ICS 35.030
CCS L 80

团　　体　　标　　准

T/CNEA 228—2025

核能行业网络安全业绩目标与评估准则

Performance objectives and criteria for nuclear industry cybersecurity peer review

2025-09-05 发布　　2025-11-01 实施

中国核能行业协会　　发布

目　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国核能行业协会提出并归口，技术支持单位为上海核工程研究设计院股份有限公司、核工业标准化研究所、苏州热工研究院有限公司、华能核能技术研究院有限公司。

本文件起草单位：中国核能行业协会、中广核智能科技（深圳）有限责任公司、中核控制系统工程有限公司、台山核电合营有限公司、阳江核电有限公司、中国广核集团有限公司、上海核工程研究设计院股份有限公司、中国核电工程有限公司、北京卓识网安技术股份有限公司、大亚湾核电运营管理有限责任公司、福建宁德核电有限公司、辽宁红沿河核电有限公司、华能山东石岛湾核电有限公司。

本文件主要起草人：邹来龙、春增军、沙睿、陈伟雄、刘高俊、朱旭东、赵宏明、姚光霖、崔泽朋、李朝历、史茹梅、刘丹、林杰东、杨梓、秦宏志、李力、程朗、胡家铭、孙旭峰、陈泠普、李柯、李若兰、刘磊、毛磊、程懿、马骏、孙莹、宋磊、张玲玲、杨萌、贾长镇、刘江、刘文彬、李实、官尹文、单玉林、咸冰、侯曰永、郭云、郑东等。

本文件首次发布。

引　言

本文件旨在描述核能行业网络安全业绩目标与评估准则。同行评估强调持续改进和追求卓越，聚焦发现管理缺陷，其立足点和评估依据就是业绩目标与评估准则。业绩目标反映了待评估领域的最新和最佳业务实践，为各级管理者不断追求卓越设定管理业绩目标，为达成业绩目标明确相应的评估准则。

本文件是核能行业网络安全同行评估系列标准之一。与本文件相关的文件包括：

——T/CNEA 229—2025　核能行业网络安全同行评估与成员支持活动实施导则。

核能行业网络安全同行评估体系规定了网络安全同行评估领域、各领域的业绩目标及评估准则。业绩目标与评估准则是评估员进行现场评估活动的参考依据。每一个目标覆盖一个单独的、被清晰定义的管理领域。每一个目标下有一组准则，描述对达成目标有贡献的确定的活动。

核能行业网络安全业绩目标与评估准则

1 范围

本文件规定了核能行业网络安全业绩目标与评估准则，为核能行业开展网络安全同行评估工作提供指导。

本文件适用于核能行业开展网络安全同行评估，也可用于指导企业开展自评估工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984—2022 信息安全技术 信息安全风险评估方法

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南

GB/T 25069—2022 信息安全技术 术语

GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求

3 术语和定义

GB/T 20984—2022、GB/T 22239—2019、GB/T 22240—2020、GB/T 25069—2022 和 GB/T 39204—2022 界定的以及下列术语和定义适用于本文件。

3.1

评估准则 peer review criteria

用于衡量和评价特定对象或活动是否达到预期标准的一套规则或指标。

3.2

三同步 three synchronizations

同步规划、同步建设、同步使用。

3.3

等级保护对象 target of classified protection

网络安全等级保护工作直接作用的对象，主要包括信息系统、通信网络设施和数据资源等。

等级保护对象 5 个安全保护等级划分参见 GB/T 22240—2020。

4 缩略语

下列缩略语适用于本文件。

E-Mail：电子邮件（Electronic Mail）

Web：万维网（World Wide Web）

Telnet：远程登录（Telecommunications Network）
FTP：文件传输协议（File Transfer Protocol）
APT：高级持续性威胁（Advanced Persistent Threat）
DDos：分布式拒绝服务（Distributed Denial of Service）
IP：网络互连协议（Internet Protocol）
SL：网络安全领导力（Security Leadership）
PE：安全物理环境（Physical Environment）
SN：安全通信网络（Security Network）
RB：安全区域边界（Region Boundary）
CE：安全计算环境（Computing Environment）
SC：安全建设管理（Security Construction）
SO：安全运维管理（Security Operation）
MP：安全监测防护（Monitoring Protection）
SM：安全管理保障（Security Management）

5　网络安全业绩目标领域划分

核能行业网络安全业绩目标与评估准则是网络安全同行评估的核心文件。业绩目标与评估准则基于网络安全等级保护基本要求和关键信息基础设施保护要求，体现聚焦管理、增强网络安全领导力、着力网络安全管理改进的本质要求，符合“三分技术、七分管理”的客观规律和内在要求。通过同行评估方式，切实从“人的安全意识和安全行为以及管理缺陷”的角度，促进网络安全等级保护系列标准及关键信息基础设施保护要求有效落实。网络安全业绩目标分为网络安全领导力 SL、安全物理环境 PE、安全通信网络 SN、安全区域边界 RB、安全计算环境 CE、安全建设管理 SC、安全运维管理 SO、安全监测防护 MP 和安全管理保障 SM 共九大子领域，整体架构见图 1。

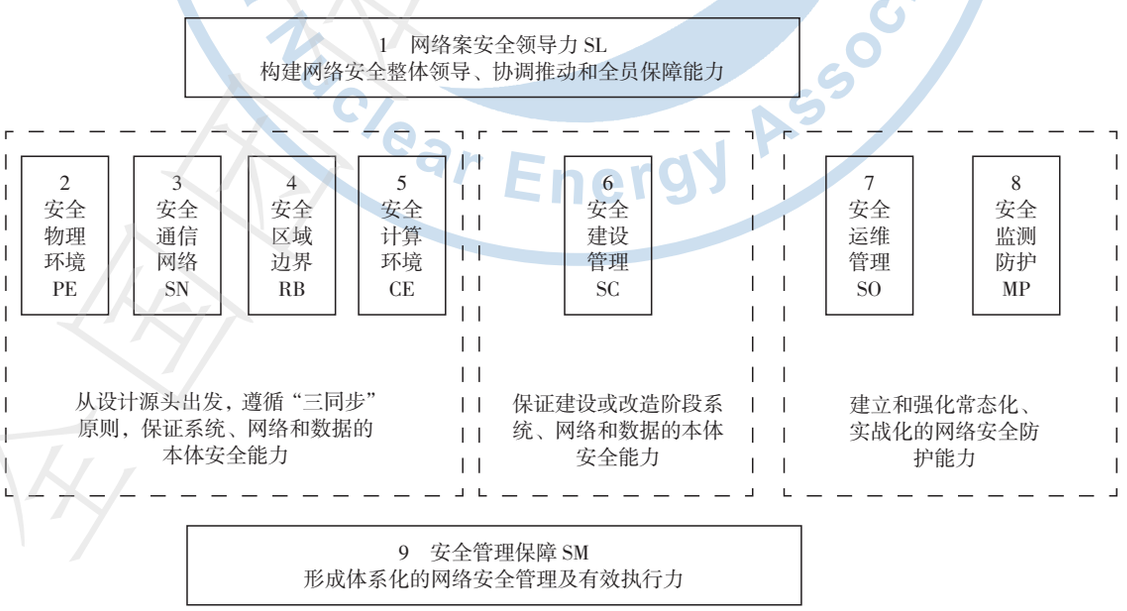

图 1　网络安全业绩目标体系架构图

6 网络安全领导力业绩目标与评估准则

6.1 网络安全观和承诺

6.1.1 以总体国家安全观为指导，准确认识和把握网络安全的特点和规律，研究确定企业网络安全观，对企业安全工作目标和方针做出承诺。该业绩目标的负责人是企业负责人。

6.1.2 网络安全观和承诺评估准则包括：

a ） 深刻认识网络安全工作的特点，准确把握和谋划网络安全工作；

b ） 经常审视外部网络安全形势和威胁，评估自身网络安全风险、隐患和威胁；

c ） 确定网络安全工作目标，对网络安全工作方针和政策做出承诺。

6.2 网络安全组织与责任

6.2.1 按照《中华人民共和国网络安全法》等法律法规和上级主管部门的要求，结合企业自身安全管控需要，设置明确网络安全工作领导、管理和专业技术组织；按照“谁主管谁负责、谁建设谁负责、谁运营谁负责、谁使用谁负责”的原则，落实网络安全工作责任制，层层分解落实责任。该业绩目标的第一责任人是企业负责人，直接责任人是企业主管网络安全的领导。

6.2.2 网络安全组织与责任评估准则包括：

a ） 明确网络安全工作主体责任、分管责任、职能管理监督和运行监测责任；

b ） 落实网络安全工作责任制，层层分解落实责任；

c ） 建立网络安全绩效考核办法并有效执行。

6.3 网络安全防御体系

6.3.1 构建全面有效的网络安全管理、技术、运维和监督四位一体综合防御体系，推动该体系有效执行和不断完善。该业绩目标的第一责任人是企业负责人，直接责任人是企业主管网络安全的领导。

6.3.2 网络安全防御体系评估准则包括：

a ） 建立企业网络安全管理、技术、运维和监督体系；

b ） 推动体系执行的有效性检查，提出持续改进要求；

c ） 通过网络安全同行评估等方式，发现体系设计或执行存在的问题，对标同行最佳实践，不断改进完善。

6.4 网络安全支持和促进

6.4.1 为支持和促进网络安全工作目标的实现，保障必要和持续的网络安全经费和人力投入，协调和促进网络安全纳入生产安全管理工作体系，支持网络安全等级保护和关键信息基础设施安全保护工作，推动风险、隐患和问题的发现和整改。该业绩目标的第一责任人是企业负责人，直接责任人是企业主管网络安全的领导。

6.4.2 网络安全支持和促进评估准则包括：

a ） 保证网络安全必要和持续的经费和人力投入；

b ） 促进将网络安全纳入生产安全管理工作体系，以生产管理方式管理网络安全；

c ） 以开展网络安全等级保护和关键信息基础设施安全保护工作为依托，持续推动风险、隐患和问题的发现和整改。

6.5 网络安全文化

6.5.1 推动网络安全文化纳入公司安全文化工作体系，强化网络安全工作中的“严、慎、细、实”作风和习惯，促进网络安全与业务工作相融合，促进与各相关领域的分工协作。该业绩目标的第一责任人是

企业负责人，直接责任人是企业主管网络安全的领导。

6.5.2 网络安全文化评估准则包括：

a ） 促进网络安全工作中形成“严、慎、细、实”的作风和习惯；

b ） 大力推行“网络安全人人有责，网络安全人人尽责”的全员网络安全防控理念；

c ） 促进与反恐安防、物业管理、保密管理、舆情管控等内部部门的协同；

d ） 加强与上级主管部门、外部标杆同行以及国家级权威专业技术机构之间的交流与合作。

6.6 网络安全规划与能力建设

6.6.1 通过指导、推进和协调网络安全专项规划制定与实施，支持网络安全专业人才培养，建立网络安全实验室和测试验证平台，加快核心技术和关键产品的自主可控研发或升级改造等措施，持续提升网络安全保障能力。该业绩目标的第一责任人是企业负责人，直接责任人是企业主管网络安全的领导。

6.6.2 网络安全规划与能力建设评估准则包括：

a ） 指导、推进和协调网络安全专项规划制定与实施；

b ） 创造条件建立网络安全实验室、工控系统测试验证平台 / 靶场等基础设施；

c ） 促进网络安全核心技术和关键产品的自主可控研发或升级改造工作；

d ） 明确并支持网络安全专业人才的培养和能力提升。

7 安全物理环境业绩目标与评估准则

7.1 物理位置选择

7.1.1 明确并制定机房场地、无线接入设备、物联网感知节点、室外控制设备等物理位置安全要求，确保云计算基础设施和大数据设备机房位于中国境内，从防震、防风、防雨、防水、防潮、防火、防盗、防强热源、防电磁干扰以及电力供应等方面采取合适的措施，保证机房设备设施的物理安全。该业绩目标的负责人是机房设施 / 系统专业负责人。

7.1.2 物理位置选择评估准则包括：

a ） 机房场地应选择在具有防震、防风和防雨等能力的建筑内（安全保护等级第二级及以上系统）；

b ） 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施（安全保护等级第二级及以上系统）；

c ） 应保证云计算基础设施位于中国境内；

d ） 应为无线接入设备的安装选择合理位置，避免过渡覆盖和电磁干扰；

e ） 感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动；

f ） 感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）；

g ） 感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡、屏蔽等（安全保护等级第三级及以上系统）；

h ） 关键感知节点设备应具有可供长时间工作的电力供应（关键网关节点设备应具有持久稳定的电力供应能力）（安全保护等级第三级及以上系统）；

i ） 室外控制设备放置于用铁板或其他防火材料制作的箱体或装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等；

j ） 室外控制设备放置应远离强电磁干扰、强热源等环境。如无法避免，应及时做应急处置及检修，保证设备正常运行；

k） 应保证承载大数据存储、处理和分析的设备机房位于中国境内（安全保护等级第二级及以上系统）。

7.2 机房安全防范

7.2.1 明确和执行机房物理访问与防盗窃、防破坏的安全要求、管理流程和记录表单，通过电子门禁系统、防盗报警系统、视频监控系统、专人值守等措施，实现机房出入安全控制，保证设备设施物理安全。该业绩目标的负责人是机房设施专业负责人。

7.2.2 机房安全防范评估准则包括：

a） 机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员（安全保护等级第三级及以上系统）；

b） 重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员（安全保护等级第四级及以上系统）；

c） 应将设备或主要部件固定，并设置明显的、不易除去的标记；

d） 应将通信线缆铺设在隐蔽安全处（安全保护等级第二级及以上系统）；

e） 应设置机房防盗报警系统或设置专人值守的视频监控系统（安全保护等级第三级及以上系统）。

7.3 机房物理防护

7.3.1 明确和执行机房物理安全防护要求、管理流程和记录表单，包括防雷击、防火、防水、防潮、防静电、电磁防护和温湿度控制等措施，保证机房设备设施物理安全。该业绩目标的负责人是机房设施专业负责人。

7.3.2 机房物理防护评估准则包括：

a） 应将各类机柜、设施和设备等通过接地系统安全接地；

b） 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等（安全保护等级第三级及以上系统）；

c） 机房应设置火灾自动消防系统，能够自动检测火情、自动报警并自动灭火（安全保护等级第二级及以上系统）；

d） 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（安全保护等级第二级及以上系统）；

e） 应对机房划分区域进行管理，区域之间设置隔离防火措施（安全保护等级第三级及以上系统）；

f） 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

g） 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（安全保护等级第二级及以上系统）；

h） 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（安全保护等级第三级及以上系统）；

i） 应采用防静电地板或地面并采用必要的接地防静电措施（安全保护等级第二级及以上系统）；

j） 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等（安全保护等级第三级及以上系统）；

k） 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（安全保护等级第二级及以上系统）；

l） 电源线和通信线缆应隔离铺设，避免互相干扰（安全保护等级第二级及以上系统）；

m） 应对关键设备或关键区域实施电磁屏蔽（安全保护等级第三级及以上系统）。

7.4 电力供应

7.4.1 通过配置稳压器和过电压防护设备、短期备用电力供应、设置冗余或并行供电线路和应急供电设施等措施，保证机房电力供应安全。该业绩目标的负责人是机房设施专业负责人。

7.4.2 电力供应评估准则包括：

a ） 应在机房供电线路上配置稳压器和过电压防护设备；

b ） 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求（安全保护等级第二级及以上系统）；

c ） 应设置冗余或并行的电力电缆线路为计算机系统供电（安全保护等级第三级及以上系统）；

d ） 应提供应急供电设施（安全保护等级第四级系统）。

8 安全通信网络业绩目标与评估准则

8.1 网络架构

8.1.1 制定和执行网络架构设计安全要求、管理流程和记录表单，从网络架构设计、网络区域隔离、设备、线路、IP 地址和带宽管理等方面采取策略，采用独立组网、物理隔离或单向隔离等措施，保证信息系统网络整体性能和安全可控。该业绩目标的负责人是网络 / 通信 / 应用专业负责人。

8.1.2 网络架构评估准则包括：

a ） 应保证网络设备的业务处理能力满足业务高峰期需要（安全保护等级第三级及以上系统）；

b ） 应保证网络各个部分的带宽满足业务高峰期需要（安全保护等级第三级及以上系统）；

c ） 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址（安全保护等级第二级及以上系统）；

d ） 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段（安全保护等级第二级及以上系统）；

e ） 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性（安全保护等级第三级及以上系统）；

f ） 应按照业务的重要程度分配带宽，优先保障重要业务（安全保护等级第四级系统）。

8.2 通信传输

8.2.1 制定和执行通信传输安全要求、管理流程和记录表单，通过应用密码技术，保证通信传输过程中数据的完整性和保密性。该业绩目标的负责人是通信 / 网络 / 保密专业负责人。

8.2.2 通信传输评估准则包括：

a ） 应采用校验技术或密码技术保证通信过程中数据的完整性（安全保护等级第三级及以上系统）；

b ） 应采用密码技术保证通信过程中数据的保密性（安全保护等级第三级及以上系统）；

c ） 应在通信前基于密码技术对通信的双方进行验证或认证（安全保护等级第四级系统）；

d ） 应基于硬件密码模块对重要通信过程进行密码运算和密钥管理（安全保护等级第四级系统）；

e ） 在工业控制系统内使用广域网进行控制指令或相关数据交换时，应采用加密认证技术手段实现身份认证、访问控制和数据加密传输（安全保护等级第二级及以上系统）。

8.3 云计算网络架构

8.3.1 制定和执行云计算网络架构安全要求、管理流程和记录表单，通过虚拟网络隔离，提供通信传输、边界防护和入侵防范等安全机制，自主设置安全策略，提供开发接口或开放性服务，设置安全标记和强制访问控制规则、通信协议转换或隔离以及独立资源池等措施，保证云计算网络架构使用安全。该业绩

目标的负责人是应用系统 / 云计算负责人。

8.3.2 云计算网络架构评估准则包括：

a ） 应保证云计算平台不承载高于其安全保护等级的业务应用系统；

b ） 应实现不同云服务客户虚拟网络之间的隔离；

c ） 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力（安全保护等级第二级及以上系统）；

d ） 应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略（安全保护等级第三级及以上系统）；

e ） 应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务（安全保护等级第三级及以上系统）；

f ） 应提供对虚拟资源的主体和客体设置安全标记的能力，保证云服务客户可以依据安全标记和强制访问控制规则确定主体对客体的访问（安全保护等级第四级系统）；

g ） 应提供通信协议转换或通信协议隔离等的数据交换方式，保证云服务客户可以根据业务需求自主选择边界数据交换方式（安全保护等级第四级系统）；

h ） 应为第四级业务应用系统划分独立的资源池（安全保护等级第四级系统）。

8.4 工控系统网络架构

8.4.1 制定和执行工控系统网络架构安全要求、管理流程和记录表单，通过落实“安全分区、网络专用、横向隔离、纵向认证”设计原则，采用独立组网、物理断开或单向隔离等措施，保证工控系统网络架构安全。该业绩目标的负责人是网络架构师 / 工控系统专业负责人。

8.4.2 工控系统网络架构评估准则包括：

a ） 将工控系统与企业其他系统划分为两个区域，区域间应采用符合国家或行业规定的专用产品实现单向安全隔离（安全保护等级第四级系统）；

b ） 工控系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段；

c ） 涉及实时控制和数据传输的工业控制系统应使用独立的网络设备组网，在物理层面实现与其他数据网及外部公共信息网的安全隔离（安全保护等级第二级及以上系统）。

8.5 大数据安全通信网络

8.5.1 通过保证大数据平台不承载高于其安全保护等级的大数据应用、分离大数据平台管理流量和系统业务流量等措施，保证大数据通信网络安全。该业绩目标的负责人是数据 / 网络 / 系统专业负责人。

8.5.2 大数据安全通信网络评估准则包括：

a ） 应保证大数据平台不承载高于其安全保护等级的大数据应用（安全保护等级第二级及以上系统）；

b ） 应保证大数据平台的管理流量与系统业务流量分离（安全保护等级第三级及以上系统）。

9 安全区域边界业绩目标与评估准则

9.1 边界防护

9.1.1 制定和执行边界防护安全要求、管理流程和记录表单，通过部署访问控制设备、非授权设备接入控制、用户非授权外联控制、无线网络管控和入网可信验证等措施，增强边界防护能力。该业绩目标的负责人是网络 / 应用系统专业负责人。

9.1.2 边界防护评估准则包括：

a） 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；

b） 应能够对非授权设备私自联到内部网络的行为进行检查或限制（安全保护等级第三级及以上系统）；

c） 应能够对内部用户非授权联到外部网络的行为进行检查或限制（安全保护等级第三级及以上系统）；

d） 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络（安全保护等级第三级及以上系统）；

e） 应能够在发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，对其进行有效阻断（安全保护等级第四级系统）；

f） 应采用可信验证机制对接入网络中的设备进行可信验证，保证接入网络的设备真实可信（安全保护等级第四级系统）。

9.2 边界访问控制

9.2.1 制定和执行边界访问控制安全要求、管理流程和记录表单，通过设置和优化访问控制规则、访问控制规则最小化、数据流进出控制、边界数据交换控制、接入认证和监控预警等措施，保证包括云计算、移动互联和工控系统等网络边界访问控制安全。该业绩目标的负责人是网络 / 应用系统专业负责人。

9.2.2 边界访问控制评估准则包括：

a） 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许的通信外受控接口拒绝所有通信（安全保护等级第二级及以上系统）；

b） 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

c） 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许 / 拒绝数据包进出；

d） 应能根据会话状态信息为进出数据流提供明确的允许 / 拒绝访问的能力（安全保护等级第二级及以上系统）；

e） 应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换（安全保护等级第四级系统）；

f） 应在工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务；

g） 应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警（安全保护等级第二级及以上系统）；

h） 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则（安全保护等级第二级及以上系统）；

i） 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；

j） 无线接入设备应开启接入认证功能，并支持采用认证服务器进行认证或国家密码管理机构批准的密码模块进行认证（安全保护等级第三级及以上系统）。

9.3 入侵、恶意代码和垃圾邮件防范

9.3.1 制定和执行防范入侵、恶意代码和垃圾邮件的安全要求、管理流程和记录表单，通过抗 APT 攻击、网络回溯、威胁情报检测、抗 DDos 攻击和入侵保护、病毒网关和防垃圾邮件网关等措施，有效防范和控制内外部入侵、恶意代码和垃圾邮件等安全危害。该业绩目标的负责人是网络 / 应用系统专业负责人。

9.3.2 入侵、恶意代码和垃圾邮件防范评估准则包括：

a） 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为（安全保护等级第三级及以上系统）；

b ） 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为（安全保护等级第三级及以上系统）；

c ） 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析（安全保护等级第三级及以上系统）；

d ） 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警（安全保护等级第三级及以上系统）；

e ） 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新（安全保护等级第二级及以上系统）；

f ） 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新（安全保护等级第三级及以上系统）。

9.4 边界安全审计和可信验证

9.4.1 制定和执行网络边界安全审计和可信验证技术要求、管理流程和记录表单，通过应用综合安全审计系统、堡垒机等系统以及审计记录保护和备份，实现边界安全审计和可信验证。该业绩目标的负责人是网络 / 安全监测专业负责人。

9.4.2 边界安全审计和可信验证评估准则包括：

a ） 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要的安全事件进行审计（安全保护等级第二级及以上系统）；

b ） 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（安全保护等级第二级及以上系统）；

c ） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等（安全保护等级第二级及以上系统）；

d ） 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启（安全保护等级第二级及以上系统）；

e ） 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计（安全保护等级第二级及以上系统）；

f ） 可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，将验证结果形成审计记录送至安全管理中心，并进行动态关联感知（安全保护等级第四级系统）。

9.5 云计算边界入侵防范

9.5.1 制定和执行云计算边界入侵防范安全要求、管理流程和记录表单，通过对网络攻击行为和异常流量的检测、记录和告警等方式，增强云计算边界入侵防范能力。该业绩目标的负责人是应用系统 / 云计算专业负责人。

9.5.2 云计算边界入侵防范评估准则包括：

a ） 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等（安全保护等级第二级及以上系统）；

b ） 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等（安全保护等级第二级及以上系统）；

c ） 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量（安全保护等级第二级及以上系统）；

d ） 应在检测到网络攻击行为、异常流量情况时进行告警（安全保护等级第三级及以上系统）。

9.6 移动互联边界防护和入侵防范

9.6.1 制定和执行移动互联边界防护和入侵防范安全要求、管理流程和记录表单，通过无线接入网关、终端准入控制、移动终端管理、抗 APT/DDos 攻击、网络回溯和威胁情报检测等措施，增强移动互联边界防护和入侵防范能力。该业绩目标的负责人是网络专业负责人。

9.6.2 移动互联边界防护和入侵防范评估准则包括：

a ） 应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备；

b ） 应能够检测到非授权无线接入设备和非授权移动终端的接入行为（安全保护等级第二级及以上系统）；

c ） 应能够检测到针对无线接入设备的网络扫描、DDos 攻击、密钥破解、中间人攻击和欺骗攻击等行为（安全保护等级第二级及以上系统）；

d ） 应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态（安全保护等级第二级及以上系统）；

e ） 应禁用无线接入设备和无线接入网关存在风险的功能，如 SSID 广播、WEP 认证等（安全保护等级第二级及以上系统）；

f ） 应禁止多个接入点使用同一个鉴别密钥（安全保护等级第二级及以上系统）；

g ） 应能够定位和阻断非授权无线接入设备或非授权移动终端（安全保护等级第三级及以上系统）。

9.7 物联网边界入侵防范和接入控制

9.7.1 制定和执行物联网边界入侵防范和接入控制安全要求、管理流程和记录表单，通过通信目的地址限制、渗透测试、设备接入控制等措施，增强物联网感知和网关节点设备的边界入侵防范能力。该业绩目标的负责人是通信 / 物联网专业负责人。

9.7.2 物联网边界入侵防范和接入控制评估准则包括：

a ） 应能够限制与感知节点通信的目的地址，以避免对陌生地址的攻击行为（安全保护等级第二级及以上系统）；

b ） 应能够限制与网关节点通信的目的地址，以避免对陌生地址的攻击行为（安全保护等级第二级及以上系统）；

c ） 应保证只有授权的感知节点可以接入。

9.8 工控系统边界防护

9.8.1 制定和执行工控系统边界防护安全要求、管理流程和记录表单，通过对无线通信用户身份鉴别和授权、传输加密、未经授权无线设备识别等安全管理与控制措施，增强工控系统边界防护能力。该业绩目标的负责人是工控系统专业负责人。

9.8.2 工控系统边界防护评估准则包括：

a ） 应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一标识和鉴别；

b ） 应对所有参与无线通信的用户（人员、软件进程或者设备）进行授权以及对执行和使用进行限制（安全保护等级第二级及以上系统）；

c ） 应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护（安全保护等级第三级及以上系统）；

d ） 对采用无线通信技术进行控制的工控系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰工控系统的行为（安全保护等级第三级及以上系统）。

10 安全计算环境业绩目标与评估准则

10.1 身份鉴别

10.1.1 制定并启用用户身份标识、身份鉴别、登录失败处理、远程控制、防窃听鉴别信息、密码技术组合鉴别、双向身份验证机制等安全控制措施，确保授权用户才能登录授权系统。该业绩目标的负责人是应用系统 / 网络 / 云计算专业负责人。

10.1.2 身份鉴别评估准则包括：

a ） 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

b ） 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

c ） 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听（安全保护等级第二级及以上系统）；

d ） 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现（安全保护等级第三级及以上系统）；

e ） 当远程管理云计算平台中的设备时，管理终端和云计算平台之间应建立双向身份验证机制（安全保护等级第三级及以上系统）。

10.2 访问控制

10.2.1 制定并执行用户账户和权限分配、默认账户及口令管理、多余 / 过期 / 共享账户管控、管理用户权限分离、访问控制策略、主体对客体的访问控制规则等安全要求，保证访问控制措施的有效性。该业绩目标的负责人是应用系统 / 网络专业负责人。

10.2.2 访问控制评估准则包括：

a ） 应对登录的用户分配账户和权限；

b ） 应重命名或删除默认账户，修改默认账户的默认口令；

c ） 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

d ） 应授予管理用户所需的最小权限，实现管理用户的权限分离（安全保护等级第二级及以上系统）；

e ） 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则（安全保护等级第三级及以上系统）；

f ） 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级（安全保护等级第三级及以上系统）；

g ） 应对主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问（安全保护等级第四级系统）。

10.3 安全审计

10.3.1 对每个用户启动安全审计，对重要的用户行为和安全事件进行审计，防止审计进程中断，审计记录完整并备份保护。该业绩目标的负责人是应用系统 / 网络 / 审计专业负责人。

10.3.2 安全审计评估准则包括：

a ） 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计（安全保护等级第二级及以上系统）；

b ） 审计记录应包括事件的日期和时间、事件类型、主体标识、客体标识和结果等（安全保护等

级第四级及以上系统）；

c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等（安全保护等级第二级及以上系统）；

d） 应对审计进程进行保护，防止未经授权的中断（安全保护等级第三级及以上系统）。

10.4 可信验证

10.4.1 根据安全保护对象的安全保护等级启用相应级别的可信验证安全机制。该业绩目标的负责人是应用系统 / 网络 / 安全专业负责人。

10.4.2 可信验证评估准则包括：

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知（安全保护等级第四级系统）。

10.5 入侵和恶意代码防范

10.5.1 推行最小安装原则，关闭不需要的系统服务、默认共享和高危端口，限制管理终端接入方式或网络地址范围，对人机接口或通信接口输入内容进行有效性验证，核查和修补高风险漏洞，重要节点和虚拟机防入侵，采用主动免疫可信验证机制，增强入侵和恶意代码防范能力。该业绩目标的负责人是应用系统 / 网络 / 安全专业负责人。

10.5.2 入侵和恶意代码防范评估准则包括：

a） 应遵循最小安装的原则，仅安装需要的组件和应用程序；

b） 应关闭不需要的系统服务、默认共享和高危端口；

c） 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制（安全保护等级第二级及以上系统）；

d） 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内容符合系统设定要求（安全保护等级第二级及以上系统）；

e） 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞（安全保护等级第二级及以上系统）；

f） 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警（安全保护等级第三级及以上系统）；

g） 应能够检测虚拟机之间的资源隔离失效，并进行告警（安全保护等级第三级及以上系统）；

h） 应能够检测非授权新建虚拟机或者重新启用虚拟机，并进行告警（安全保护等级第三级及以上系统）；

i） 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警（安全保护等级第三级及以上系统）；

j） 应采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断（安全保护等级第四级系统）。

10.6 数据完整性和保密性

10.6.1 推进（国产）密码技术应用，对鉴别数据、重要业务 / 审计 / 配置 / 视频 / 个人等信息，保证其在传输、存储和应用以及云服务模式下的完整性、保密性和合规性。该业绩目标的负责人是应用系统 / 网络 / 数据安全专业负责人。

10.6.2 数据完整性和保密性评估准则包括：

a） 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、

重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等（安全保护等级第三级及以上系统）；

b ） 应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等（安全保护等级第三级及以上系统）；

c ） 在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖（安全保护等级第四级系统）；

d ） 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等（安全保护等级第三级及以上系统）；

e ） 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等（安全保护等级第三级及以上系统）；

f ） 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；

g ） 应保证只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限（安全保护等级第二级及以上系统）；

h ） 应使用校验技术或密码技术保证虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施（安全保护等级第三级及以上系统）；

i ） 应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程（安全保护等级第三级及以上系统）。

10.7 数据备份恢复

10.7.1 建立和执行数据中心（包括租用云服务）数据备份恢复安全要求、操作流程和记录表单，实现重要系统热冗余以及重要数据的本地备份和恢复、异地实时备份、异地灾难备份等，保证系统和数据的高可用性及业务的连续性。该业绩目标的负责人是数据 / 系统 / 云计算专业负责人。

10.7.2 数据备份恢复评估准则包括：

a ） 应提供重要数据的本地数据备份与恢复功能；

b ） 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地（安全保护等级第三级及以上系统）；

c ） 应提供重要数据处理系统的热冗余，保证系统的高可用性（安全保护等级第三级及以上系统）；

d ） 应建立异地灾难备份中心，提供业务应用的实时切换（安全保护等级第四级系统）；

e ） 云服务客户应在本地保存其业务数据的备份（安全保护等级第二级及以上系统）；

f ） 应提供查询云服务客户数据及备份存储位置的能力（安全保护等级第二级及以上系统）；

g ） 云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致（安全保护等级第三级及以上系统）；

h ） 应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程（安全保护等级第三级及以上系统）。

10.8 剩余信息和个人信息保护

10.8.1 明确并执行剩余信息和个人信息保护的安全要求、操作流程和记录表单，保护鉴别信息、敏感数据和用户个人信息在采集、存储、使用、备份或删除全生命周期信息安全。该业绩目标的负责人是数据安全 / 保密专业负责人。

10.8.2 剩余信息和个人信息保护评估准则包括：

a ） 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除（安全保护等级第二级及

以上系统）；

b ） 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除（安全保护等级第三级及以上系统）；

c ） 应保证虚拟机所使用的内存和存储空间回收时得到完全清除（安全保护等级第二级及以上系统）；

d ） 云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除（安全保护等级第二级及以上系统）；

e ） 应仅采集和保存业务必需的用户个人信息（安全保护等级第二级及以上系统）；

f ） 应禁止未授权访问和非法使用用户个人信息（安全保护等级第二级及以上系统）。

10.9 云计算环境镜像和快照保护

10.9.1 明确并执行虚拟机镜像和快照的安全要求、管理流程和记录表单，采取操作系统安全加固、完整性校验和密码技术等手段，防止镜像或快照被恶意篡改或非法访问。该业绩目标的负责人是系统 / 云计算专业负责人。

10.9.2 云计算环境镜像和快照保护评估准则包括：

a ） 应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务（安全保护等级第二级及以上系统）；

b ） 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改（安全保护等级第二级及以上系统）；

c ） 应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问（安全保护等级第三级及以上系统）。

10.10 移动终端和应用管控

10.10.1 明确移动终端和应用管控安全要求，通过移动终端管理系统、证书签名和白名单等方式对移动终端和应用软件实施安全管控，有效防范针对移动终端和应用的攻击。该业绩目标的负责人是系统 / 应用专业负责人。

10.10.2 移动终端和应用管控评估准则包括：

a ） 应保证移动终端安装、注册并运行终端管理客户端软件（安全保护等级第三级及以上系统）；

b ） 移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如远程锁定、远程擦除等（安全保护等级第三级及以上系统）；

c ） 应具有选择应用软件安装、运行的功能；

d ） 应只允许指定证书签名的应用软件安装和运行（安全保护等级第三级及以上系统）；

e ） 应具有软件白名单功能，应能根据白名单控制应用软件安装、运行（安全保护等级第三级及以上系统）；

f ） 应保证移动终端只用于处理指定业务（安全保护等级第四级系统）；

g ） 应具有接受移动终端管理服务端推送的移动应用软件管理策略并根据该策略对软件实施管控的能力（安全保护等级第四级系统）。

10.11 物联网设备和数据安全

10.11.1 制定并执行物联网感知和网关等节点设备以及应用系统的安全策略、管理流程和记录表单，通过软件应用配置控制、身份标识和鉴别、关键密钥和配置参数在线更新、抗数据重放攻击等措施，保证物联网设备和数据安全。该业绩目标的负责人是物联网 / 系统 / 云计算专业负责人。

10.11.2 物联网设备和数据安全评估准则包括：

a ） 应保证只有授权的用户才可以对感知节点设备上的软件应用进行配置或变更（安全保护等级第三级及以上系统）；

b ） 应具有对其连接的网关节点设备（包括读卡器）进行身份标识和鉴别的能力（安全保护等级第三级及以上系统）；

c ） 应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力（安全保护等级第三级及以上系统）；

d ） 应具有对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力（安全保护等级第三级及以上系统）；

e ） 应具有过滤非法节点和伪造节点所发送的数据的能力（安全保护等级第三级及以上系统）；

f ） 授权用户应能够在设备使用过程中对关键密钥进行在线更新（安全保护等级第三级及以上系统）；

g ） 授权用户应能够在设备使用过程中对关键配置参数进行在线更新（安全保护等级第三级及以上系统）；

h ） 应能够鉴别数据的新鲜性，避免历史数据的重放攻击（安全保护等级第三级及以上系统）；

i ） 应能够鉴别历史数据的非法修改，避免数据的修改重放攻击（安全保护等级第三级及以上系统）；

j ） 应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用（安全保护等级第三级及以上系统）；

k ） 应对不同数据之间的依赖关系和制约关系等（例如：一类数据达到某个门限时会影响对另一类数据采集终端的管理指令）进行智能处理（安全保护等级第四级系统）。

10.12 工控系统控制设备安全

10.12.1 明确不同等级工控控制设备的安全要求、安全策略、控制措施和记录表单，通过身份鉴别、访问控制、安全审计、外设和端口最少化、上线前或维修中安全性检测或评估等方式，保证工控系统控制设备的安全运行和维护管理。该业绩目标的负责人是工控系统 / 设备专业负责人。

10.12.2 工控系统控制设备安全评估准则包括：

a ） 控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；

b ） 应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；

c ） 应关闭或拆除控制设备的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理（安全保护等级第三级及以上系统）；

d ） 应使用专用设备和专用软件对控制设备进行更新（安全保护等级第三级及以上系统）；

e ） 应保证控制设备在上线前经过安全性检测，避免控制设备固件中存在恶意代码（安全保护等级第三级及以上系统）。

10.13 大数据安全计算环境

10.13.1 依据核能行业数据分类分级规则，制定分级分类保护安全策略；建立和执行大数据平台、大数据应用和数据管理系统等安全要求、管理流程和记录表单，通过身份鉴别、访问控制、安全标记、数据脱敏、数据溯源、清洗转换控制、隔离存放、故障屏蔽、区分处置和集中管控等措施，保证大数据计算环境及

其应用安全。该业绩目标的负责人是应用系统 / 数据 / 云计算专业负责人。

10.13.2 大数据安全计算环境评估准则包括：

a ） 大数据平台应对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别；

b ） 大数据平台应能对不同客户的大数据应用实施标识和鉴别（安全保护等级第二级及以上系统）；

c ） 大数据平台应为大数据应用提供集中管控其计算和存储资源使用状况的能力（安全保护等级第二级及以上系统）；

d ） 大数据平台应对其提供的辅助工具或服务组件实施有效管理（安全保护等级第二级及以上系统）；

e ） 大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行（安全保护等级第二级及以上系统）；

f ） 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术（安全保护等级第二级及以上系统）；

g ） 对外提供服务的大数据平台，平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理（安全保护等级第二级及以上系统）；

h ） 大数据平台应提供数据分类分级安全管理功能，供大数据应用针对不同类别、不同级别的数据采取不同的安全保护措施（安全保护等级第三级及以上系统）；

i ） 大数据平台应提供设置数据安全标记功能，基于安全标记的授权和访问控制措施，满足细粒度授权访问控制管理能力要求（安全保护等级第三级及以上系统）；

j ） 大数据平台应在数据采集、存储、处理、分析等各个环节支持对数据进行分类、分级处置，并保证安全保护策略保持一致（安全保护等级第三级及以上系统）；

k ） 涉及重要数据接口、重要服务接口的调用，应实施访问控制，包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作（安全保护等级第三级及以上系统）；

l ） 应在数据清洗和转换过程中对重要数据进行保护，以保证重要数据清洗和转换后的一致性，避免数据失真，并在产生问题时能有效还原和恢复（安全保护等级第三级及以上系统）；

m ） 应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程，溯源数据满足合规审计要求（安全保护等级第三级及以上系统）；

n ） 大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力（安全保护等级第三级及以上系统）；

o ） 大数据平台应具备对不同类别、不同级别的数据全生命周期区分处置的能力（安全保护等级第四级系统）。

11 安全建设管理业绩目标与评估准则

11.1 定级备案和等级测评

11.1.1 按照国家和行业网络安全等级保护与关键信息基础设施保护管理要求和技术标准，落实网络安全“三同步”原则，规范、专业地开展网络与信息系统安全定级、论证审定、审批备案和测评整改，确保合规，促进设计、建设和运维等关键环节的安全水平提升。该业绩目标的负责人是网络信息管理 / 信息安全与保密专业负责人。

11.1.2 定级备案和等级测评评估准则包括：

a ） 应以书面的形式说明保护对象的安全保护等级以及确定等级的方法和理由；

b ） 应组织相关部门和有关安全设计专家对定级结果的合理性和正确性进行论证和审定（安全保护等级第二级及以上系统）；
c ） 应保证定级结果经过相关部门的批准（安全保护等级第二级及以上系统）；
d ） 应将备案材料报主管部门和公安机关备案（安全保护等级第二级及以上系统）；
e ） 应定期进行等级测评，发现不符合相应等级保护标准要求的问题及时整改（安全保护等级第二级及以上系统）；
f ） 应在发生重大变更或级别发生变化时进行等级测评（安全保护等级第二级及以上系统）；
g ） 应确保测评机构的选择符合国家有关规定（安全保护等级第二级及以上系统）；
h ） 被认定为关键信息基础设施的网络系统，应在上级主管部门登记备案，并开展相应检测评估。
i ） 在关键信息基础设施发生改建、扩建、所有人变更等较大变化时，应重新开展识别工作，可能影响认定结果的，应及时将相关情况报告保护工作部门，并更新资产清单；
j ） 应自行或者委托网络安全服务机构对关键信息基础设施安全性和可能存在的风险，每年至少进行一次检测评估，并及时整改发现的问题。

11.2 方案设计和产品采购

11.2.1 编制、论证和审定安全整体规划、安全专项方案和安全措施，审核验证拟采购网络安全产品、密码产品与服务的合规性，从方案设计、产品选型测试和专项测试等关键环节提升网络结构和系统本体安全能力。该业绩目标的负责人是信息安全与保密专业负责人 / 项目建设负责人。

11.2.2 方案设计和产品采购评估准则包括：

a ） 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
b ） 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含与密码技术和网络结构安全相关的内容，并形成配套文件（安全保护等级第三级及以上系统）；
c ） 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施（安全保护等级第三级及以上系统）；
d ） 应确保网络安全产品采购和使用符合国家的有关规定；
e ） 应确保密码产品与服务的采购和使用符合国家密码管理部门的要求（安全保护等级第二级及以上系统）；
f ） 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（安全保护等级第三级及以上系统）；
g ） 应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品（安全保护等级第四级系统）；
h ） 应强化采购渠道管理，保持采购的网络产品和服务来源的稳定或多样性。
i ） 采购网络关键设备和网络安全专用产品目录中的设备产品时，应采购通过国家检测认证的设备和产品。

11.3 软件开发

11.3.1 制定和执行软件开发安全要求、控制流程和记录表单，包括开发和运行环境、测试数据、开发过程控制、代码编写安全规范、安全性测试、软件源代码审查、程序资源库管控、软件设计文档控制、外包软件开发管理等，有效提升软件本体质量和抗攻击能力。该业绩目标的负责人是网络信息管理 / 软件专业负责人。

11.3.2 软件开发评估准则包括：

a ） 应将开发环境与实际运行环境在物理上分开，测试数据和测试结果受到控制（安全保护等级

第二级及以上系统）；

b ） 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则（安全保护等级第三级及以上系统）；

c ） 应制定代码编写安全规范，要求开发人员参照规范编写代码（安全保护等级第三级及以上系统）；

d ） 应具有软件设计的相关文档和使用指南，并对文档使用进行控制（安全保护等级第三级及以上系统）；

e ） 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测（安全保护等级第二级及以上系统）；

f ） 应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制（安全保护等级第三级及以上系统）；

g ） 应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查（安全保护等级第三级及以上系统）；

h ） 应在软件交付前检测其中可能存在的恶意代码（安全保护等级第二级及以上系统）；

i ） 应保证开发单位提供软件设计文档和使用指南（安全保护等级第二级及以上系统）；

j ） 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道（安全保护等级第三级及以上系统）。

11.4 工程实施与测试交付

11.4.1 制定和执行工程实施与测试交付安全要求、控制流程和记录表单，采用第三方监理，开展上线前安全性测试和运维人员技能培训，按要求完成设备、软件的测试验收和文档交付，有效夯实工程实施与测试交付环节的安全基础。该业绩目标的负责人是网络信息管理 / 项目建设负责人。

11.4.2 工程实施与测试交付评估准则包括：

a ） 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；

b ） 应制定安全工程实施方案控制工程实施过程（安全保护等级第二级及以上系统）；

c ） 应通过第三方工程监理控制工程实施过程（安全保护等级第三级及以上系统）；

d ） 应制定测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告（安全保护等级第二级及以上系统）；

e ） 应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容（安全保护等级第三级及以上系统）；

f ） 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

g ） 应对负责运行维护的技术人员进行相应的技能培训；

h ） 应保证提供建设过程文档和运行维护文档（安全保护等级第二级及以上系统）。

11.5 服务供应商选择

11.5.1 制定和执行服务供应商选择和使用的安全要求、控制流程和记录表单，通过服务协议、保密协议、定期审核、服务水平评价等措施，有效控制安全服务、云服务、数据服务等安全风险，提升供应链攻击防范能力。该业绩目标的负责人是网络信息管理 / 项目建设负责人。

11.5.2 服务供应商选择评估准则包括：

a ） 应确保服务供应商的选择符合国家的有关规定；

b ） 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务（安全保护等级第二级及以上系统）；

c ） 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制（安全保护等级第三级及以上系统）；

d ） 应选择安全合规的云服务商，云服务商提供的云计算平台应为其承载的业务应用系统提供相应等级的安全保护能力；

e ） 应在服务水平协议中规定云服务的各项服务内容和具体技术指标；

f ） 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；

g ） 应在服务水平协议中规定服务合约到期时完整提供云服务客户数据，并承诺将相关数据在云计算平台上清除（安全保护等级第二级及以上系统）；

h ） 应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据（安全保护等级第三级及以上系统）；

i ） 应将供应链安全事件信息或安全威胁信息及时传达到云服务客户（安全保护等级第二级及以上系统）；

j ） 应保证服务供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险采取措施对风险进行控制（安全保护等级第三级及以上系统）。

11.6 移动应用安全建设要求

11.6.1 制定和执行移动应用软件开发和安装使用安全技术要求，加强开发者或外包商的资格审查和安全监督，保证分发渠道或证书签名的安全可靠，有效控制移动应用成为攻击入口产生的安全风险。该业绩目标的负责人是网络信息管理 / 项目建设 / 应用专业负责人。

11.6.2 移动应用安全建设要求评估准则包括：

a ） 应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名；

b ） 应保证移动终端安装、运行的应用软件由指定的开发者开发（安全保护等级第三级及以上系统）；

c ） 应对移动业务应用软件开发者进行资格审查（安全保护等级第二级及以上系统）；

d ） 应保证开发移动业务应用软件的签名证书的合法性（安全保护等级第二级及以上系统）。

11.7 工控系统安全建设要求

11.7.1 制定和执行工控系统重要设备、开发单位和供应商安全和保密要求，开展安全性检测和供应商履责评估，有效控制重要设备供应、关键技术扩散和设备行业专用等方面的安全风险。该业绩目标的负责人是工控系统 / 项目建设专业负责人。

11.7.2 工控系统安全建设要求评估准则包括：

a ） 工控系统重要设备应通过专业机构的安全性检测后方可采购和使用（安全保护等级第二级及以上系统）；

b ） 应在外包开发合同中规定针对开发单位、供应商的约束条款，包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的内容（安全保护等级第二级及以上系统）。

11.8 大数据安全建设要求

11.8.1 明确选择大数据平台及服务的安全要求，通过服务合同、服务水平协议和安全声明等措施，保证数据、数据应用与服务的安全。该业绩目标的负责人是数据 / 系统 / 项目建设专业负责人。

11.8.2 大数据安全建设要求评估准则包括：

a ） 应选择安全合规的大数据平台，它应为其承载的大数据应用提供相应等级的安全保护能力（安

全保护等级第二级及以上系统）；

b） 应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容（安全保护等级第二级及以上系统）；

c） 应明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力（安全保护等级第三级及以上系统）。

12 安全运维管理业绩目标与评估准则

12.1 环境管理

12.1.1 建立和执行机房安全管理制度，明确安全管理责任人、人员和物品出入控制要求和机房设施维护作业规程，落实信息安全保密和重要安全区域实时监视等安全措施，确保各类机房和云计算平台等环境安全。该业绩目标的负责人是机房设施专业负责人。

12.1.2 环境管理评估准则包括：

a） 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

b） 应建立机房安全管理制度，对有关物理访问、物品进出和环境安全等方面的管理做出规定（安全保护等级第三级及以上系统）；

c） 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸质文件和移动介质等（安全保护等级第二级及以上系统）；

d） 应对出入人员进行相应级别的授权，对进入重要安全区域的人员和活动进行实时监视等（安全保护等级第四级系统）；

e） 云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵照国家相关规定（安全保护等级第二级及以上系统）。

12.2 资产和配置管理

12.2.1 建立和执行设备、软件和移动终端等IT资产管理规定、资产清单和分类管理措施，明确资产管理、系统管理和配置管理等关键责任人，记录和变更维护基本配置信息，确保资产和配置信息的及时、完整和准确。该业绩目标的负责人是安全监测负责人/各专业资产管理员。

12.2.2 资产和配置管理评估准则包括：

a） 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容（安全保护等级第二级及以上系统）；

b） 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（安全保护等级第三级及以上系统）；

c） 应对信息分类与标识方法做出规定，并对信息的使用、传输和存储等进行规范化管理（安全保护等级第三级及以上系统）；

d） 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等（安全保护等级第二级及以上系统）；

e） 应将基本配置信息改变纳入系统变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库（安全保护等级第三级及以上系统）；

f） 应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别（安全保护等级第三级及以上系统）。

12.3 设备维护和介质管理

12.3.1 建立和执行设备设施维护、介质和存储信息的管理规定和流程表单，明确设备维护和介质管理责任人，实现对设备维护过程与质量、介质及其存储信息的安全控制。该业绩目标的负责人是各专业负责人。

12.3.2 设备维护和介质管理评估准则包括：

a ） 应对各种设备（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；

b ） 应建立配套设施、软硬件维护方面的管理制度，对其进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维护过程的监督控制等（安全保护等级第三级及以上系统）；

c ） 信息处理设备应经过审批才能带离机房或办公地点。含有存储介质的设备带出工作环境时，其中的重要数据应加密（安全保护等级第三级及以上系统）；

d ） 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储介质专人管理，并根据存档介质的目录清单定期盘点；

e ） 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，并对介质的归档和查询等进行登记记录（安全保护等级第二级及以上系统）；

f ） 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用（安全保护等级第三级及以上系统）。

12.4 网络和系统安全管理

12.4.1 建立和执行网络和系统安全管理制度，明确各管理员角色及其责任和权限，制定重要设备的配置和操作手册并严格执行，严格审批和控制变更性运维、运维工具使用、远程运维开通以及与外部的连接，通过日志、监测和报警数据分析研判，及时发现可疑行为，有效管控网络和系统管理安全风险。该业绩目标的负责人是网络 / 系统 / 安全监测专业负责人。

12.4.2 网络和系统安全管理评估准则包括：

a ） 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；

b ） 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；

c ） 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面做出规定（安全保护等级第二级及以上系统）；

d ） 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等（安全保护等级第二级及以上系统）；

e ） 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容（安全保护等级第二级及以上系统）；

f ） 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为（安全保护等级第三级及以上系统）；

g ） 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库（安全保护等级第三级及以上系统）；

h ） 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据（安全保护等级第三级及以上系统）；

i ） 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道（安全保护等级第三级及以上系统）；

j ） 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为（安全保护等级第三级及以上系统）。

12.5 漏洞和恶意代码防范

12.5.1 建立和执行漏洞、隐患、恶意代码防范等安全要求和流程表单，定期开展安全测评，验证防范技术、措施和流程的有效性，及时采取改进措施。该业绩目标的负责人是网络 / 系统 / 安全监测专业负责人。

12.5.2 漏洞和恶意代码防范评估准则包括：

a ） 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；

b ） 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题（安全保护等级第三级及以上系统）；

c ） 应提高所有用户的防恶意代码意识，对外来计算机或存储设备在接入系统前进行恶意代码检查等；

d ） 应定期验证防范恶意代码攻击的技术措施的有效性（安全保护等级第三级及以上系统）。

12.6 密码管理

12.6.1 遵循密码相关国家标准和行业标准，使用国家密码主管部门认证的密码技术和产品，使密码管理与应用工作合规且有效。该业绩目标的负责人是信息安全与保密专业负责人。

12.6.2 密码管理评估准则包括：

a ） 应遵循密码相关国家标准和行业标准（安全保护等级第二级及以上系统）；

b ） 应使用国家密码管理部门认证核准的密码技术、产品和服务（安全保护等级第二级及以上系统）；

c ） 应采用硬件密码模块实现密码运算和密钥管理（安全保护等级第四级系统）。

12.7 变更管理

12.7.1 建立和执行变更管理规定、控制流程和记录表单，实现对变更需求、变更方案、变更申请、变更中止、变更恢复等环节的有效控制和书面记录。该业绩目标的负责人是安全监测 / 各专业负责人。

12.7.2 变更管理评估准则包括：

a ） 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施（安全保护等级第二级及以上系统）；

b ） 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程（安全保护等级第三级及以上系统）；

c ） 应建立中止变更并从失败变更中恢复的程序，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（安全保护等级第三级及以上系统）。

12.8 备份与恢复管理

12.8.1 建立和执行备份与恢复的策略、程序、方式、频度、存储介质、保存期等具体规定，确保重要业务信息、系统数据和软件系统持续可用。该业绩目标的负责人是数据 / 系统专业负责人。

12.8.2 备份与恢复管理评估准则包括：

a ） 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；

b ） 应规定备份信息的备份方式、备份频度、存储介质、保存期等；

c ） 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、备份程序和恢复程序等（安全保护等级第二级及以上系统）。

12.9 外包运维管理

12.9.1 通过签订外包运维服务协议等措施，明确外包运维服务商的法律义务、安全责任、安全运维能力、

信息保密和业务连续性保障等安全要求，并在履约过程中检查落实。该业绩目标的负责人是网络信息管理 / 外包管理负责人。

12.9.2 外包运维管理评估准则包括：

a ） 应确保外包运维服务商的选择符合国家的有关规定（安全保护等级第二级及以上系统）；

b ） 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容（安全保护等级第二级及以上系统）；

c ） 应保证选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确（安全保护等级第三级及以上系统）；

d ） 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等（安全保护等级第三级及以上系统）。

12.10 物联网节点设备管理

12.10.1 制定和执行物联网节点设备全过程管理规定，对其部署环境及环境的保密性等进行巡视、维护和记录，有效防范社会工程学攻击。该业绩目标的负责人是通信物联网专业负责人。

12.10.2 物联网节点设备管理评估准则包括：

a ） 应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护；

b ） 应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程做出明确规定，并进行全程管理（安全保护等级第二级及以上系统）；

c ） 应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等（安全保护等级第三级及以上系统）。

12.11 大数据安全运维管理

12.11.1 制定并执行数字资产安全管理策略、数据分类分级保护策略、重要数据脱敏使用、数据类别级别变更等管理规定、安全要求和记录表单，保证大数据运维和使用安全。该业绩目标的负责人是数据 / 系统专业负责人。

12.11.2 大数据安全运维管理评估准则包括：

a ） 应建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程（安全保护等级第二级及以上系统）；

b ） 应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施（安全保护等级第三级及以上系统）；

c ） 应在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程（安全保护等级第三级及以上系统）；

d ） 应定期评审数据的类别和级别，如需要变更数据的类别或级别，应依据变更审批流程执行变更（安全保护等级第三级及以上系统）。

13 安全监测防护业绩目标与评估准则

13.1 安全管理中心

13.1.1 建立安全管理中心，明确系统管理员、审计管理员和安全管理员的身份鉴别、操作规范及操作审计等安全要求，并分别执行集中系统管理功能、审计功能和安全管理功能的系统操作。通过安全管理中心的集中管控，实现网络安全状况的集中监测、安全事项的集中管理、审计数据的集中分析和各类安全事件的识别、报警、分析和处置，并保证这些安全设备或安全组件的独立性和安全性。该业绩目标的负责人是网络安全监测 / 系统专业负责人。

13.1.2 安全管理中心评估准则包括：

a ） 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计（安全保护等级第二级及以上系统）；

b ） 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、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等（安全保护等级第二级及以上系统）；

c ） 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计（安全保护等级第二级及以上系统）；

d ） 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等（安全保护等级第二级及以上系统）；

e ） 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计（安全保护等级第三级及以上系统）；

f ） 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，对主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等（安全保护等级第三级及以上系统）。

g ） 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控（安全保护等级第三级及以上系统）；

h ） 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理（安全保护等级第三级及以上系统）；

i ） 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测（安全保护等级第三级及以上系统）；

j ） 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求（安全保护等级第三级及以上系统）；

k ） 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理（安全保护等级第三级及以上系统）；

l ） 应能对网络中发生的各类安全事件进行识别、报警和分析（安全保护等级第三级及以上系统）；

m ） 应保证系统范围内的时间由唯一确定的时钟产生，以保证各种数据的管理和分析在时间上的一致性（安全保护等级第四级系统）。

13.2 云计算集中管控

13.2.1 针对云计算平台实现网络安全的集中管控，包括资源统一管理调度和分配、管理流量和业务流量分离、审计数据的收集和集中审计、安全状况的集中监测等。该业绩目标的负责人是系统 / 云计算专业负责人。

13.2.2 云计算集中管控评估准则包括：

a ） 应能对物理资源和虚拟资源按照策略做统一管理调度与分配（安全保护等级第三级及以上系统）；

b ） 应保证云计算平台管理流量与云服务客户业务流量分离（安全保护等级第三级及以上系统）；

c ） 应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计（安全保护等级第三级及以上系统）；

d ） 应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等运行状况的集中监测（安全保护等级第三级及以上系统）。

13.3 安全事件处置

13.3.1 制定和执行安全事件监测发现、通报预警、应急处置、根本原因分析和经验反馈的管理制度和流程表单，实现跨单位安全事件的联合防护和应急处置。该业绩目标的负责人是安全监测专业负责人。

13.3.2 安全事件处置评估准则包括：

a ） 应及时向安全管理部门报告发现的安全弱点和可疑事件；

b ） 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，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等（安全保护等级第二级及以上系统）；

c ） 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（安全保护等级第二级及以上系统）；

d ） 对造成系统中断和造成信息泄露的重大安全事件应采用不同的处理程序和报告程序（安全保护等级第三级及以上系统）；

e ） 应建立联合防护和应急机制，负责处置跨单位安全事件（安全保护等级第四级系统）。

13.4 应急预案管理

13.4.1 制定和执行统一的应急预案框架、重要事件应急预案和重大事件跨单位联合应急预案，定期开展应急预案的培训和应急演练，定期评估执行情况并修订完善。该业绩目标的负责人是信息安全与保密 / 安全监测专业负责人。

13.4.2 应急预案管理评估准则包括：

a ） 应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容（安全保护等级第三级及以上系统）；

b ） 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容（安全保护等级第二级及以上系统）；

c ） 应定期对与系统相关的人员进行应急预案培训，并进行应急预案的演练（安全保护等级第二级及以上系统）；

d ） 应定期对原有的应急预案重新评估，修订完善（安全保护等级第三级及以上系统）；

e ） 应建立重大安全事件的跨单位联合应急预案，并进行应急预案的演练（安全保护等级第四级系统）。

13.5 情报收集与利用

13.5.1 建立和执行网络安全情报收集利用的网络、责任和流程表单，实现情报全面快速收集、威胁分析研判和行动计划部署，有效预防控制潜在的网络安全风险。该业绩目标的负责人是安全监测专业负责人。

13.5.2 情报收集与利用评估准则包括：

a ） 应明确网络安全情报工作负责人，建立情报收集网络和情报员联系表（安全保护等级第二级

及以上系统）；

b ） 应建立网络安全情报工作流程，包括收集、汇总、去重、相关性分析、潜在影响研判以及应急行动决策和部署（安全保护等级第二级及以上系统）；

c ） 应评估和记录情报驱动的应急行动计划执行情况和效果，并开展经验反馈（安全保护等级第二级及以上系统）；

d ） 应关注国内外及行业关键信息基础设施安全事件、安全漏洞、解决方法和发展趋势，并对涉及的关键信息基础设施安全性进行研判分析，必要时发出预警。

13.6 值班值守

13.6.1 通过建立和执行网络安全值班值守工作机制和电子化工作平台，实现对网络安全状态的实时监测、事件的即时处置、任务的按时完成、经验的反馈整改和能力的持续提升。该业绩目标的负责人是安全监测专业负责人。

13.6.2 值班值守评估准则包括：

a ） 应建立和执行网络安全值班值守工作机制，（重要敏感期）应实现 7×24 小时值班值守，并编制值班值守监测日报（安全保护等级第三级及以上系统）；

b ） 应建立值班值守的预警机制和处置流程，实现事件的即时处置和通报预警（安全保护等级第三级及以上系统）；

c ） 应建立值班值守情报信息和安全事件跟踪管理电子化工作平台，实现处置事件和工作任务的闭环跟踪（安全保护等级第三级及以上系统）。

13.7 实战演练

13.7.1 通过邀请权威可信的网络安全专业机构，组织并管控专业攻击队伍开展全面或专项的实网实战攻击，全面深度发现网络安全弱项、隐患、风险和管理缺陷，为网络安全整改和能力提升提供有针对性的输入。该业绩目标的负责人是安全监测专业负责人。

13.7.2 实战演练评估准则包括：

a ） 应制订年度实网实战攻防演练工作计划，包括全面的攻防演练，或专项的渗透检测，或攻防沙盘推演（安全保护等级第三级及以上系统）；

b ） 应与负责组织攻击或检测的安全专业机构签订实施合同和保密协议（安全保护等级第三级及以上系统）；

c ） 应开展专项复盘总结，列举问题清单、根本原因和整改建议（安全保护等级第三级及以上系统）。

13.8 研判整改

13.8.1 基于网络安全技术监测、管理巡视、检查审计和实战攻防等问题和风险，建立和执行网络安全态势研判和整改提升工作机制，实现网络安全防护能力跨单位的全面持续有效的整改提升。该业绩目标的负责人是安全监测专业负责人。

13.8.2 研判整改评估准则包括：

a ） 应建立和执行网络安全态势分析研判报告和例会工作机制（安全保护等级第三级及以上系统）；

b ） 应通过例行会议机制进行整改项的闭环跟踪、协调和管理，实现有效整改（安全保护等级第三级及以上系统）。

14 安全管理保障业绩目标与评估准则

14.1 安全策略和管理制度

14.1.1 依据相关法律法规和业务要求，建立由安全策略、管理制度、操作规程和记录表单等构成的全面的网络安全管理制度体系，定期论证、审定、修订和正式发布，为网络安全工作提供指导、支持和保障。该业绩目标的负责人是网络信息分管领导 / 网络信息管理专业负责人。

14.1.2 安全策略和管理制度评估准则包括：

a ） 应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等（安全保护等级第二级及以上系统）；

b ） 应对安全管理活动中的各类管理内容建立安全管理制度（安全保护等级第三级及以上系统）；

c ） 应对管理人员或操作人员执行的日常管理操作建立操作规程（安全保护等级第二级及以上系统）；

d ） 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系（安全保护等级第三级及以上系统）。

e ） 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（安全保护等级第二级及以上系统）；

f ） 安全管理制度应通过正式、有效的方式发布，并进行版本控制（安全保护等级第二级及以上系统）；

g ） 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订（安全保护等级第二级及以上系统）。

14.2 岗位设置和人员配备

14.2.1 建立网络安全管理组织架构，设立关键岗位，配备合适人员，建立和执行领导有力、职责明确和分工协作的网络安全责任机制和工作机制。该业绩目标的负责人是网络信息分管领导 / 信息安全与保密专业负责人。

14.2.2 岗位设置和人员配备评估准则包括：

a ） 应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主要领导担任或授权（安全保护等级第三级及以上系统）；

b ） 应设立网络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（安全保护等级第二级及以上系统）；

c ） 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责（安全保护等级第二级及以上系统）；

d ） 应配备一定数量的系统管理员、审计管理员和安全管理员等（安全保护等级第二级及以上系统）；

e ） 应配备专职安全管理员，不可兼任（安全保护等级第三级及以上系统）；

f ） 关键事务岗位应配备多人共同管理（安全保护等级第四级系统）；

g ） 各级组织和人员均应有效履行自身网络安全责任，与他人高效协作开展工作（安全保护等级第二级及以上系统）。

14.3 授权审批和沟通合作

14.3.1 建立、维护和执行各部门和岗位对网络安全事项的授权审批程序、流程和表单，建立和维持内部各单位之间以及与外部单位的沟通与合作机制，及时发现、预测、分析和处置网络安全问题。该业绩目标的负责人是网络信息管理 / 信息安全与保密专业负责人。

14.3.2 授权审批和沟通合作评估准则包括：

a ） 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；

b ） 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（安全保护等级第三级及以上系统）；

c ） 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（安全保护等级第三级及以上系统）；

d ） 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题（安全保护等级第二级及以上系统）；

e ） 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通（安全保护等级第二级及以上系统）；

f ） 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（安全保护等级第二级及以上系统）。

14.4 安全检查和审计监督

14.4.1 定期开展常规和全面安全检查与审计监督，及时发现、报告和通报网络安全问题和风险，分析根本原因，制订整改计划，开展经验反馈，确保及时发现和有效整改网络安全问题，控制和预防类似安全风险。该业绩目标的负责人是内部审计 / 信息安全与保密专业负责人。

14.4.2 安全检查和审计监督评估准则包括：

a ） 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况（安全保护等级第二级及以上系统）；

b ） 应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（安全保护等级第三级及以上系统）；

c ） 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（安全保护等级第三级及以上系统）；

d ） 应建立和执行内部和外部独立的网络安全专项审计工作机制（安全保护等级第二级及以上系统）；

e ） 应对安全检查与审计监督发现的问题或风险进行根本原因分析，开展经验反馈，对整改计划执行有效性进行检查和监督（安全保护等级第二级及以上系统）。

14.5 人员录用和离岗

14.5.1 建立和执行人员录用和离岗安全要求、流程和表单，包括人员录用、审查和考核，签署保密协议、岗位责任协议，关键岗位人员选拔，管控调离和离岗权限及保密承诺等，有效控制人员录用和离岗产生的网络安全风险。该业绩目标的负责人是网络信息管理 / 信息安全与保密专业负责人。

14.5.2 人员录用和离岗评估准则包括：

a ） 应指定或授权专门的部门或人员负责人员录用；

b ） 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核（安全保护等级第三级及以上系统）；

c ） 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议（安全保护等级第三级及以上系统）；

d ） 应从内部人员中选拔从事关键岗位的人员（安全保护等级第四级系统）；

e ） 应及时终止离岗人员的所有访问权限，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；

f ） 离岗人员应办理严格的调离手续，并承诺调离后的保密义务后方可离开（安全保护等级第三级及以上系统）。

14.6 安全教育和培训

14.6.1 明确各类人员网络安全意识教育和岗位技能培训大纲与执行计划，按计划组织开展培训、考核和授权上岗，促进各类人员理解、掌握和执行公司网络安全方针、制度、技术标准和工作程序。该业绩目标的负责人是信息安全与保密专业 / 各部门负责人。

14.6.2 安全教育和培训评估准则包括：

a ） 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；

b ） 应针对不同岗位制订不同的培训计划，至少每年一次对网络安全相关人员进行培训，包括但不限于安全基础知识、岗位操作规程等，应该根据培训内容进行考核（安全保护等级第三级及以上系统）；

c ） 应定期对不同岗位的人员进行技能考核，对关键岗位人员考核合格后方可上岗（安全保护等级第三级及以上系统）。

14.7 外部人员访问管理

14.7.1 建立和执行外部人员访问安全要求、流程和表单，包括外部人员物理访问受控区域、接入受控网络访问系统、离场后访问权限清除、信息安全责任和保密义务等，有效控制因外部人员访问产生的相关网络安全风险。该业绩目标的负责人是网络信息管理 / 信息安全与保密专业负责人。

14.7.2 外部人员访问管理评估准则包括：

a ） 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案（安全保护等级第二级及以上系统）；

b ） 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案（安全保护等级第二级及以上系统）；

c ） 外部人员离场后应及时清除其所有的访问权限（安全保护等级第二级及以上系统）；

d ） 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息（安全保护等级第三级及以上系统）

e ） 对关键区域或关键系统不允许外部人员访问（安全保护等级第四级系统）。

参 考 文 献

[1] 《中华人民共和国网络安全法》
[2] 《电力监控系统安全防护规定》（国家发展改革委令第 27 号）
[3] GB/T 18336.1—2024 网络安全技术 信息技术安全评估准则 第 1 部分：简介和一般模型
[4] GB/T 22080—2016 信息技术安全技术 信息安全管理体系 要求
[5] GB/T 22081—2016 信息技术安全技术 信息安全控制实践指南
[6] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
[7] GB/T 28449—2018 信息安全技术 网络安全等级保护测评过程指南
[8] GB/T 31722—2015 信息技术 安全技术 信息安全风险管理
[9] GB/T 36572—2018 电力监控系统网络安全防护导则
[10] GB/T 37980—2019 信息安全技术 工业控制系统安全检查指南
[11] GB/T 38318—2019 电力监控系统网络安全评估指南
[12] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
[13] GB/T 41241—2022 核电厂工业控制系统网络安全管理要求
[14] GB/T 43206—2023 信息安全技术 信息系统密码应用测评要求
[15] DL/T 2613—2023 电力行业网络安全等级保护测评指南
[16] DL/T 2614—2023 电力行业网络安全等级保护基本要求

中国核能行业协会

核能行业网络安全业绩目标与评估准则

T/CNEA 228—2025

科学技术文献出版社

官方网址：www. stdp. com. cn

地址：北京市复兴路15号　邮编：100038

出版部：（010）58882941，58882087（传真）

发行部：（010）58882868，58882870（传真）

科学技术文献出版社发行　全国各地新华书店经销

北京虎彩文化传播有限公司印刷

开本：880×1230　1/16　印张：2.25　字数：56千

版次：2025年11月第1版　2025年11月第1次印刷

统一书号：155189·748

定价：34.00元

155189·748