ICS 33.040.01
CCS F230

CIIPA

团　　体　　标　　准

T/CIIPA 00014—2024

电力行业省级公司网络安全体系运营指南

Network Security System Operation Guidelines Of Provincial Companies In The Power Industry

（征求意见稿）

20XX-XX-XX 发布　　20XX-XX-XX 实施

中关村华安关键信息基础设施安全保护联盟　发布

目　　次

前　　言 4
引　　言 5
1 范围 6
2 规范性引用文件 6
3 术语和定义 6
4 缩略语 7
5 建设要求 7
5.1 总体要求 7
5.2 网络安全要求 7
5.3 数据安全要求 8
5.4 业务安全要求 8
6 安全管理体系 8
6.1 管理组织 8
6.2 管理制度 8
6.3 管理人员 9
6.4 建设管理 9
6.5 运营管理 10
6.6 监督管理 13
7 安全技术体系 13
7.1 网络安全技术架构 13
7.2 密码学应用 14
7.3 安全防护 15
7.4 监测感知 16
7.5 响应对抗 18
7.6 数据安全防护 19
7.7 统一安全支撑 20
7.8 新兴技术防护 20
8 安全保障体系 21
8.1 人才队伍 21
8.2 经费保障 21
8.3 宣传教育 21
8.4 重大活动安全保障 21

8.5 先进技术应用研究 21
9 安全运营体系 22
9.1 网络安全运营 22
9.2 业务安全运营 24
9.3 网络与业务安全联动 26

前　言

本文件按照《中关村华安关键信息基础设施安全保护联盟标准管理办法（暂行）》的要求，依据 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。

本文件由中关村华安关键信息基础设施安全保护联盟提出。

本文件由中关村华安关键信息基础设施安全保护联盟网络安全标准专业委员会技术归口和解释。

本文件起草单位：国家能源集团青海电力有限公司、国能青海黄河玛尔挡水电开发有限公司、国能信控技术股份有限公司、国富瑞数据系统有限公司、北京掌数信息技术有限公司、重庆巽诺科技有限公司、开元华创有限科技(集团)公司、中国电力科学研究院有限公司、北京地铁科技发展有限公司、甘肃赛飞安全科技有限公司、杭州中尔网络科技有限公司、天津市兴先道科技有限公司、北京网藤科技有限公司、成都创信华通信息技术有限公司。

本文件主要起草人：

本文件首次发布。

引　　言

电力行业作为关键基础设施行业，其网络安全运营的重要性不言而喻。电力行业省级公司网络安全运营体系建设不仅关乎企业自身的稳定运营，更对整个社会的能源供应和经济发展有着至关重要的影响。随着数字化进程的加速，电力行业省级公司面临的网络安全威胁日益复杂，其网络安全运营体系建设的规范化、标准化已成为行业发展的迫切需求。为此制定《电力行业省级公司网络安全体系运营指南》团体标准，旨在指导电力行业省级公司网络安全体系运营工作，提升其网络安全运营能力，确保电力行业省级公司的稳健运行。

本文件围绕电力行业省级公司网络安全体系运营工作，主要包括五大方面：一是建设要求，从总体要求、网络安全要求、数据安全要求、业务安全要求等角度，明确指出了网络安全运营体系建设的方向、目标和遵循的准则，确保建设过程的准确性和合规性。二是安全管理体系，详细制定了管理组织、管理制度、管理人员、建设管理、运营管理、监督管理等方面的标准和建议，构建了网络安全运营体系的管理框架，确保网络安全运营过程的有序性、规范性和高效性。三是安全技术体系，针对网络安全技术架构、密码学应用、安全防护、监测感知、响应对抗、数据安全防护、统一安全支撑平台、新兴技术安全防护等维度，提出了具体的技术标准和实施指南，为网络安全运营提供了坚实的技术支撑和保障。四是安全保障体系，明确了人才队伍、经费保障、宣传教育、重大活动安全保障、先进技术应用研究等方面的标准和指导，为网络安全运营工作提供全方位的保障和支持。五是安全运营体系，制定了网络安全运营、业务安全运营、网络与业务安全联动等方面的标准和流程，强化了网络安全运营的全流程管理和业务属性，确保运营过程的稳定性和安全性。

通过实施本文件，期望能够提升电力行业省级公司网络安全体系运营工作的规范化和标准化水平，进一步筑牢电力行业省级公司的网络安全防线，保障电力行业的稳定发展。

电力行业省级公司网络安全体系运营指南

1 范围

本文件提供了电力行业省级公司网络安全体系运营工作的建设要求、安全管理体系、安全技术体系、安全保障体系、安全运营体系等方面的工作指导。

本文件适用于电力行业省级公司的网络安全体系运营工作，也可供其他级别的组织参考使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅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（包括所有的修改单）适用于本文件。

GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求

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 37092-2018 信息安全技术 密码模块安全要求

GB/T 37138-2018 电力信息系统安全等级保护实施指南

DL/T 2613-2023 电力行业网络安全等级保护测评指南

DL/T 2614-2023 电力行业网络安全等级保护基本要求

GB/T 25069-2022 信息安全技术 术语

GB/T 20984-2022 信息安全技术 信息安全风险评估方法

3 术语和定义

GB/T 22239-2019、GB/T 25069-2022 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了 GB/T 22239-2019 和 GB/T 25069-2022 中的一些术语和定义。

3.1 网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[来源：GB/T 22239-2019，3.1]

3.2 业务安全 business security

保护业务系统免受安全威胁的措施或手段。

3.3 个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用就有可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注 1：个人敏感信息包括公民身份号码、个人生物特征信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等。

注 2：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的，也属于个人敏感信息。

[来源：GB/T 25069-2022，3.195]

3.4 实体 entity

存在或者可能存在的任何具体或抽象的事物，包括这些事物间的关系。

[来源：GB/T 25069-2022，3.550]

4 缩略语

下列缩略语适用于本文件。

HTTP：超文本传输协议（HyperText Transfer Protocol）

gRPC：gRPC 远程过程调用（gRPC Remote Procedure Call）

AMQP：高级消息队列协议（Advanced Message Queuing Protocol）

API：应用程序编程接口（Application Programming Interface）

FTP：文件传输协议（File Transfer Protocol）

USB：通用串行总线（Universal Serial Bus）

AI：人工智能（Artificial Intelligence）

IP：（在网络通信中）网际协议（Internet Protocol）

K-Means：K-Means 聚类算法（一种迭代求解的聚类分析算法）

ARIMA：自回归积分滑动平均模型（AutoRegressive Integrated Moving Average Model）

CPU：中央处理器（Central Processing Unit）

5 建设要求

5.1 总体要求

a）建立现代化网络安全运营体系，包括网络安全、数据安全、业务安全等方面；

b）具备物理层、网络层、应用层、数据层、供应链等多层面的安全防护能力；

c）符合国家法律法规和行业标准的要求，并结合单位自身的实际情况和特点，覆盖公司各项业务和流程；

d）明确责任分工和考核机制，确保各项安全措施有序执行；

e）包含安全管理体系、安全技术体系、安全保障体系和安全运营体系等内容。

5.2 网络安全要求

a）建立实战化、体系化与常态化的安全技术体系，具备密码应用、架构安全、安全防护、监测感知、响应对抗、统一安全支撑和新兴技术防护等能力；

b）建立安全保障体系，建全网络安全制度，明确组织、人员职能、经费保障等；

c）建立安全运营体系，形成安全事件的处置闭环。

5.3 数据安全要求

a）建立数据安全防护体系，具备数据识别、身份鉴别与访问控制、数据脱敏、数据防泄露、数据接口安全、数据备份恢复等能力；

b）建立个人信息保护机制。

5.4 业务安全要求

a） 建立风险控制体系，识别、评估、监控和应对业务过程中的安全风险；
b） 建立业务系统的数据采集、治理、分析能力；
c） 建立业务安全运营体系和与网络安全的联动体系。

6 安全管理体系

6.1 管理组织

6.1.1 组织设立

a） 成立网络安全工作委员会或领导小组,其最高领导由单位主管领导担任或授权,明确一名领导班子成员作为网络安全主要负责人,分管本组织范围内信息系统的网络安全保护工作；
b） 通过正式文件通告领导小组的成立；
c） 定义网络安全工作委员会或领导小组及成员的职责，按照职责文件开展网络安全工作体系建设和管理。

6.1.2 机构组成

a） 设立网络安全管理工作职能部门及各方面负责人，并定义部门及岗位职责。

6.1.3 沟通和联系

a） 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；
b） 建立外部组织联络机制，定期与电力监管机构、公安机关、网络安全职能部门、各类供应商、业界专家及安全组织进行合作沟通。

6.2 管理制度

6.2.1 总体方针

a） 制定网络安全总体方针，明确网络安全保护工作的目标，从管理体系、技术体系、保障体系、运营体系等方面进行规划；
b） 建立制度核查机制，涵盖等级保护、数据安全等方面。

6.2.2 管理制度

a） 建立安全管理制度，涵盖机房安全管理、办公环境安全管理、网络和系统安全管理、供应商管理、变更管理、备份和恢复管理、软件开发管理等方面；
b） 对日常管理操作建立配套操作规程，包括但不限于主机操作手册、数据库操作手册、网络设备操作手册、安全设备操作手册、应急处理手册、机房设施维护手册等；
c） 依据安全管理制度内容制定各类文档模板，记录制度执行情况并定期存档；

d） 制度要通过正式方式进行发布。

6.2.3 评审和修订

a） 制度管理部门定期进行制度的评审修订；
b） 除定期开展的制度评审以外，一旦公司网络体系或系统运行情况发生重大变化，需及时开展制度适用性和合理性评审。

6.2.4 制度移交

a） 当制度进行移交时，保证制度移交的完整性、规范性和可追溯性；
b） 当制度进行移交时，提供移交清单，移交清单应涵盖制度文件、执行记录、培训材料、测评报告等内容。

6.3 管理人员

6.3.1 录用及审查

a） 指定或授权专门的部门或人员负责人员录用；
b） 对被录用人员进行审查，审查通过方可从事相关岗位工作；
c） 签署保密协议，包括但不限于保密范围、保密责任、违约责任、协议有效期限和责任人签字等；
d） 签署岗位责任协议，包括但不限于岗位安全责任、协议有效期限和责任人签字等。

6.3.2 调动及离职

a） 人员发生工作调动时，需评估公司网络逻辑和物理访问权限，调整权限后应及时通知相关人员；
b） 人员离职时，及时终止或撤销与该人员相关的所有访问权限，归还公司资产、物料等软硬件设备；
c） 与离职人员签订离职保密协议，承诺离职后的保密义务。

6.3.3 培训及考核

a） 建立网络安全教育培训制度，定期开展安全意识教育和基本安全技能培训，为关键岗位人员提供专业安全技能培训；
b） 针对不同岗位制定培训计划，培训内容包括但不限于网络安全相关制度和规定、网络安全基础知识、网络安全保护技术、网络安全风险意识、岗位操作规程等；
c） 定期开展技术技能考核，考核结果进行记录并归档。

6.3.4 职责分离

a） 制定明确的管理要求，关键岗位职责要分离；
b） 遵循职责分离原则配置访问授权，以避免不当使用组织资产。

6.3.5 访问管理

a） 对申请资产访问权限（物理访问/逻辑访问）的人员(含外部人员)进行筛选；
b） 与获得公司访问权限（物理访问/逻辑访问）的人员(包含外部人员)签订保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息；
c） 外部人员离场后，及时清除其所有访问权限。

6.4 建设管理

6.4.1 保护对象定级、备案和测评

a) 以书面形式确定安全保护等级，并说明确定该等级所采用的方法及背后的理由，进而形成定级报告；
b) 组织相关部门和有关安全技术专家，对定级结果的合理性与正确性展开论证和审定工作；
c) 定级结果应获得上级部门的正式批准，并且将备案材料报送至能源局或其派出机构，以及所在地的公安机关进行；
d) 定期进行等级测评、商用密码应用安全性评估、风险评估等，不达标者及时整改；
e) 发生重大变更或级别发生变化时需重新进行等级测评、商用密码应用安全性评估、风险评估等；
f) 开展电力信息系统测评的机构需具备国家网络安全等级保护测评资质，且通过电力主管部门的技术能力评估认证，从事电力信息系统测评的技术人员需通过国家能源局组织的电力系统专业技术培训和考核。

6.4.2 安全防护、服务和产品采购

a) 实现网络安全技术措施与电力监控系统工程同步规划、同步建设、同步使用；
b) 依据保护对象安全保护等级匹配相应安全措施；
c) 根据保护对象安全保护等级进行整体规划和方案设计，并形成配套文件；
d) 对制定的整体规划及其配套文件的合理性和正确性展开论证和审定工作，重大项目要向行业网络安全监管部门进行报备；
e) 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，在设备选型时，应禁止选用被通报存在漏洞的系统及设备，对于已经投入运行的系统及设备，应及时进行整改；
f) 采购的重要设备及专用网络安全产品应通过电力行业实验室的安全性检测；
g) 确保供应商的选择符合国家及行业有关规定；
h) 与选定供应商签订协议时 ，应明确供应链各方需履行的网络安全义务；
i) 定期监督、评审和审核供应商提供的产品、服务。

6.4.3 软件开发、购买和系统建设

a) 将开发环境与实际运行环境物理隔离；
b) 制定软件开发管理制度和代码安全编写规范；
c) 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；
d) 供应商应委托电力实验室检测可能存在的恶意软件、后门和隐蔽信道等；
e) 在采购、开发合同中针对开发单位、供应商的约束条款中应包括有关保密、禁止关键技术扩散等方面内容；
f) 制定安全工程实施方案，并指定专门部门或人员负责工程实施过程的管理。

6.4.4 上线测试与验收

a) 制订测试验收方案，记录测试验收结果并形成测试验收报告；
b) 委托电力行业实验室进行上线前的安全性测试，测试内容包含漏洞分析、源代码安全检测和密码应用安全性测试等内容，并出具安全测试报告；
c) 制定交付清单，根据交付清单进行货物清点；
d) 对负责运行维护的技术人员进行相应的技能培训；
e) 提供建设过程文档和运行维护文档。

6.5 运营管理

6.5.1 存储介质管理

a) 在存储介质进行物理传输时，要对人员的选择、打包操作、交付环节等情况实施控制，详细记录介质的归档和查询操作；
b) 对重要数据和软件使用加密介质进行存储，根据其重要性对介质进行分类和标识管理；
c) 依据承载信息敏感程度匹配存储介质的处理方式和处理流程,存储介质的处理涵盖数据清除及存储介质销毁等操作；
d) 严格控制生产控制大区移动存储介质的使用,严格控制在生产控制大区和管理信息大区之间交叉使用移动存储介质，确需使用的应采用安全管理和技术监控手段；
e) 明确需要定期备份的重要业务信息、系统数据以及软件系统等，规定备份方式、备份频率、所使用的存储介质以及保存期限等；
f) 根据数据的重要性及其对系统运行的影响制定数据备份和恢复策略。

6.5.2 设备维护、漏洞管理和恶意软件防护

a) 对各种设备（涵盖备份和冗余设备）以及线路等，应指定专门的部门或人员进行定期的维护和管理工作；
b) 建立完善的配套设施、软硬件维护管理制度，管理制度应明确维护人员具体责任，规范维修和服务审批流程，并对维修过程进行监督和控制，确保维护工作规范有序；
c) 信息处理设备带离机房或办公地点应经过审批,含有存储介质的设备带出工作环境时需对其重要数据加密；
d) 含有存储介质的设备，在进行重用或报废操作前，应使用专用工具对其存储的数据信息实施完全清除处理,或者采用物理粉碎等不可恢复性销毁处理手段确保该设备上的敏感数据和授权软件无法被恢复并重新使用；
e) 采取必要措施来识别系统中存在的安全漏洞和隐患，对于一些较为复杂的情况，在修补之前，先评估其可能产生的影响，再实施相应的修补操作；
f) 外来计算机或存储设备接入系统之前，宜对其进行恶意软件检查；
g) 更新恶意软件库、入侵检测规则库时，应首先在测试环境中完成测试，测试通过后方可进行更新操作。

6.5.3 网络和系统安全管理

a) 将网络和系统的运维管理工作划分为不同的管理员角色，为每个角色明确其相应的责任和权限，并且在权限设定时遵循最小授权原则，确保权限的授予合理且必要，防止权限滥用和安全风险；
b) 指定专门的部门或人员来负责账户管理工作，对账户的申请、建立和删除等操作进行严格的控制，确保账户管理的规范性和安全性；
c) 建立完善的网络和系统安全管理制度，该制度对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁以及口令更新周期等多个方面进行详细规定，形成一套完整的网络和系统安全管理规范；
d) 制定重要设备的配置和操作手册，在设备的安全配置和优化配置等操作过程中，严格依据该手册进行操作，保障设备操作的标准化和安全性；
e) 详细记录运维操作日志，将日常巡检工作、运行维护记录、参数的设置和修改等信息纳入日志记录范围，为后续的运维分析和故障排查提供依据；
f) 安排专门的部门或人员对关键安全设备、服务器的日志、监测和报警数据等信息进行分析和统计，以便及时发现安全管理体系内存在的安全隐患和异常访问行为；
g) 把控变更性运维操作，在改变连接、安装系统组件或调整配置参数之前，需经过审批流程，在操作过程中要保留不可更改的审计日志，操作结束后要同步更新配置信息库，保证运维操作的可追溯性和系统配置的一致性；

h) 控制运维工具的使用，经过审批后可将其接入系统进行操作，在操作过程中，保留不可更改的审计日志，操作结束后删除工具中的敏感数据，避免敏感信息泄露；
i) 优先使用已在本组织登记备案的运维工具，若确实需要使用未登记备案的运维工具，在使用前对其进行恶意软件检测等相关测试，确保工具的安全性；
j) 严格禁止生产控制大区开通远程运维，生产控制大区中除安全接入区外，禁止选用具有无线通信功能的设备，禁止便携式和移动式设备接入网络；
k) 保证所有与外部的连接均得到授权和批准，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；
l) 电力调度机构指定专人负责管理本级调度数字证书系统。

6.5.4 配置和变更管理

a) 对基本配置信息进行记录和妥善保存，这些信息需涵盖网络拓扑结构、各个设备所安装的软件组件、软件组件的版本以及补丁信息；
b) 把基本配置信息的改变纳入系统变更范畴，对配置信息的改变实施严格控制，并且要根据配置信息的变更情况，及时对基本配置信息库进行更新操作，以保证信息库的准确性和时效性；
c) 在关键控制系统软件进行升级以及安装补丁之前，由专业的技术机构对其开展安全评估和验证工作，确保升级和补丁安装过程不会引入新的安全风险；
d) 在实施变更前，需根据变更需求制定变更方案，且要经过评审和审批流程之后才能够予以实施；
e) 建立变更的申报和审批控制程序记录变更实施过程；
f) 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；
g) 在进行变更操作之前，做好系统和数据的备份工作，对于那些可能对系统稳定运行产生影响的变更，在变更完成后要对系统的运行情况进行跟踪监测。

6.5.5 监测预警

a) 建立并落实常态化监测预警、快速响应机制，制定自身的监测预警和信息通报制度，确定网络安全预警分级准则，明确监测策略、监测内容和预警流程；
b) 关注国内外及行业安全事件、安全漏洞、解决方法和发展趋势，并对信息系统安全性进行研判分析，必要时预警；
c) 建立预警信息报告和响应处置程序，明确不同级别预警的报告、响应和处置流程；
d) 建立通报预警及协作处置机制，建立和维护外联单位联系列表。

6.5.6 安全事件处置

a) 若发生对关键业务造成危害的安全事件，需及时向安全管理机构汇报，并组织相关人员进行研判，最终形成事件报告；
b) 制定完善的安全事件报告和处置管理制度，明确不同类型安全事件的报告、处置以及响应流程；
c) 为网络安全事件的处置提供充足的资源保障，组织并建立专门的网络安全应急支撑队伍和专家队伍；
d) 在安全事件的报告和响应处理过程中，分析并鉴定事件产生的原因，同时做好证据的收集工作，详细记录处理过程；
e) 对于造成系统中断和信息泄漏的重大安全事件，分别采用不同的处理程序和报告程序；
f) 在完成关键业务和信息系统的恢复工作后，要对关键业务和信息系统的恢复情况进行全面评估，并采取有效措施防止关键业务和信息系统再次遭受破坏、危害或出现故障。

6.5.7 应急预案和演练管理

a) 制定针对各类重要事件的应急预案，该预案需涵盖应急处理流程、系统恢复流程等关键内容；
b) 在应急预案中需明确指出，当信息系统出现中断、受到损害或发生故障时，哪些关键业务功能需要进行维护，同时要明确在遭受破坏的情况下，恢复关键业务和全部业务所需的具体时间；
c) 在制定应急预案时，与内部的相关计划（如业务持续性计划、灾难备份计划等）以及外部的应急计划相协调，保证各计划之间的连贯性和一致性；
d) 应急预案中包含在非常规时期、遭受大规模攻击等特殊情况下的处置流程，确保在不同的复杂场景下都能有应对预案；
e) 不定期对系统相关人员开展应急预案培训工作，同时进行应急预案的演练活动；
f) 不定期对原有的应急预案进行重新评估，根据评估结果对其进行修订和完善，确保应急预案的有效性和实用性。

6.6 监督管理

6.6.1 安全监督管理制度制定

a) 建立健全网络安全监督管理、评价考核制度及相关标准要求；
b) 建立网络安全联席会议制度，协调推进网络安全监督管理工作；
c) 制定专用安全产品、安全服务监督管理要求。

6.6.2 监督管理机构

a) 明确有关职能部门负责安全监督管理工作，并配备安全监督管理人员；
b) 负责监督各部门、所属各单位全员安全责任制落实情况；
c) 组织开展单位内部安全监督检查，监督单位内部重大隐患整改；
d) 制定监督检查清单，包含安全策略、安全管理制度的执行情况等；
e) 协助做好安全事件报告、应急处置等有关工作，组织开展安全事件内部调查处理；
f) 强化网络安全协同监督管理,加强与网络安全主管部门、有关部门的沟通；
g) 组织或委托外部机构开展本组织范围内信息系统的评估、检查工作；
h) 推动网络安全防护技术能力建设，监督、检查本组织范围内信息系统的立项、建设、运行等过程中网络安全责任落实情况，监督、检查本组织范围内信息系统的设计、开发、运行、维护、更新改造等过程的网络安全工作落实情况；
i) 监督、检查本组织范围内信息系统的网络安全应急预案的编制、修订工作落实情况；
j) 监督、检查本组织范围内电力业务系统运行、维护、更新改造等过程的网络安全工作落实情况，组织制定电力业务系统安全保护计划。

6.6.3 安全监督实施

a) 定期进行安全监督，发现不符合要求的督促整改；
b) 安全监督组人数不少于 3 名，人员需来自单位内网络安全部门、业务部门和质量部门；
c) 安全监督结束后，要及时向被检查单位或部门反馈检查情况，提出处理意见；
d) 健全安全监督工作台账，加强跟踪督办，确保隐患和问题整改到位。

7 安全技术体系

7.1 网络安全技术架构

7.1.1 网络防护架构

a) 需识别电力业务系统的范围与安全防护边界，在此基础上规划网络防护架构；

b) 需划分网络区域，并制定安全互联和网络访问控制等安全策略。

7.1.2 分布式架构

a) 电力业务系统应采用分布式架构，将系统的组件分布在不同的网络节点如物理服务器、虚拟机或容器；
b) 通过网络进行节点之间通信，并采用标准协议（如 HTTP、gRPC、AMQP 等）以确保通信的可靠和安全；
c) 电力业务系统宜采用分布式服务等技术，提升应用和数据的高可用性；
d) 电力业务系统需具备高度容错能力，能够耐受部分节点的故障，并确保系统在高可用性状态下运行；
e) 电力业务系统宜实现健康检查、自动重启、故障转移等机制，以提高系统的容错性和稳定性；
f) 电力业务系统中采用缓存、异步处理、并行计算等技术手段来提升系统性能；
g) 电力业务系统中需具备完善的监控和调试功能，以便实时监控系统运行状态和性能指标；
h) 宜采用集中式日志管理、分布式追踪等技术和工具来提高系统监控能力。

7.1.3 冗余链路

a) 在电力业务系统中建立冗余链路的多电信运营商多路由保护能力；
b) 在电力业务系统中关键节点和重要设施建立“双节点”冗余能力；
c) 应保障网络设备的业务处理能力和带宽，以满足业务高峰期需要；
d) 建立电力业务系统链路切换能力，当主链路故障时，动态路由协议能够迅速切换到备用链路，确保数据传输的连续性；
e) 建立电力业务系统的快速故障检测能力，能够实时监测链路的健康状态。

7.1.4 冗余架构

a) 为电力业务系统配备足够的网络资源、计算资源、存储资源，在部分硬件发生故障时可自动切换至备用环境，确保电力业务系统的服务不中断；
b) 建设电力业务系统数据库安全能力，利用数据库复制技术（如主从复制、多主复制等）来实现数据同步；
c) 建设故障转移能力，当一个数据中心或节点故障时，能够迅速将流量转移到其他数据中心或节点上。

7.2 密码学应用

7.2.1 总体要求

a) 在业务系统规划阶段制定密码应用方案，并经第三方对方案进行评审；
b) 在业务系统建设阶段按照通过评审的密码应用方案进行建设，在业务系统投入运行前开展密码应用安全性评估，评估通过后方可正式上线运行，并在系统运行过程中定期开展密码应用安全性评估；
c) 在上线前对业务系统进行数字签名标准符合性测试，并出具测试报告；
d) 业务系统所用的密码产品需具有商用密码产品认证证书。

7.2.2 身份鉴别要求

a) 采用密码技术对业务系统登录用户进行身份鉴别，保证用户身份的真实性；
b) 采用密码技术实现业务系统身份鉴别信息的机密性保护。

7.2.3 数据保护要求

a) 采用数字签名技术实现对所传输和保存的业务数据、关键日志数据的数据完整性、真实性和不可否认性保护，数字签名运算宜在密码产品内部进行；
b) 采用密码技术实现对业务系统所存储的关键日志数据的数据完整性保护。

7.2.4 数据验证要求

a) 业务系统在接收到业务数据后，先对其进行数字签名验证，确定其合法性后才可以进行后续操作；
b) 业务系统对关键日志数据的数据完整性进行验证。

7.2.5 密钥管理要求

a) 密钥生成采用专用硬件密码卡/设备生成，并同步记录密钥关联信息；
b) 对称密钥分发采用密钥分散或真随机生成的形式进行安全下发，非对称密钥主要采用数字证书形式分发；
c) 密钥以密文方式存储，防止被非授权的访问或篡改，支持密钥外部加密存储；
d) 提供可靠的身份认证机制，确定服务使用者身份及访问权限，可防止服务使用者的数据被恶意访问、篡改、外泄等；
e) 密钥超过使用期限、已泄露或存在泄露风险时，支持根据密钥更新策略进行密钥更新；
f) 对系统历史密钥、被注销密钥进行归档，并对归档密钥进行加密处理再存储，归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；
g) 执行密钥备份后，同步生成审计信息；
h) 执行密钥恢复后，同步生成审计信息；
i) 具备用户密钥由于某些原因（暂时不使用、怀疑泄密等）进行密钥销毁的能力，销毁过程不可逆，即无法从销毁结果中恢复原密钥。

7.3 安全防护

7.3.1 应用安全

a) 建立资产管理与核查机制，形成资产、配置、漏洞、补丁的统一管理和运维能力；
b) 建立软件供应链安全机制，能够采用源代码分析技术分析代码层面、组件层面的脆弱性；
c) 建立进程级安全防护机制，采用必要的技术手段，防止应用软件被恶意中止。

7.3.2 系统安全

7.3.3 操作系统安全

a) 开启登录失败处理功能，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；
b) 重命名或删除默认账户，修改默认账户的默认口令，停用或删除多余的、过期的或弃用的账号，避免共享账号存在；
c) 授予管理用户所需的最小权限，实现管理用户的权限分离，系统不支持的宜部署日志服务器保证管理员的操作能够被审计，且特权用户管理员无权对审计记录进行操作；
d) 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，访问控制的粒度达到主体为用户级或进程级，客体为文件、数据库表级；
e) 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使用密码技术来实现；
f) 启用安全审计功能或利用生产控制大区、管理信息大区专用安全审计系统进行安全审计，审计覆盖每个用户，对重要的用户行为和重要安全事件进行审计；

g) 对审计记录进行保护，定期备份，保证审计进程无法被未授权中断，避免受到未预期的删除、修改或覆盖等；
h) 关闭非必要的系统服务、组件、高危端口、默认共享服务和远程管理等，如必须使用远程管理，使用如 SSH 等协议，防止鉴别信息在网络传输过程中被窃听；
i) 关闭多余的 USB 接口、网络接口、光盘驱动等硬件接口，对正在使用的硬件接口进行监控，确保现有硬件接口可控；
j) 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；
k) 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证并在检测到其可信性受到破坏后进行报警。

7.3.4 数据库安全

a) 对登录的用户进行身份标识和鉴别，身份标识应专人专用保证唯一性，身份鉴别信息应具有复杂度要求并定期更换；
b) 开启登录失败处理功能，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) 重命名或删除默认账户，修改默认账户的默认口令，应停用或删除多余的、过期的或弃用的账号，避免共享账号存在；
d) 授予管理用户所需的最小权限，实现管理用户的权限分离，系统不支持的部署数据库审计保证数据库的动作能够被审计，且特权用户管理员无权对审计记录进行操作；
e) 启用数据库的安全审计功能，审计覆盖每个用户，对重要的用户行为和重要安全事件进行审计；
f) 对审计记录进行保护，定期备份，保证审计进程无法被未授权中断，避免受到未预期的删除、修改或覆盖等；
g) 关闭数据库的远程管理功能，如必须使用远程管理，使用如 SSH 等协议，防止鉴别信息在网络传输过程中被窃听；
h) 通过设定终端接入方式或网络地址范围对通过网络管理的管理终端进行限制。

7.3.5 内容安全

a) 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；
b) 采用校验技术或密码技术保证重要数据在传输和存储过程中的完整性；
c) 采用密码技术保证重要数据在传输和存储过程中的保密性；
d) 提供重要数据的本地数据备份与恢复功能，备份数据能够完全恢复至备份执行时状态，数据保存期限符合国家相关规定；
e) 采用外设隔离手段，对进入系统的文件，进行授权和杀毒，防止恶意软件通过外设存储类设备进入系统；
f) 通过技术手段，对主机系统的外设接口进行管控，非必要接口进行技术封堵。

7.4 监测感知

7.4.1 恶意软件分析

a) 主机需安装防恶意软件或配置具有相应功能的软件；
b) 通过防恶意软件、网络流量在线监测等技术，快速、准确地监测和清除系统存在的恶意软件；
c) 针对主机恶意软件、网络流量恶意软件进行监测与分析。

7.4.2 漏洞扫描

a) 关闭不需要的系统服务、默认共享和高危端口；
b) 采用自动化扫描工具与手动测试相结合的方式，选择合适的漏洞扫描工具并定时更新；
c) 漏洞扫描对象包括主流操作系统、数据库、网络设备、应用程序等资产；
d) 发现可能存在的已知漏洞，在经过安全性、兼容性和稳定性等方面充分测试评估后，及时修补漏洞；
e) 根据系统的重要性和风险等级，制定合理的漏洞检测周期。对于关键系统和应用，应至少每年进行一次漏洞扫描；
f) 在扫描完成后生成详细报告，包括扫描过程中发现的问题、漏洞的严重性、修复建议等，报告能输出为通用的文档格式，可对扫描结果数据执行导入导出操作。

7.4.3 入侵检测

a) 在电力调度控制中心、变电站及发电厂监控系统及电力数据传输网络等关键网络节点处检测、防止或限制从内、外部发起的网络攻击行为；
b) 采取技术手段，实现对网络攻击特别是新型网络攻击行为的分析，实现系统主动防护，及时识别入侵和病毒行为；
c) 遵循最小安装原则，服务器、工作站等主机仅安装需要的组件和应用程序；
d) 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；
e) 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。

7.4.4 安全审计

a) 使用专用审计系统，或启用设备或系统的审计功能，对网络边界、重要网络节点进行安全审计；
b) 对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析；
c) 对电力业务系统工业协议深度解析，工业网络通信流量、内容、行为监控进行审计，对工业网络中的异常流量进行实时监测和告警；
d) 对提供接口的调用情况以及各类重要账号的操作情况进行审计；
e) 能实时将监视分析电力监控系统网络安全运行状态及可疑行为告警进行审计；
f) 调度主站、变电站、发电厂记录电力监控系统网络运行状态、网络安全事件的日志应保存不少于六个月；
g) 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；
h) 审计过程中应尽量避免对原始安全数据的重复采集；
i) 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；
j) 严格限制审计数据的访问控制权限，实现审计用户与其他用户的权限分离。

7.4.5 API 安全

a) 建立 API 风险的持续发现能力，实现 API 资产发现与管理、API 业务漏洞和第三方组件漏洞发现等功能；
b) 建立 API 威胁的持续检测能力，实现 API 漏洞攻击检测、逻辑异常攻击检测、异常行为检测等功能；
c) 建立 API 接口的数据异常流转及泄露检测，实现敏感数据识别、数据流转检测、失陷主机检测等功能；
d) 建立 API 接口的防护能力，实现认证授权、访问控制、加解密、API 限流限速等功能。

7.4.6 威胁情报

a) 建立内部威胁情报共享机制，组织联动上下级单位，开展威胁情报收集、加工、共享和处置等；
b) 建立外部威胁情报共享机制，与权威网络威胁情报机构开展协同，实现跨行业领域网络安全联防联控；
c) 具备威胁情报建设能力，威胁情报的内容至少包括：信息来源、更新时间、内容描述、关联事件、关联 IP 地址等；
d) 支持对不同来源的威胁情报进行汇聚并及时更新。

7.4.7 态势感知

a) 应建设基于数据分析的态势感知技术，以具备对高级威胁的对抗能力；
b) 集成先进的威胁检测技术，包括但不限于电力业务系统工业协议识别、行为分析、机器学习、人工智能等，对各类已知和未知威胁进行精准识别；
c) 建立网络安全监测预警机制，建设基于内置探针等的网络安全监测手段，实时监视分析电力业务系统网络安全运行状态及可疑行为；
d) 将与电力调度数据网相连的电力监控系统其网络安全运行状态及可疑行为告警信息同步传送至相应电力调度机构，监视过程中尽量避免对原始安全数据的重复采集；
e) 支持态势展示，包括但不限于对综合安全态势、安全事件态势、资产安全态势、流量态势、异常行为态势及威胁态势等进行展示；
f) 支持生成态势报告，根据数据分析、态势评估的结果生成整体网络安全状况分析报告并导出。

7.4.8 智能行为分析

a) 全面采集网络流量数据、系统日志、应用日志等关键信息，对采集到的数据进行预处理，包括数据清洗、去重、格式化等；
b) 学习异常行为、已知威胁和敏感操作，并结合电力行业特有的生产控制操作指令、行为基线、生产工艺模型，建立相应的电力行业行为分析模型；
c) 具备利用机器学习、人工智能等技术，对采集到的数据和行为分析结果进行智能分析与识别的能力；
d) 具备异常行为库，实时监测网络行为，与已建立的行为库进行对比，识别异常行为。

7.5 响应对抗

7.5.1 攻击面收敛

a) 建立攻击面收敛机制，利用网络空间测绘、入侵检测模拟、暗网监测等手段，减少单位的互联网暴露面；
b) 进行必要的互联网收口工作，定期检查多互联网出口的情况；
c) 减少对外暴露组织架构、邮箱账号、组织通信录等内部信息，防范社会工程学攻击；
d) 不宜在公共存储空间(代码托管平台、文库、网盘等)存储如网络拓扑图、源代码、互联网协议地址规划等可能被攻击者利用的技术文档。

7.5.2 攻击诱捕

a) 建立攻击诱捕机制，利用蜜罐、密网、密点等技术，实现定向攻击的监测能力。

7.5.3 应急响应

a) 建立应急响应技术能力，通过应急处置、通报预警、追踪溯源等手段来应对突发安全事件。

7.5.4 攻防演练

a) 建立红蓝对抗能力，保证一年不少于一次的定期攻防演练。

7.6 数据安全防护

7.6.1 数据识别

a) 配备技术能力，定期对相关平台系统数据资产进行扫描，通过工具的方式对数据资产进行动态管理，主要是元数据管理，并具备数据分类和分级的打标能力；
b) 能够发现识别个人敏感信息,定期对数据脱敏效果进行验证。

7.6.2 身份鉴别与访问控制

a) 建立用户、设备、应用系统的身份鉴别机制，确保身份标识具有唯一性；
b) 身份鉴别信息具备复杂度并定期更换,并要杜绝可绕过鉴别机制的访问方式存在；
c) 登录失败时采取结束会话、限制非法登录次数、设置抑制时间和网络登录连接超时自动退出等措施；
d) 当远程管理时，采取必要措施防止鉴别信息在网络传输中被窃听；
e) 处理重要数据的信息系统，采用口令技术、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鉴别；
f) 建立与数据类别级别相适应的访问控制机制情况,满足业务实际需要的最小化权限原则进行授权，并限定用户可访问数据范围；
g) 建立数据权限授权审批流程，明确用户账号分配、开通、使用、变更、注销等安全保障要求，对数据权限申请和变更进行审核，严格控制管理员权限账号数量；
h) 建立系统管理员、安全管理员、安全审计员等人员角色分离设置和权限管理；
i) 建立系统权限分配表并予以定期更新，用户账号实际权限应满足最少够用、职权分离原则；多余、重复、过期、离职人员的账户和角色应及时予以清除；
j) 数据批量复制、下载、导出、修改、删除等数据敏感操作宜采取多人审批授权或操作监督，并进行日志审计。

7.6.3 数据脱敏

a) 建立数据脱敏管理措施和技术措施，包括数据脱敏规则、脱敏方法和脱敏数据的使用限制、需要进行数据脱敏处理的应用场景、处理流程及操作记录等；
b) 建立静态数据脱敏和动态数据脱敏技术措施；
c) 对匿名化或去标识化处理的个人信息建立相关风险评估机制和保护措施。

7.6.4 数据防泄露

a) 涉及存储和处理重要数据和个人敏感信息的平台系统宜配备数据防泄露能力,优先从网络侧和终端侧等进行部署，逐步扩大能力覆盖范围；
b) 具备对网络、邮件、FTP、USB 等多种数据导入导出渠道进行实时监控的能力，及时对异常数据操作行为进行预警拦截，防范数据泄露风险。

7.6.5 数据接口安全

a) 建立面向互联网及合作方数据接口的接口认证鉴权与安全监控能力，限制违规接入，对接口调用进行必要的自动监控和处理；
b) 建立 API 密钥及密钥安全存储措施，避免密钥被恶意搜索或枚举；
c) 建立不同安全等级系统间、不同区域间跨系统、跨区域数据流动的安全控制措施；

d) 建立接口安全控制策略，包括规定使用数据接口的安全限制和安全控制措施，明确包括接口名称、接口参数等内容的数据接口安全要求；
e) 对涉及个人信息和重要数据的传输接口实施调用审批；
f) 定期对接口（特别是对外数据接口）进行清查，不符合要求的接口应立即关停；
g) 涉及敏感数据的接口调用应具备安全通道、加密传输、时间戳等安全措施；
h) 数据接口宜部署身份鉴别、访问控制、授权策略、接口签名、安全传输协议等防护措施；
i) 与接口调用方明确数据的使用目的、供应方式、保密约定及数据安全责任等；
j) 对接口访问做日志记录，同时对接口异常事件进行告警通知。

7.6.6 数据备份恢复

a) 建立数据备份恢复策略和操作规程，建立本地或异地数据灾备功能；
b) 定期开展数据备份恢复、备份和归档数据访问控制措施的有效性验证工作，并保留相关记录；
c) 定期采取必要的技术措施查验备份和归档数据完整性和可用性情况；
d) 定期开展灾难恢复演练，并保留相关记录。

7.6.7 个人信息保护

a) 对授权收集到的个人敏感信息，采取去标识化、关键字段加密安全存储措施；
b) 在跨安全域或通过互联网传输个人敏感信息时，采用加密传输措施(如可确保安全的加密算法或传输通道)；
c) 在用户端显示个人敏感信息时，采取技术措施防止未授权人员获取个人敏感信息。

7.7 统一安全支撑

7.7.1 网络安全统一管理平台

a) 建立全方位的资产信息、运行状态、脆弱性、安全威胁、攻击及影响、风险和安全管理水平感知能力；
b) 提供多种数据可视化技术与交互式安全分析手段,能够结合海量数据组合,发现网络安全事件。

7.7.2 业务安全统一管理平台

a) 能够利用 AI 技术对业务数据进行建模分析，持续学习业务数据、业务流程，为用户构建动态安全模型，对违模型的异常事件进行问题处置，从而发现对业务运行有实际影响的安全事件；
b) 能够将 AI 模型与安全场景结合，建立基于业务场景的安全分析能力；
c) 能够对规律性或随机性行为进行判断，并对破坏性操作或恶意行为进行预警；
d) 能够建立实体分析能力，实现人为操作行为、应用间调用行为、业务流程顺序规律、数据分布特性等实体的行为分析。

7.7.3 自动化处置平台

a) 能够基于工作流引擎、可视化剧本编辑技术，实现安全自动化编排能力；
b) 能够实现全方位、智能化、编排化与自动化的告警响应能力。

7.8 新兴技术防护

7.8.1 大数据安全

a) 建立大数据安全能力，对大数据应用提供安全监测技术手段和脆弱性发现能力。

7.8.2 人工智能技术

a） 建立人工智能安全能力，对人工智能应用提供安全监测技术手段和脆弱性发现能力。

7.8.3 区块链安全

a） 建立区块链安全能力，对区块链应用提供安全监测技术手段和脆弱性发现能力。

8 安全保障体系

8.1 人才队伍

a）每年组织网络安全方面的培训班、研讨会，提升运营团队人员的技能水平；
b）设立人才激励政策，对有突出贡献人员给予奖励；
c）依托高校、行业联盟、安全企业的网络安全实训基地，为运营团队人员提供系统化的技能提升路径；
d）网络安全运营的关键岗位应由本单位员工担任，符合人事相关规定，具备正式劳动合同，签订有保密协议。

8.2 经费保障

a）将网络安全工作经费纳入年度经费预算，并在正式的财务预算中列支专门的网络安全条目，内容可包含网络安全防护加固、升级改造、安全运维、检测评估、宣传教育、技能认证培训、安全应急处置等。

8.3 宣传教育

a） 不定期开展网络安全宣传周、主题日等活动，可利用海报、横幅、电子屏幕等多种形式宣传网络安全知识和最佳实践；
b） 建立单位网络安全文化，单位高层应树立良好榜样，可设立安全建议箱、奖励机制等方式；
c） 组织网络安全事件的模拟演练，强化应急处置流程，提升实战能力和应急处理能力；
d） 结合网络安全形势，邀请专家分享最新的网络安全政策法规、安全威胁、案例分析和防护措施等；
e） 组织订阅或印发期刊、安全手册等，宣传安全政策、操作规程和案例事件等，并维持更新手册、期刊更新，确保信息的时效性和实用性。

8.4 重大活动安全保障

a） 由单位网络信息安全领导小组负责重大活动网络安全保障工作的规划、组织和监督，可设立综合协调组、安全保障组、应急处置组等，各工作组定期召开协调会议，交流工作进展、问题和解决方案；
b） 制定重大活动安全保障工作方案，内容涵盖工作组织、保障内容、网络资产梳理、安全风险自查及整改、应急演练、教育培训、保障支撑、值班值守等，并明确工作完成时间；
c） 重大活动网络安全保障结束后对安全保障工作进行总结，形成专题报告，并向领导小组汇报和分享工作经验。

8.5 先进技术应用研究

a） 设立专项科研资金，用于支持网络安全先进技术应用研究项目，鼓励技术团队探索如人工智能、大数据分析、区块链等新兴技术在电力网络安全防护中的创新应用，不定期启动相关研究课题；

b) 积极与高校、科研机构开展产学研合作，建立联合实验室或技术研发中心，借助外部科研力量攻克电力网络安全领域的难题，合作开展重大项目，促进科研成果转化为实际的网络安全防护能力；
c) 跟踪国际、国内网络安全技术前沿动态，定期组织技术团队参加行业顶级技术研讨会、学术交流会议，参会人员返回后进行内部汇报分享，确保团队能及时掌握最新技术趋势；
d) 建立内部技术创新激励机制，对在网络安全先进技术应用研究方面取得突出成果、成功转化新技术到实际运营场景、发表高质量相关学术论文或专利的员工给予表彰与物质奖励；
e) 定期对新技术应用效果进行评估，以网络安全防护效能提升、运维成本降低、风险预警及时性等指标为衡量标准，依据评估结果及时调整技术研究方向与应用策略，确保先进技术切实服务于电力网络安全保障工作。

9 安全运营体系

9.1 网络安全运营

9.1.1 业务识别

a) 识别本组织的关键业务，并明确关键业务的范围分布、运营情况、影响范围、业务类别、业务逻辑等，测绘业务网络结构、区域分布、核心节点、业务接口等业务图谱，为掌握业务运行状态和安全态势提供支撑；
b) 分析识别本单位的关键业务和关键业务所依赖的外部业务，绘制关键业务网络、逻辑、边界、关联关系等图谱；
c) 当本单位关键业务为外部业务提供服务时，识别并标识关键业务对外部业务的重要等级；
d) 应及时发现业务关键属性的变化,并根据变化更新关键业务等级。

9.1.2 资产识别

a) 确定资产分类方法并进行资产识别，可根据资产的表现形式，将资产分为数据、服务、信息系统、平台或支撑系统、基础设施及人员等；
b) 基于资产类别、资产本身的重要性以及资产所支撑业务的重要性，对资产进行优先排序，确定资产防护优先级；
c) 应建立和维护各类资产清单，明确资产的管理部门与责任人；
d) 实现资产数据的统一管理，为安全防护、检测评估、监测预警主动防御、事件处置等安全活动提供数据或接口；
e) 建立健全资产管理制度，对资产上线、变更、下线等流程进行跟踪和管理，明确资产管理责任人及资产供应链；
f) 建立健全资产台账，定期识别未知或新增资产，动态确认并完善资产的各种属性，识别资产间的关联关系，绘制资产关联图谱；
g) 对资产属性变更进行监测和管理，对变更的敏感项进行记录和审核。

9.1.3 风险识别

a) 采用探测扫描、检测评估、渗透测试、情报共享等方式，对业务、资产、威胁、脆弱性及已有安全措施进行识别，分析主要安全风险点，确定风险处置的优先级，形成安全风险报告；
b) 评估资产价值及脆弱性的严重程度，判断安全事件造成的损失对组织的影响；
c) 采用风险识别动态管控技术手段，掌握风险危害程度、分布状况和态势信息，动态持续性开展风险识别和管理,掌握软硬件供应链安全风险状况,考虑极端情况下可能引发安全风险的要素。

9.1.4 安全防护

a） 具备唯一且确定的时钟，保证时间上的一致性；
b） 设立统一的安全策略库，将不同厂商、设备的安全策略根据模板通用格式进行统一入库登记，实现对策略的集中管控；
c） 具备对安全策略多维度视图展现、策略统计分析和安全策略查询的能力；
d） 对安全设备进行维护和管理，并结合安全运维实际工作的情况，对相关安全措施的有效性进行验证；
e） 确定资产安全现状和资产关联关系，评估安全缺陷或安全隐患的影响范围和严重程度；
f） 落实加固举措，安全加固前做数据备份、版本备份，分阶段、分批次有序开展安全加固举措、测试验证；
g） 通过测试、攻击等手段，针对安全加固后的系统验证其有效性。

9.1.5 检测评估

a） 电力行业省级公司自行或者委托网络安全服务机构对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；
b） 定期检查组织机构建设情况和人员投入情况；
c） 检查下属行业单位的信息基础设施网络安全专项经费落实情况、信息基础设施网络安全教育培训开展情况及网络安全等级保护制度落实情况；
d） 检查信息基础设施数据的使用、加工、传输、提供、公开、销毁等关键环节的数据安全性，检查数据备份恢复机制的落实情况；
e） 检查信息基础设施供应链安全保护情况，检查软件供应链的开源组件安全情况，检查供应链安全评估机制落实情况；
f） 在信息基础设施发生改建、扩建、所有人变更等较大变化时，自行或者委托网络安全服务机构进行检测评估,依据风险变化以及发现的安全问题进行有效整改后方可上线；
g） 出具评估报告，根据评估报告制定整改方案，进行合规整改，并针对建设整改结果开展评估复测。

9.1.6 监测预警

a） 在电力行业省级公司关键网络边界、网络出入口等网络关键节点部署攻击监测设备，发现网络攻击和未知威胁，并定期维护攻击监测设备的升级和更新；
b） 对关键业务所涉及的系统进行监测,对监测信息采取保护措施，防止其受到未授权的访问、修改和删除 ；
c） 全面收集网络安全日志，构建违规操作模型、攻击入侵模型、异常行为模型，强化监测预警能力 ；
d） 将关键业务运行所涉及的各类信息进行关联，并分析整体安全态势，通过安全态势分析结果来确定安全策略和安全控制措施是否合理有效；
e） 对网络安全共享信息和报警信息等进行综合分析、研判，必要时生成内部预警信息,对于可能造成较大影响的，应按照相关部门要求进行通报。

9.1.7 主动防御

a） 在不同等级的网络区域边界部署访问控制机制，设置优化的访问控制规则，访问控制粒度达到端口级；
b） 分析网络攻击的方法、手段，针对分布式拒绝服务攻击等各类攻击，采取有针对性的防护策略和技术措施，制定总体技术应对方案；

c） 针对监测发现的攻击活动，分析攻击路线、攻击目标，设置多道防线，采取捕获、干扰、阻断、封控、加固等多种技术手段，切断攻击路径，快速处置网络攻击；

d） 及时对网络攻击活动开展溯源，对攻击者进行画像，为案件侦查、事件调查、完善防护策略和措施提供支持。

9.1.8 事件处置

a） 在应急预案中明确，一旦信息系统中断、受到损害或者发生故障时，需要维护的关键业务功能，并明确遭受破坏时恢复关键业务和恢复全部业务的时间；

b） 在制定应急预案时，同所涉及的运营者内部相关计划以及外部服务提供者的应急计划进行协调，以确保连续性要求得以满足；

c） 在应急预案中包括非常规时期、遭受大规模攻击时等处置流程，并定期进行评估修订和持续改进；

d） 当遭受网络攻击，关键基础设施系统出现异常或者故障时，应立即启动应急预案，并联合采取紧急防护措施；

e） 根据检测评估、监测顶警、主动防御中发现的安全隐患或发生的安全事件以及处置结果开展风险评估工作。

9.2 业务安全运营

9.2.1 数据采集与管理

a)全面梳理公司业务流程，明确涉及业务运营各个环节的数据需求，界定数据采集范围，数据采集应涵盖客户基本信息、交易记录、操作日志、设备状态数据、市场数据等；

b）根据数据的特点和来源匹配相应的采集和存储方式，对于结构化数据，通过数据库查询接口定期获取，对于非结构化数据，采用日志采集工具进行实时或定时采集，对于外部数据，通过网络爬虫技术或与第三方数据提供商合作获取；

c）制定数据采集操作规范，明确数据采集的启动条件、执行步骤、数据传输方式及存储路径等；

d）确定合理的数据采集频率，对于实时性要求高的数据，如电力系统运行状态数据，进行秒级或毫秒级采集，对于变化相对缓慢的数据，如客户基本信息，可按天或周进行采集；

e) 在数据采集过程中设置数据校验环节，对采集到的数据进行格式、范围、完整性等方面的初步检查，确保数据质量；

f） 构建集中化的数据存储和管理平台，采用高性能、高可靠的数据库系统对业务数据进行分类存储；

g）根据数据的重要性、敏感性和使用频率等因素，划分不同的数据存储区域，并实施相应的访问控制策略。

9.2.2 行为规律学习与建模

a）对原始数据进行清洗、转换和归一化处理，去除噪声、填补缺失值并纠正格式，确保数据质量，为后续分析建模奠定基础；

b)从预处理后的数据中提取能够反映用户行为和系统运行特征的关键指标,如用户登录时间间隔、操作频率、交易金额分布、系统 CPU 使用率、内存占用率等；

c）依据业务与数据特点选择相应的机器学习算法构建行为模型，并划分训练集和测试集进行训练与优化，以准确率、召回率等指标衡量性能。

9.2.3 业务异常检测

a）将业务系统实时数据接入行为分析平台，利用实时计算技术与正常行为模型比对和分析，计算各项行为特征指标与模型中正常范围的偏离程度；

b）采用多维度检测方法，结合阈值、规则检测及关联分析技术，综合考虑用户行为、系统性能和业务流程等因素，提高异常检测准确性与全面性；

c）根据异常事件对业务安全的影响程度和紧急程度，将其划分为不同级别，针对不同级别的异常，制定相应的预警策略和通知方式；

d）在异常检测过程中，持续收集新产生的行为数据，不断更新行为画像，以适应业务变化。

9.2.4 安全策略优化

a)当发现异常情况后，应对异常事件进行深入分析，确定异常原因和可能影响范围，并根据分析结果，针对性地调整安全策略；

b)建立安全策略的动态优化机制，持续监测业务系统运行状态和安全态势，定期评估现有安全策略的有效性，引入人工智能和机器学习技术实现策略的自适应优化。

9.2.5 实时响应与处置

a）建立实时响应机制，确保在检测到业务安全事件或异常行为时能够迅速启动响应流程，该机制应明确响应的触发条件、责任人员、响应步骤和时限要求，确保相关人员能及时了解事件情况并展开行动；

b）制定应急处置预案，针对不同类型的业务安全事件，明确应急处置的具体措施、所需资源和协作部门，预案应经过定期演练和评估，确保其可操作性和有效性；

c）事件发生时，应按照预案迅速展开应急处置工作，包括但不限于隔离受影响的系统或设备、恢复受损的业务功能、收集和分析事件信息等；

d）积极引入自动化响应与处置机制，分析不同业务安全事件的场景，制定相应的应急响应剧本，剧本应涵盖事件的识别、分析、响应和处置等环节；

e）实施持续监控和评估，确保应急处置工作的有效性和及时性；

f）事件处置过程中，实时记录处置过程和结果，包括采取的措施、消耗的资源、处置的效果等；

g）处置结束后，组织相关部门对事件进行复盘和分析，总结经验教训，完善应急处置流程和预案；

h）建立应急响应效果反馈机制，根据事件处置的结果和反馈，不断调整和优化应急响应流程和措施。

9.2.6 持续优化与闭环反馈

a）在业务安全事件处置完成后，组织相关部门和人员对事件进行复盘；

b）根据事件复盘结果对业务安全运营流程和安全策略进行优化调整，同时对应急预案进行更新和完善，补充新的应急场景和处置措施；

c）定期组织培训和演练活动；

d）建立全面的持续优化机制，包括数据采集与管理、行为规律学习与建模、业务异常检测以及实时响应与处置等，通过定期回顾和评估，发现潜在问题，提出改进方案，并持续跟踪实施效果，确保业务安全运营的持续优化和改进；

e）积极探索人工智能、大数据、云计算等技术在业务安全运营中的应用，提升业务安全运营的智能化和自动化水平；

f）建立闭环反馈机制，对问题进行跟踪和记录，确保问题得到及时解决，并总结经验教训，完善相关流程和预案。

9.2.7 业务安全运营成效评估

a）从业务系统安全性（漏洞发现与修复、安全事件情况、入侵检测准确率等）、业务连续性（系统可用率、中断时长等）和数据完整性（错误率、丢失率、一致性检查通过率）等维度构建科学合理的评估指标体系，明确各指标定义、计算方法和目标值；

b）定期收集安全监测、运维管理和业务系统日志等数据，依计算方法得出各指标实际值，如通过漏洞扫描工具获取数据计算漏洞修复率、从监控平台数据计算系统可用率，保证数据准确完整以确保评估可靠；

c）运用数据分析方法对比各项指标的实际值与目标值，评估业务安全运营工作的效果，通过趋势分析判断业务安全状况的增减趋势，并分析指标间相关性，找出影响业务安全运营成效的关键因素；

d）根据评估分析结果，形成详细的业务安全运营成效评估报告，向公司管理层和相关部门汇报，报告明确指出业务安全运营工作取得的成绩、存在的问题及改进建议；

e）将评估结果与绩效考核挂钩，激励员工积极参与业务安全运营工作，推动业务安全运营工作不断优化和提升。

9.3 网络与业务安全联动

9.3.1 信息共享与协同机制

a）构建安全信息共享平台，整合网络攻击日志、漏洞报告、业务异常数据和用户权限变更记录等信息，方便安全与业务部门查询调用；

b）明确规定信息共享的范围、方式、频率和权限管理等内容，定期推送网络安全态势信息，并建立严格审核机制；

c）成立跨部门安全协同团队，定期组织安全例会，共同分析研讨共享信息，评估网络安全对业务影响及业务变化对网络安全的需求。

9.3.2 联动响应策略

a）检测到攻击或异常流量时，及时传递信息给业务部门，业务部门据此采取暂停业务操作、调整访问策略和加强数据保护等措施；

b）业务部门发现异常情况（如异常交易、用户登录异常）应通知网络安全团队；

c）针对影响极大且处置明确的异常场景，宜关联分析网络与业务安全策略，并建立自动处置机制。

9.3.3 联合演练与培训

a）制定联合应急演练计划，模拟各种复杂的网络安全事件场景制订应急预案；

b）演练过程中，网络安全团队和业务部门按照预定的联动响应流程协同作战，检验和优化双方在信息共享、应急响应、协同处置等方面的配合能力；

c）演练结束后，组织全面的复盘会议，分析演练过程中存在的问题和不足，针对性地修订和完善联动应急预案；

d）开展面向全体员工的联合安全培训，涵盖网络安全基础、业务系统安全操作规范、联动机制和应急处置流程等内容。

9.3.4 持续改进与优化

a） 建立网络与业务安全联动效果指标体系，包括但不限于信息共享及时性（如从安全事件发生到相关信息传递至业务部门的时间间隔）、联动响应速度（如从发现异常到采取有效防护措施的时间）、业务系统因网络安全事件导致的损失减少率、安全策略调整的有效性（如调整后的策略对防范类似安全事件的成功率）等；

b） 定期收集和分析指标数据，客观评价联动机制的运行效果；

c） 定期进行联动效果评估，找出联动机制中存在的薄弱环节和问题点，制定针对性的改进措施。