网进行数据交换的前置机、数据库服务器、交换机等；
- 核心业务区：包括能耗在线监测系统应用业务服务器、数据库服务器、中间件服务器、数据存储设备、安全防护设备、核心网络交换设备及安全管理系统等，该区域应在规划设计中进行子安全区域划分。

#### 5.1.2.2 网络环境防护

网络环境安全防护面向能耗在线监测系统运行的整体支撑性网络设施，以及提供网络支撑平台的网络环境基础设施，网络环境具体包括网络中的连接设备及安全防护引入安全设备、网络基础服务设施，应对经由网络传输信息流安全保障进行设计。

国家平台网络环境防护设计要求如下：

### 1) 结构安全设计

能耗在线监测系统应重点加强网络结构、边界互连等方面设计，以保证向各类用户提供稳定、持续的安全服务：

- 应保证网络设备业务处理能力具备冗余空间，满足业务高峰期需要；
- 应保证网络各个部分的带宽满足业务高峰期需要；
- 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；
- 应绘制与当前运行情况相符的网络拓扑结构图；
- 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；
- 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；
- 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。

### 2) 关键设备安全保护

设备安全防护应实现对国家平台网络、安全防护等关键设备设施的保护，包括在提供网络运营支撑及安全防护的防火墙、交换机，以及安全隔离防护网关等自身保护。

- 应对登录网络设备用户进行身份认证；
- 应对网络设备管理员登录地址进行限制；
- 网络设备用户的标识应唯一；
- 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；
- 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；
- 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；
- 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
- 应实现设备特权用户的权限分离。
- 配置文件备份，应当每次更新网络设备或安全设备配置后，以及定期进行配置文件备份，防止配置意外更改或丢失。

### 3、身份鉴别及系统审计

- 应在管理员登录网络及安全设备系统时，进行两种或两种以上组合机制身份鉴别，并对鉴别数据进行保密性和完整性保护。
- 应所有对网络设备及安全设施中操作配置的相关事件，能对特定的安全事件进行报警，同时为安全管理中心提供数据传输接口，实现审计日志的集中传输及存储分析。

### 5.1.2.3 主机安全防护

能耗在线监测系统的业务主机包括具备能源相关数据在线采集、处理、验证、存储、上传的业务服务器操作系统及数据库。

国家平台主机安全防护设计要求如下：

#### 1) 身份鉴别

- 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；
- 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；
- 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；
- 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；
- 应为操作系统和数据库的不同用户分配不同的用户名，确保用户名具有唯一性；
- 应对同一用户统一采用数字证书方式+USBKEY 实现用户身份鉴别。

#### 2) 访问控制

- 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；
- 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；
- 应实现操作系统和数据库系统特权用户的权限分离；
- 应严格限制默认帐户的访问权限，重命名系统默认帐户，并修改这些帐户的默认口令；
- 应及时删除多余的、过期的帐户，避免共享帐户的存在。
- 应对重要信息资源设置敏感标记；
- 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；

#### 3) 安全审计

- 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；

- 审计内容应包括重要用户行为、系统资源的异常采用和重要系统命令的采用等系统内重要的安全相关事件；
- 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；
- 应能够根据记录数据进行分析，并生成审计报告；
- 应保护审计进程，避免受到未预期的中断；
- 应保护审计记录，避免受到未预期的删除、修改或覆盖等。

#### 4) 剩余信息保护

- 应保证操作系统和数据库管理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；
- 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用户前得到完全清除。

#### 5) 入侵防范

- 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；
- 应能够对重要程序完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；
- 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。

#### 6) 恶意代码防范

- 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；
- 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；
- 应支持防恶意代码的统一管理。

#### 7) 资源控制

- 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；
- 应根据安全策略设置登录终端的操作超时锁定；
- 应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的采用情况；
- 应限制单个用户对系统资源的最大或最小采用限度；
- 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。

#### 5.1.2.4 业务交互应用防护

能耗在线监测系统业务用于采集重点耗能单位的能源消费总量、消费结构等数据，经整理、汇总与分析，生成动态的数据曲线和报表，实现节能目标进行预测预警等功能。能耗在线监测系统数据应用体现在企业数据上传，用户侧数据，国家和区域中心数据同步，在业务交互应用方面应按照下述要求进行设计。

在业务应用登录上，应采用基于双因子认证对操作及来访问者实体身份鉴别，或通过集中认证措施，实现统一的身份鉴别、访问控制身份管理及审计。国家平台业务交互应用防护要求如下：

#### 1) 身份鉴别

- 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；
- 应统一采用数字证书方式+USBKEY实现用户身份鉴别；
- 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。

#### 2) 访问控制

- 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体访问；
- 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；
- 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；
- 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。
- 应具有对重要信息资源设置敏感标记的功能；
- 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；

#### 3) 安全审计

- 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；
- 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；
- 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；
- 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。

#### 4) 剩余信息保护



- 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；
- 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。

#### 5) 通信完整性

应采用密码技术保证通信过程中数据的完整性。

#### 6) 通信保密性

- 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；
- 应对通信过程中的整个报文或会话过程进行加密。

#### 7) 抗抵赖

- 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；
- 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。

#### 8) 软件容错

- 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
- 应提供自动保护功能，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。

#### 9) 资源控制

- 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；
- 应能够对系统的最大并发会话连接数进行限制；
- 应能够对单个帐户的多重并发会话进行限制；
- 应能够对一个时间段内可能的并发会话连接数进行限制；
- 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；
- 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；
- 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。

#### 5.1.2.5 数据备份与恢复

- 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；

- 应提供异地数据备份功能，利用通信网络将关键数据至少每天批量传送至备用场地；
- 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；
- 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。

### 5.1.3 区域边界安全

能耗在线监测系统部署在政务外网-国家信息中心的公用网络区，通过国家电子政务外网及互联网实现与全国各省级平台、用能单位能耗监测端设备实现互联。

在区域边界防护设计上，应建立对进出系统所在网络边界的逻辑隔离控制及检测措施，安全检测措施应包括网络入侵检测（IDS）、内容访问过滤等，隔离剂控制措施应包括至少网络访问控制、入侵防护、以及对于远程接入用户及设备的标识与鉴别 / 访问权限控制。

国家平台区域边界安全防护设计应满足下述设计要求：

#### 5.1.3.1 访问控制

- 应在网络边界部署访问控制设备，启用访问控制功能；
- 应在互联网连接处边界，建立安全网络隔离与数据传输措施；
- 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；
- 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；
- 应限制网络最大流量数及网络连接数；
- 重要网段应采取技术手段防止地址欺骗；
- 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；
- 应限制具有拨号访问权限的用户数量。

#### 5.1.3.2 安全审计

- 应在安全区域边界设置必要的审计机制，并对确认的违规行为及时报警；
- 应能够根据记录数据进行分析，并生成审计报告；
- 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。

#### 5.1.3.3 边界完整性检查

- 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；

- 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。

#### 5.1.3.4 入侵防范

- 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；
- 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。

#### 5.1.3.5 恶意代码防范

- 应在网络边界处对恶意代码进行检测和清除；
- 应维护恶意代码库的升级和检测系统的更新。

#### 5.1.4 通信网络安全

通信安全是对国家平台经由网络传输的业务信息流业务数据所采取安全措施以保证经由网络传输信息的安全，应保证敏感信息经由网络传输时不被非法侦听、不被非法篡改或删除内容，并根据访问国家平台的用户或单位进行接入的可信控制。

国家平台通信网络安全防护设计要求如下：

##### 5.1.4.1 通信网络安全审计

- 应在安全通信网络中设置必要的审计机制，由安全管理中心集中管理，并对确认的违规行为及时报警。
- 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；
- 应能够根据记录数据进行分析，并生成审计报告；
- 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。

##### 5.1.4.2 数据完整性保护

采用由密码技术支持的完整性校验机制或具有相当安全强度的其他安全机制，以实现网络数据传输完整性保护，并在发现完整性破坏时进行恢复。

##### 5.1.4.3 数据保密性保护

采用由密码技术支持的保密性保护机制或具有相当安全强度的其他安全机制，以实现网络数据传输保密性保护。

##### 5.1.4.4 网络可信接入

可采用由密码技术实现的接入控制措施，通过对连接到网络的设备及用户进行身份认证，确保其接入网络的真实可信，防止非法接入对资源的非法访问。

### 5.1.5 安全管理中心

安全计算环境、区域边界和通信网络形成了基本的能耗在线监测系统的信息安全防护体系，为加强对资产管理、介质管理、网络安全管理、系统安全管理以及恶意代码防范管理，应建立安全管理中心，实现统一安全策略、统一安全管理等技术。

#### 5.1.5.1 系统管理

国家平台应建设系统管理子系统，实现对各业务主机、安全区域边界、安全通信网络实施集中管理和维护，包括用户身份管理、资源管理、应急处理等，系统管理员应采用双因子身份鉴别，并可对其操作进行记录审计。

#### 5.1.5.2 安全管理

国家平台应建设安全管理子系统，通过集中制定相应的系统安全策略，对各区域内的主机、区域边界设备和通信网络设备等进行强制执行，从而实现对整个信息系统的集中管理。安全管理员应采用双因子身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并进行审计。

#### 5.1.5.3 审计管理

国家平台核心内网，应建设安全管理子系统，通过集中制定审计策略，实现对整个信息系统的行为审计，确保抵赖违反系统安全策略的行为的追查及监控，同时为应急处理提供依据。审计管理员应采用双因子身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并进行审计。

### 5.1.6 安全管理

#### 5.1.6.1 安全管理机构

##### (1) 岗位设置

- 应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
- 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责；
- 应成立指导和管理工作信息安全的委员会或领导小组，其最高领导由单位主管领导委任或授权；
- 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

##### (2) 人员配备

- 应配备一定数量的系统管理员、网络管理员、安全管理员等；
- 应配备专职安全管理员，不可兼任；
- 关键事务岗位应配备多人共同管理。

### (3) 授权和审批

- 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
- 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
- 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
- 应记录审批过程并保存审批文档。

### (4) 沟通和合作

- 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题；
- 应加强与兄弟单位、公安机关、电信公司的合作与沟通；
- 应加强与供应商、业界专家、专业安全公司、安全组织的合作与沟通；
- 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；
- 应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。

### (5) 审核和检查

- 安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
- 应由内部人员或上级单位定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
- 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；
- 应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

## 5.1.6.2 安全管理制度

### (1) 管理制度

- 应制定信息安全工作的总体方针和安全策略,说明机构安全工作的总体目标、范围、原则和安全框架等;
- 应对安全管理活动中的各类管理内容建立安全管理制度;
- 应对要求管理人员或操作人员执行的日常管理操作建立操作规程;
- 应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。

#### (2) 制定和发布

- 应指定或授权专门的部门或人员负责安全管理制度的制定;
- 安全管理制度应具有统一的格式,并进行版本控制;
- 应组织相关人员对制定的安全管理制度进行论证和审定;
- 安全管理制度应通过正式、有效的方式发布;
- 安全管理制度应注明发布范围,并对收发文进行登记。

#### (3) 评审和修订

- 信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定;
- 应定期或不定期对安全管理制度进行检查和审定,对存在不足或需要改进的安全管理制度进行修订。

### 5.1.6.3 人员安全管理

#### (1) 人员录用

- 应指定或授权专门的部门或人员负责人员录用;
- 应严格规范人员录用过程,对被录用人的身份、背景、专业资格和资质等进行审查,对其所具有的技术技能进行考核;
- 应签署保密协议;
- 应从内部人员中选拔从事关键岗位的人员,并签署岗位安全协议。

#### (2) 人员离岗

- 应严格规范人员离岗过程,及时终止离岗的员工的所有访问权限;
- 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备;
- 应办理严格的调离手续,关键岗位人员离岗须承诺调离后的保密义务后方可离开。

#### (3) 人员考核

- 应定期对各个岗位的人员进行安全技能及安全认知的考核;
- 应对关键岗位的人员进行全面、严格的安全审查和技能考核;

- 应对考核结果进行记录并保存。
- (4) 安全意识教育和培训
- 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；
- 应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；
- 应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训；
- 应对安全教育和培训的情况和结果进行记录并归档保存。
- (5) 外部人员访问管理
- 应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案；
- 对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。

#### 5.1.6.4 系统建设管理

##### (1) 安全方案设计

- 应根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施；
- 应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；
- 应根据信息系统等级划分情况，统一制定安全保障体系总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；
- 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；
- 应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

##### (2) 产品采购和采用

- 应确保安全产品采购和采用符合国家的有关规定；
- 应确保密码产品采购和采用符合国家密码主管部门的要求；
- 应指定或授权专门的部门负责产品的采购；

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

### (3) 外包软件开发

- 应根据开发需求检测软件质量；
- 应在软件安装之前检测软件包中可能存在的恶意代码；
- 应要求开发单位提供软件设计的相关文档和采用指南；
- 应要求开发单位提供软件源代码，并审查软件中可能存在的后门。

### (4) 工程实施

- 应指定或授权专门的部门或人员负责工程实施过程的管理；
- 应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程；
- 应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。

### (5) 测试验收

- 应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；
- 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；
- 应对系统测试验收的控制方法和人员行为准则进行书面规定；
- 应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；
- 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

### (6) 系统交付

- 应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
- 应对负责系统运行维护的技术人员进行相应的技能培训；
- 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档；
- 应对系统交付的控制方法和人员行为准则进行书面规定；
- 应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。

### (7) 等级测评



- 在系统运行过程中，国家级每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改；
- 应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；
- 应选择具有国家相关技术资质和安全资质的测评单位进行等级测评；
- 应指定或授权专门的部门或人员负责等级测评的管理。

#### (8) 安全服务商选择

- 应确保安全服务商的选择符合国家的有关规定；
- 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；
- 应确保选定的安全服务商提供技术培训和承诺，必要的与其签订服务合同。

### 5.1.6.5 系统运维管理

#### (1) 环境管理

- 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；
- 应指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；
- 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；
- 应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。

#### (2) 资产管理

- 应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
- 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和采用的行为；
- 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
- 应对信息分类与标识方法作出规定，并对信息的采用、传输和存储等进行规范化管理。

### (3) 介质管理

- 应建立介质安全管理制度，对介质的存放环境、采用、维护和销毁等方面作出规定；
- 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；
- 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点；
- 应对存储介质的采用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁；
- 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；
- 应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。

### (4) 设备管理

- 应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
- 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；
- 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；
- 应对终端计算机、工作站、便携机、系统和网络等设备的操作和采用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；
- 应确保信息处理设备必须经过审批才能带离机房或办公地点。

### (5) 监控管理和安全管理中心

- 应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；
- 应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；

- 应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

#### (6) 网络安全管理

- 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；
- 应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；
- 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；
- 应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；
- 应实现设备的最小服务配置，并对配置文件进行定期离线备份；
- 应保证所有与外部系统的连接均得到授权和批准；
- 应依据安全策略允许或者拒绝便携式和移动式设备的网络接入；
- 应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

#### (7) 系统安全管理

- 应根据业务需求和系统安全分析确定系统的访问控制策略；
- 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补；
- 应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；
- 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定；
- 应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则；
- 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；
- 应定期对运行日志和审计数据进行分析，以便及时发现异常行为。

#### (8) 恶意代码防范管理

- 应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；

- 应指定专人对网络和主机进行恶意代码检测并保存检测记录；
- 应对防恶意代码软件的授权采用、恶意代码库升级、定期汇报等作出明确规定；
- 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录,对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理,并形成书面的报表和总结汇报。

#### (9) 密码管理

应建立密码采用管理制度,采用符合国家密码管理规定的密码技术和产品。

#### (10) 变更管理

- 应确认系统中要发生的变更,并制定变更方案;
- 应建立变更管理制度,系统发生变更前,向主管领导申请,变更和变更方案经过评审、审批后方可实施变更,并在实施后将变更情况向相关人员通告;
- 应建立变更控制的申报和审批文件化程序,对变更影响进行分析并文档化,记录变更实施过程,并妥善保存所有文档和记录;
- 应建立中止变更并从失败变更中恢复的文件化程序,明确过程控制方法和人员职责,必要时对恢复过程进行演练。

#### (11) 备份与恢复管理

- 应识别需要定期备份的重要业务信息、系统数据及软件系统等;
- 应建立备份与恢复管理相关的安全管理制度,对备份信息的备份方式、备份频度、存储介质和保存期等进行规范;
- 应根据数据的重要性和数据对系统运行的影响,制定数据的备份策略和恢复策略,备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法;
- 应建立控制数据备份和恢复过程的程序,对备份过程进行记录,所有文件和记录应妥善保存;
- 应定期执行恢复程序,检查和测试备份介质的有效性,确保可以在恢复程序规定的时间内完成备份的恢复。

#### (12) 安全事件处置

- 应报告所发现的安全弱点和可疑事件,但任何情况下用户均不应尝试验证弱点;
- 应制定安全事件报告和处置管理制度,明确安全事件的类型,规定安全事件的现场处理、事件报告和后期恢复的管理职责;

- 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分；
- 应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；
- 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；
- 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。

#### (13) 应急预案管理

- 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；
- 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；
- 应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次；
- 应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；
- 应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。

## 5.2 省级平台

省级平台安全设计应参照国家信息安全等级保护第二级基本要求加以设计。

### 5.2.1 物理安全

省级平台物理安全包括机房、UPS 电源、监控等场地设施和周围环境及消防安全，应符合国家相关标准，并至少满足断电情况下，关键设备 2 小时或以上的不间断运行保护。

省级平台物理安全保障要求如下：

#### 1) 物理位置的选择

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。

#### 2) 物理访问控制

- a) 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) 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。

#### 3) 防盗窃和防破坏

- a) 应将主要设备放置在机房内；
- b) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；
- c) 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；

- d) 应对介质分类标识，存储在介质库或档案室中；
- e) 应利用光、电等技术设置机房防盗报警系统；

#### 4) 防雷击

- a) 机房建筑应设置避雷装置；
- b) 机房应设置交流电源地线。

#### 5) 防火

机房应设置灭火设备和火灾自动报警系统。

#### 6) 防水和防潮

- a) 水管安装，不得穿过机房屋顶和活动地板下；
- b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
- c) 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；

#### 7) 防静电

主要设备应采用必要的接地防静电措施；

#### 8) 温湿度控制

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。

#### 9) 电力供应

- a) 应在机房供电线路上配置稳压器和过电压防护设备；
- b) 应提供短期备用电力供应，至少满足断电情况下的关键设备 2 小时以上的不间断运行保护；

#### 10) 电磁防护

应采用接地方式防止外界电磁干扰和设备寄生耦合干扰。

### 5.2.2 计算环境安全

#### 5.2.2.1 安全域划分

安全域是由一组具有相同安全保障需求、并相互信任的系统组成的逻辑区域，同一安全域的系统共享相同的安全保障策略。省级平台安全域划分应根据能耗在线监测系统的数据传输流程及网络位置，对其进行安全域划分，并按照这些安全功能需求设计和实现相应的安全隔离与保护措施。

省级平台安全域总体划分情况如下：

- 互联网 DMZ 区：包括连接互联网的防火墙、接入交换机及其它安全防护设备，部署有与省内各能耗监测端设备数据交换的前置机、数据库服务器、交换机等。
- 核心业务区：包括能耗在线监测系统的核心业务服务器、数据库服务器、中间件服务器、数据存储设备、安全防护设备、核心网络交换设备及安全管理系统等，该区域应在规划设计中进行子安全区域划分。

### 5.2.2.2 网络环境防护

网络环境安全防护面向能耗在线监测系统运行的整体支撑性网络设施，以及提供网络支撑平台的网络环境基础设施，网络环境具体包括网络中的连接设备及安全防护引入安全设备、网络基础服务设施，应对经由网络传输信息流安全保障进行设计。

省级平台网络环境防护设计要求如下：

#### 1) 结构安全设计

能耗在线监测系统安全稳定运行，应重点加强网络结构、边界互连等方面设计，以保证向各类用户提供稳定、持续的安全服务：

- 应保证关键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；
- 应保证接入网络和核心网络的带宽满足业务高峰期需要；
- 应绘制与当前运行情况相符的网络拓扑结构图；
- 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。

#### 2) 关键设备安全保护

设备安全防护应实现对国家平台网络、安全防护等关键设备设施的自身保护，包括在提供网络运营支撑及安全防护的防火墙、交换机，以及安全隔离网关等安全设备自身的安全防护。

- 应对登录网络设备的用户进行身份鉴别；
- 应对网络设备的管理员登录地址进行限制；
- 网络设备用户的标识应唯一；
- 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；
- 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；
- 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。

- 配置文件备份，应当每次更新网络设备或安全设备配置后，以及定期进行配置文件备份，防止配置意外更改或丢失。

#### 4、身份鉴别及系统审计

- 应在管理员登录网络及安全设备系统时，进行两种或两种以上组合机制身份鉴别，并对鉴别数据进行保密性和完整性保护。
- 应所有对网络设备及安全设施中操作配置的相关事件，能对特定的安全事件进行报警，同时为安全管理中心提供数据传输接口，实现审计日志的集中传输及存储分析。

#### 5.2.2.3 主机安全防护

能耗在线监测系统的业务主机包括具备能源相关数据在线采集、处理、验证、存储、上传的业务服务器操作系统及数据库。

国家平台主机安全防护设计要求如下：

##### 1) 身份鉴别

- 应对登录操作系统和数据库系统用户进行身份标识和鉴别；
- 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；
- 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；
- 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；
- 应为操作系统和数据库的不同用户分配不同的用户名，确保用户名具有唯一性。

##### 2) 访问控制

- 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；
- 应实现操作系统和数据库系统特权用户的权限分离；
- 应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；
- 应及时删除多余的、过期的帐户，避免共享帐户的存在。

##### 3) 安全审计

- 审计范围应覆盖到服务器上的每个操作系统用户和数据库用户；
- 审计内容应包括重要用户行为、系统资源的异常采用和重要系统命令的采用等系统内重要的安全相关事件；
- 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；
- 应保护审计记录，避免受到未预期的删除、修改或覆盖等。



#### 4) 入侵防范

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。

#### 5) 恶意代码防范

- 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；
- 应支持防恶意代码软件的统一管理。

#### 6) 资源控制

- 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；
- 应根据安全策略设置登录终端的操作超时锁定；
- 应限制单个用户对系统资源的最大或最小采用限度。

#### 5.2.2.4 业务交互应用防护

区域数据中心，负责采集归属区域范围内能耗企业真实的一线数据，为政府节能形势分析和预警调控提供及时准确的数据支持，是能耗监测系统的省级核心区域。其部署在各试点区域节能中心，通过政务外网和互联网两个出口提供服务。

在业务应用登录上，应采用基于双因子认证对操作及来访问者实体身份鉴别，或通过集中认证措施，实现统一的身份鉴别、访问控制身份管理及审计。省级平台业务交互应用防护要求如下：

##### 1) 身份鉴别

- 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；
- 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。

##### 2) 访问控制

- 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；
- 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；
- 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；
- 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。

### 3) 安全审计

- 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；
- 应保证无法删除、修改或覆盖审计记录；
- 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。

### 4) 通信完整性

应采用密码技术保证通信过程中数据的完整性。

### 5) 通信保密性

本项要求包括：

- 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；
- 应对通信过程中的敏感信息字段进行加密。

### 6) 软件容错

- 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；
- 在故障发生时，应用系统应能够继续提供一部分功能，确保能够实施必要的措施。

### 7) 资源控制

- 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；
- 应能够对应用系统的最大并发会话连接数进行限制；
- 应能够对单个帐户的多重并发会话进行限制。

#### 5.2.2.5 数据备份与恢复

- 应能够对重要信息进行备份和恢复；
- 应提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。

#### 5.2.3 区域边界安全

各试点省（区域）平台通过国家电子政务外网和互联网实现与国家平台和各用能单位的能耗监测端设备实现互联，同时对系统在线接收、存储、汇总、分析方面的不同，在省级平台内部应划分不同的网络区域。

在区域边界防护设计上，应建立对进出系统所在网络边界的逻辑隔离控制及检测措施，安全检测措施应包括网络入侵检测（IDS）、内容访问过滤等，隔离剂控制措施应包括至少网络访问控制、入侵防护、以及对于远程接入用户及设备的标识与鉴别 / 访问权限控制。

省级平台区域边界安全防护设计应满足下述设计要求：

#### 5.2.3.1 访问控制

- 应在网络边界部署访问控制设备，启用访问控制功能；
- 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，控制粒度为网段级。
- 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；
- 应限制具有拨号访问权限的用户数量。

#### 5.2.3.2 安全审计

- 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；
- 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。

#### 5.2.3.3 边界完整性检查

应能够对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查。

#### 5.2.3.4 入侵防范

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；

#### 5.2.3.5 通信网络安全

通信安全是对省级平台经由网络传输的业务信息流业务数据所采取安全措施以保证经由网络传输信息的安全，应保证敏感信息经由网络传输时不被非法侦听、不被非法篡改或删除内容，并根据省级平台连入用户/单位或连出进行接入的可信控制。

省级平台通信网络安全防护设计要求如下：

#### 5.2.3.6 通信网络安全审计

- 应在安全通信网络中设置必要的审计机制，由安全管理中心集中管理。
- 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。

#### 5.2.3.7 数据完整性保护

可采用由密码技术支持的完整性校验机制或具有相应强度的其他安全机制，以实现网络数据传输完整性保护。

#### 5.2.3.8 数据保密性保护

可采用由密码技术支持的保密性保护机制或具有相应强度的其他安全机制,以实现网络数据传输保密性保护。

#### 5.2.4 安全管理中心

安全计算环境、区域边界和通信网络形成了基本能耗在线监测系统的信息安全防护体系,为加强对资产管理、介质管理、网络安全管理、系统安全管理以及恶意代码防范管理,省级平台应建立安全管理中心,实现统一安全策略、统一安全管理等技术。

##### 5.2.4.1 系统管理

省级平台应建设系统管理子系统,对系统资源和运行进行配置、控制和管理,包括用户身份和授权管理、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复以及恶意代码防范等。系统管理员应采用双因子身份鉴别,只允许其通过特定的命令或操作界面进行安全管理操作,并进行审计。

##### 5.2.4.2 审计管理

省级平台应建设安全管理子系统,包括根据安全审计策略对审计记录进行分类,提供按时间段开启和关闭相应类型的安全审计机制,对各类审计记录进行存储、管理和查询等。审计管理员应采用双因子身份鉴别,只允许其通过特定的命令或操作界面进行安全管理操作,并进行审计。

#### 5.2.5 安全管理

##### 5.2.5.1 安全管理机构

###### (1) 岗位设置

- 应设立安全主管、安全管理各个方面的负责人岗位,并定义各负责人的职责;
- 应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责。

###### (2) 人员配备

- 应配备一定数量的系统管理员、网络管理员、安全管理员等;
- 安全管理员不能兼任网络管理员、系统管理员、数据库管理员等。

###### (3) 授权和审批

- 应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批;
- 应针对关键活动建立审批流程,并由批准人签字确认。

###### (4) 沟通和合作

- 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题；
- 应加强与兄弟单位、公安机关、电信公司的合作与沟通；

#### (5) 审核和检查

安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

### 5.2.5.2 安全管理制度

#### (1) 管理制度

- 应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；
- 应对安全管理活动中重要的管理内容建立安全管理制度；
- 应对安全管理人员或操作人员执行的重要管理操作建立操作规程。

#### (2) 制定和发布

- 应指定或授权专门的部门或人员负责安全管理制度的制定；
- 应组织相关人员对制定的安全管理制度进行论证和审定；
- 应将安全管理制度以某种方式发布到相关人员手中。

#### (3) 评审和修订

应定期对安全管理制度进行评审，对存在不足或需要改进的安全管理制度进行修订。

### 5.2.5.3 人员安全管理

#### (1) 人员录用

- 应指定或授权专门的部门或人员负责人员录用；
- 应规范人员录用过程，对被录用人员的身份、背景和专业资格等进行审查，对其所具有的技术技能进行考核；
- 应与从事关键岗位的人员签署保密协议。

#### (2) 人员离岗

- 应规范人员离岗过程，及时终止离岗员工的所有访问权限；
- 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
- 应办理严格的调离手续。

#### (3) 人员考核

应定期对各个岗位的人员进行安全技能及安全认知的考核。

#### (4) 安全意识教育和培训

- 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；
- 应告知人员相关的安全责任和惩戒措施，并对违反违背安全策略和规定的人员进行惩戒；
- 应制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行培训。

#### (5) 外部人员访问管理

应确保在外部人员访问受控区域前得到授权或审批，批准后由专人全程陪同或监督，并登记备案。

### 5.2.5.4 系统建设管理

#### (1) 安全方案设计

- 应根据系统的安全保护等级选择基本安全措施，依据风险分析结果补充和调整安全措施；
- 应以书面形式描述对系统的安全保护要求、策略和措施等内容，形成系统的安全方案；
- 应对安全方案进行细化，形成能指导安全系统建设和安全产品采购和采用的详细设计方案；
- 应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。

#### (2) 产品采购和采用

- 应确保安全产品采购和采用符合国家的有关规定；
- 应确保密码产品采购和采用符合国家密码主管部门的要求；
- 应指定或授权专门的部门负责产品的采购。

#### (3) 外包软件开发

- 应根据开发要求检测软件质量；
- 应确保提供软件设计的相关文档和采用指南；
- 应在软件安装之前检测软件包中可能存在的恶意代码；
- 应要求开发单位提供软件源代码，并审查软件中可能存在的后门。

#### (4) 工程实施

- 应指定或授权专门的部门或人员负责工程实施过程的管理；
- 应制定详细的工程实施方案，控制工程实施过程。

(5) 测试验收

- 应对系统进行安全性测试验收；
- 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；
- 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

(6) 系统交付

- 应制定系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
- 应对负责系统运行维护的技术人员进行相应的技能培训；
- 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档。

(7) 安全服务商选择

- 应确保安全服务商的选择符合国家的有关规定；
- 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；
- 应确保选定的安全服务商提供技术支持和服务承诺，必要的与其签订服务合同。

**5.2.5.5 系统运维管理**

(1) 环境管理

- 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；
- 应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；
- 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；
- 应加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等。

(2) 资产管理

- 应编制与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
- 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和采用的行为。

(3) 介质管理

- 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；

- 应对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点；
- 应对需要送出维修或销毁的介质，首先清除其中的敏感数据，防止信息的非法泄漏；
- 应根据所承载数据和软件的重要程度对介质进行分类和标识管理。

#### (4) 设备管理

- 应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
- 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；
- 应对终端计算机、工作站、便携机、系统和网络等设备的操作和采用进行规范化管理，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；
- 应确保信息处理设备必须经过审批才能带离机房或办公地点。

#### (5) 网络安全管理

- 应指定人员对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；
- 应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；
- 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；
- 应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；
- 应对网络设备的配置文件进行定期备份；
- 应保证所有与外部系统的连接均得到授权和批准。

#### (6) 系统安全管理

- 应根据业务需求和系统安全分析确定系统的访问控制策略；
- 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补；
- 应安装系统的最新补丁程序，在安装系统补丁前，应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；
- 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出规定；



- 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；
- 应定期对运行日志和审计数据进行分析，以便及时发现异常行为。

#### (7) 恶意代码防范管理

- 应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；
- 应指定专人对网络和主机进行恶意代码检测并保存检测记录；
- 应对防恶意代码软件授权采用、恶意代码库升级、定期汇报等作出明确规定。

#### (8) 密码管理

应建立密码采用管理制度，采用符合国家密码管理规定的密码技术和产品。

#### (9) 变更管理

- 应确认系统中要发生的重要变更，并制定相应的变更方案；
- 系统发生重要变更前，应向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告。

#### (10) 备份与恢复管理

- 应识别需要定期备份的重要业务信息、系统数据及软件系统等；
- 应规定备份信息的备份方式、备份频度、存储介质、保存期等；
- 应根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法。

#### (11) 安全事件处置

- 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；
- 应制定安全事件报告和处置管理制度，明确安全事件类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；
- 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分；
- 应记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。

#### (12) 应急预案管理

- 应在统一的应急预案框架下制定不同事件的应急预案,应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容;
- 应对系统相关的人员进行应急预案培训,应急预案的培训应至少每年举办一次。

### 5.3 能耗监测端设备

能耗监测端设备安全设计应以身份鉴别与访问控制技术为主,结合网络隔离和数据安全传输、数据校验及恶意代码防范等技术手段来综合防护,同时可参照国家信息安全等级保护相关要求完成在此要求基础上的增强性设计。

#### 5.3.1 结构安全及边界防护

能耗监测端设备能耗监测端设备所在的网络结构应满足下述要求:

- 采用网络设备性能及带宽应满足数据采集及上传的需要;
- 确定能耗监测端设备与所在单位企业的网络位置及各边界情况,并采用安全隔离与访问控制措施实现保护。

#### 5.3.2 身份鉴别与访问控制

- 能耗监测端设备应采用统一要求的CA数字证书进行身份验证,通过身份验证后才能接入系统平台。
- 在能耗监测端设备所在的企业网络,对企业内部网络,应建立数据安全传输及隔离控制措施,保证数据安全传输及企业内网边界隔离要求;
- 在能耗监测端设备所在的企业网络,对于向系统平台互联的互联网边界,应建立安全隔离访问控制及入侵攻击行为检测措施,保证能耗监测端设备不被非法访问及攻击事件的实时监测;

#### 5.3.3 安全审计

能耗监测端设备应具备对所有登录操作、登录时间、访问对象、传输链路资源使用及账户变更、管理员登录操作等情况日志记录功能,便于事后行为追溯。

#### 5.3.4 通信完整性与保密性

应在能耗监测端设备所在用能单位端的互联网边界,建立数据安全加密传输保护、数据完整性校验措施,实现与系统平台之间的安全通信,保证数据传输的保密性、完整性及可用性。

#### 5.3.5 数据备份与恢复

- 能耗监测端设备应采用冗余措施,防止单点故障的发生。
- 能耗监测端设备应具备策略配置文件等相应备份。

- 能耗监测端设备应具备数据备份与恢复功能。
- 制定数据备份与恢复方案，满足系统平台必要时的数据重传需要，以及安全事件发生时的数据恢复需要。

### 5.3.6 安全维护管理

能耗监测端设备在安全维护管理方面，可参照信息系统等级保护安全管理要求，结合用能单位信息安全管理现状，在人员、制度及应急流程方面分别制定相应要求，以加强对设备运行及数据传输过程中各类安全突发事件及时响应处置。