ICS 35.040
CCS L80

TD

中华人民共和国土地管理行业标准

XX/T XXXXX—XXXX

自然资源网络安全保护技术规范

Technical specifications for cybersecurity protection of natural resources

(点击此处添加与国际标准一致性程度的标识)

（报批稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国自然资源部　　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。

本文件由中华人民共和国自然资源部提出。

本文件由全国地理信息标准化技术委员会（SAC/TC230）归口。

本文件起草单位：自然资源部信息中心、重庆市规划和自然资源信息中心、深信服科技股份有限公司、杭州安恒信息技术股份有限公司、绿盟科技集团股份有限公司、国家海洋信息中心、中国地质调查局、国家林业和草原局信息中心、国家基础地理信息中心、自然资源部国土卫星遥感应用中心、国家卫星海洋应用中心、中国测绘科学研究院、北京航空航天大学、浙江省自然资源厅信息中心。

本文件主要起草人：于志刚、李泽慧、王颖、李正、兰小强、徐沛东、乔时、蒋巍巍、王永刚、范其乐、余前佳、张延德、魏奇、王建兵、邬阳、吴伟民、周春磊、闫晓楠、韩伟、周舟、顾红波、赵根、孙华清、卢文虎、马照亭、马小龙、关振宇、边松、孙东明、刘磊、王新春、胡轶之、刘金普、王菁玉、孔勇。

引　言

为落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》《网络数据安全管理条例》等法律法规要求，基于国家网络、数据安全相关标准规范以及2024年自然资源部印发的《自然资源数字化治理能力提升总体方案》相关要求，借鉴自然资源部近年来开展网络安全保护工作的成熟经验，结合自然资源行业特色，针对性设计了网络安全防护体系，为各单位网络安全建设提供标准化、规范化和科学化指引，切实提升自然资源网络安全管理和防御水平，制定本文件。

自然资源网络安全保护技术规范

1 范围

本文件规定了自然资源网络安全保护框架、安全管理要求、安全技术要求、安全运营要求等方面的安全保护规范。

本文件适用于网络安全等级保护等级为二级及以上的自然资源领域保护对象的网络安全保护。

本文件不适用自然资源部涉密内网（政务内网）的建设。

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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 网络安全等级保护定级指南

GB/T 25069 信息安全技术 术语

GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 38674 信息安全技术 应用软件安全编程指南

GB/T 39204 信息安全技术 关键信息基础设施安全保护要求

GB/T 42884 信息安全技术 移动互联网应用程序（App）生命周期安全管理指南

3 术语和定义

GB/T 25069、GB/T 22239、GB/T 25070界定的以及下列术语和定义适用于本文件。

3.1

自然资源“一张网” a network of natural resources

承担国家公共通信、自然资源信息传输的业务网、政务外网、政务内网等信息网络。

注：自然资源部涉密内网（政务内网）、业务网（信息交换域）、政务外网（互联网），本文件涉及的网络不包括涉密内网（政务内网）。

[来源：GB/T 25069-2022,3.261,有修改]

3.2

自然资源云 natural resource cloud

由硬件资源和资源抽象控制组件构成，支撑自然资源云计算的基础设施。

注：基于自然资源“一张网”建设的自主可控分布式算力基础设施，由自然资源部数据中心及测绘、卫星、土地、海洋、地质等数据中心构成。在自然资源部数据中心的“自然资源云”管理平台，实现对各数据中心计算、存储、网络等算力资源的统一管理和动态调度，为各单位提供云服务。

[来源：GB/T 25069-2022,3.758,有修改]

3.3

数据 data

信息的可再解释的形式化表示，以适用于自然资源领域通信、解释或处理。

注：自然资源数据主要包括基础地理信息、遥感影像等地理信息数据，测绘、地质、林草、海洋等自然资源调查监测数据，总体规划、详细规划、专项规划等国土空间规划数据，用途管制、资产管理、耕地保护、生态修复、开发利用、不动产登记等自然资源管理数据。

[来源：GB/T 35295-2017,2.2.1,有修改]

3.4

应用系统 application system

在约定的业务环境下，用于实现用户特定需求的应用软件及其运行的软环境和承载业务直接关联的数据。

注：包括国土空间信息基础平台，基于平台构建的智能工具集，以及底线守护、格局优化、绿色低碳及权益维护四大主题场景涉及的应用系统。

3.5

主机 host

在基于传输控制协议/互联网协议（TCP/IP）的网络（如互联网）中，可设定地址的系统或计算机。

注：包括服务器主机和云主机。

3.6

终端 terminal

能够接入自然资源“一张网”，具有能够提供应用程序开发接口的开放操作系统，并能够安装和运行第三方应用软件的手持或便携设备。

注：包括办公终端、运维终端、便携式计算机、移动智能终端。

3.7

高级可持续威胁 advanced persistent threat

指隐匿而持久的电脑入侵过程，通常由某些人员精心策划，针对特定的目标。

3.8

物联网 internet of things

通过感知设备，按照约定协议，连接物、人、系统和信息资源，实现对物理和虚拟世界的信息进行处理并作出反应的智能服务系统。

3.9

保护对象 protecting objects

指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的网络、主机和应用等，包括自然资源“一张网”、自然资源云、国土空间基础信息平台以及底线守护、格局优化、绿色低碳、权益维护等应用场景。

3.10

虚拟专用网 virtual private network

一种在公共通信基础网络上通过逻辑方式隔离出来的网络。

4 概述

4.1 保护对象

指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的网络、主机和应用等，包括自然资源“一张网”、自然资源云、国土空间基础信息平台以及底线守护、格局优化、绿色低碳、权益维护等应用场景。

4.2 基本原则

自然资源网络安全保护应遵循以下基本原则。

——合规性。根据网络安全等级保护、关键信息基础设施安全保护等政策文件规定，以自然资源实际需求为导向，在合规的基础上考虑整体安全设计，保障自然资源网络安全体系工作的推进。

——系统性。紧密结合自然资源系统数字化发展工作相关要求，以《自然资源数字化治理能力提升总体方案》为重要依据，从安全管理、安全技术、安全运营三个层面，系统性推动行业网络安全保护工作。

——前瞻性。充分考虑自然资源数字化发展前景，对“一张网”、“一张图”、“一平台”的数字化治理体系框架进行全面分析，并在整体规划中构建制度、管理和技术衔接配套的安全防护体系，守住网络安全底线。

——实际性。着眼自然资源系统及省、市、县多级用户，衔接自然资源部统筹监管工作要求，覆盖物理、网络、主机、应用、数据、终端、云、物联网、供应链等各维度，形成满足实际需求并可执行落地的全方位安全保障体系。

5 网络安全保护框架

自然资源网络安全保护框架重点基于GB/T 22239、GB/T 22240、GB/T 25070、GB/T 39204要求，以及《自然资源数字化治理能力提升总体方案》《自然资源领域数据安全管理办法》，针对保护对象从安全管理要求、安全技术要求、安全运营要求三个维度进行防护设计，框架见图1：

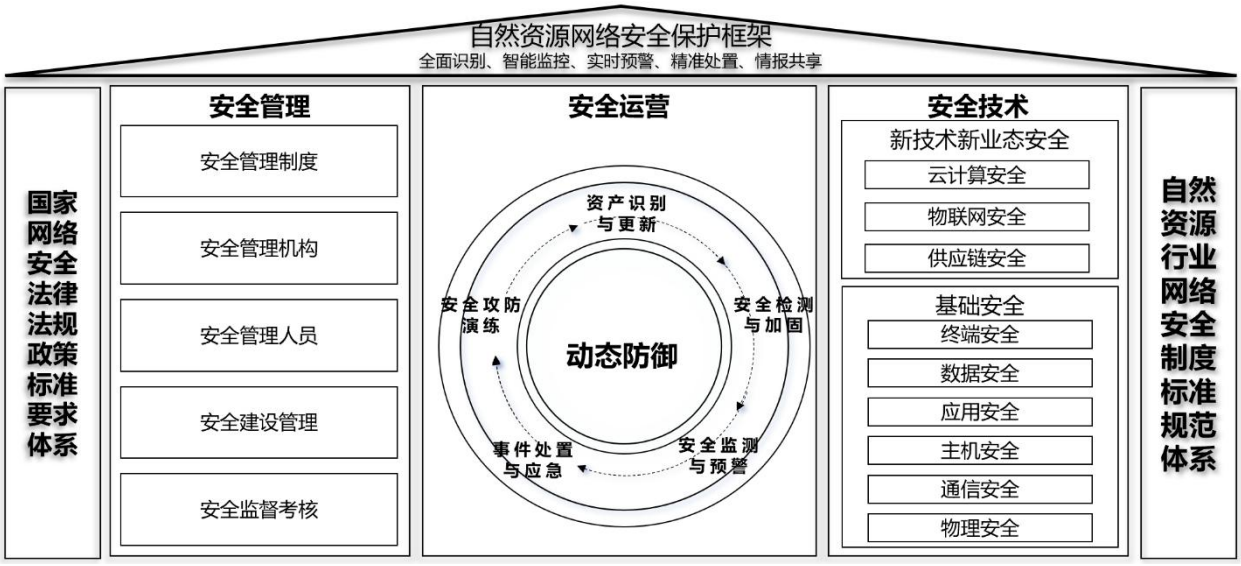

图 1 自然资源网络安全保护框架

安全管理包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全监督考核五个部分。

安全技术要求包括基础安全和新技术新业态安全两部分，其中基础安全包括物理安全、通信安全、主机安全、应用安全、数据安全、终端安全；新技术新业态安全包括云计算安全、物联网安全、供应链安全。

安全运营包括资产识别与更新、安全检测与加固、安全监测与预警、事件处置与应急、安全攻防演练五个部分。

6 安全管理要求

6.1 安全管理制度

6.1.1 安全策略

安全策略应符合以下要求：

a) 主管部门应制定网络安全工作的总体的方针、目标、范围、原则和安全框架等；

b) 应参照总体方针制定安全策略，包括但不限于安全互联策略、安全设计策略、身份管理策略、入侵防范策略、数据安全防护策略、自动化机制策略（配置、漏洞、补丁、病毒库等）、供应链安全管理策略、安全运维策略、安全运营策略等；

c) 关键信息基础设施运营单位应按照 GB/T 39204 要求，制定安全策略。

6.1.2 管理制度

管理制度应符合以下要求：

a) 应对安全管理活动中的各类管理内容建立安全管理制度，包括但不限于：网络安全应急响应制度、数据安全事件应急响应制度、网络安全考核及监督问责制度、网络安全教育培训制度、人员管理制度、业务连续性管理及容灾备份制度、三同步制度（安全措施同步规划、同步建设和同步使用）、供应链安全管理制度；
b) 应形成由安全策略、管理制度、操作规程、记录表单等构成的安全管理制度；
c) 关键信息基础设施运营者应制定网络安全保护计划，安全保护工作目标，从管理、技术、运营、等方面进行规划，网络安全保护计划应每年至少修订一次，或发生重大变化时进行修订。

6.1.3 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和发布。

6.1.4 评审和修订

评审和修订应符合以下要求：
a) 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，对安全管理制度进行修订；
b) 关键信息基础设施运营单位在发生重大变化时，应评审和修订安全策略、管理制度以及规程文件。

6.2 安全管理机构

6.2.1 岗位设置

岗位设置应符合以下要求：
a) 应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；
b) 应设立网络安全管理工作的职能部门，并定义负责人的职责；
c) 应设立系统管理员、审计管理员、安全管理员、数据安全管理员等岗位，并明确岗位职责及考核要求。

6.2.2 人员配备

人员配备应符合以下要求：
a) 应配备一定数量的系统管理员、审计管理员、安全管理员、数据安全管理员等；
b) 应对关键信息基础设施运营单位负责人和关键岗位人员进行安全背景审查和安全技能考核，符合要求的人员才能上岗，网络安全管理机构明确关键岗位，并配备 2 人以上共同管理。

6.3 安全管理人员

6.3.1 人员管理

人员管理应符合以下要求：
a) 应与所有被录用人员签署保密协议，包括岗位职责、离岗后的脱密期限等；
b) 应由专人负责外部人员账户开设、注销，权限分配、撤销等相关工作，并严格执行登记制度。

6.3.2 安全培训

安全培训应符合以下要求：
a) 应至少每年开展一次安全意识教育和培训工作；
b) 关键信息基础设施运营单位应定期安排网络安全管理机构人员参加国家、行业或业界网络安全相关活动，及时获取网络安全动态。

6.4 安全建设管理

6.4.1 定级和备案

定级和备案应符合以下要求：
a) 安全保护等级初步确定为第二级及以上的，定级对象的网络运营者应符合 GB/T 22240 相应的管理规定，开展定级和备案工作；

b） 应将备案材料报主管部门网络安全和信息化领导小组办公室和属地公安机关备案（第二级以上）。

6.4.2 等级测评

等级测评应符合以下要求：

a） 应定期进行等级测评，第三级信息系统应当每年至少进行一次等级测评，并对测评中不符合相应等级保护标准要求的及时整改；
b） 应在定级对象发生重大变更或级别发生变化时进行等级测评；
c） 应选择符合国家规定的测评机构。

6.4.3 密码管理

密码管理应符合以下要求：

a） 应按照《中华人民共和国密码法》《商用密码管理条例》开展密码安全建设工作；
b） 关键信息基础设施、网络安全等级保护第三级及以上信息系统，应自行或者委托商用密码检测机构每年至少开展一次商用密码应用安全性评估。

6.4.4 供应链管理

供应链管理应符合以下要求：

a） 应选择符合国家规定的产品、服务供应商；
b） 应建立和维护合格供应方目录；
c） 应与网络、安全产品和服务的提供者签订安全保密协议。

6.5 安全监督考核

6.5.1 安全管理考核

安全管理考核应符合以下要求：

a） 应建立网络安全管理机构，明确机构责任人、负责部门和岗位职责；
b） 应定期专题研究网络安全、数据安全等重大事项；
c） 应制定网络安全管理制度等文件；
d） 应提供网络安全工作预算清单等文件；
e） 应开展网络安全培训工作。

6.5.2 安全建设考核

安全建设考核应符合以下要求：

a） 应提供安全保护等级第二级及以上系统备案材料；
b） 应提供安全保护等级第三级及以上系统等级测评、商用密码应用安全性评估结果；
c） 应提供云计算服务安全评估结果；关键信息基础设施运营者对采购的产品和服务以及数据处理活动，提供网络安全审查材料；
d） 应制定网络安全规划、实施计划、实施方案、设计方案等文件。

6.5.3 安全运维考核

安全运维考核应符合以下要求：

a） 应制定运行维护年度计划和运维操作规程，包括环境、资产、介质、设备维护、配置等；
b） 应提供网络拓扑图、重要资产清单、关键供应链、网络日志等资料，并针对等级测评、检测评估、风险分析、实战检验等工作中发现的安全隐患和风险建立清单，制定整改方案；
c） 应提供关键信息基础设施网络安全检测和风险评估报告。

6.5.4 数据保护考核

数据保护考核应符合以下要求：

a） 应制定数据安全管理制度；

b） 应开展数据分类分级工作。

6.5.5 监测预警考核

监测预警考核应符合以下要求：

a） 应建立网络安全信息通报机制，收集、汇总、分析各方面的网络安全信息，进行通报预警处置；
b） 应提供与主管部门网络安全和信息化领导小组办公室、属地公安部门、网信部门以及网络安全服务机构之间的信息共享工作等材料；
c） 应提供风险漏洞和网络安全事件处置反馈等材料。

6.5.6 应急处置考核

应急处置考核应符合以下要求：

a） 应制定应急预案或实施细则，明确处置应对责任机构、指挥机制、响应流程、处置权限等；
b） 应提供应急演练文档资料或记录，对于关键信息基础设施是否制定专项应急预案。

6.5.7 供应链安全考核

供应链安全考核应符合以下要求：

a） 应制定本单位供应链考核制度；
b） 应将供应链考核结果上报至主管部门。

7 安全技术要求

7.1 物理安全

应根据保护对象等级，按照GB/T 22239的要求进行网络安全防护建设。

7.2 通信安全

7.2.1 通信传输

通信传输应符合以下要求：

a） 宜对业务网、政务外网（互联网）等通信线路采取“一主一备”保护，应对网络关键节点和重要设施实施冗余备份；
b） 应避免将重要网络区域部署在边界处，各网络区域之间应采取技术隔离手段，如网闸、防火墙等；
c） 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、保密性。

7.2.2 边界防护

边界防护应符合以下要求：

a） 应完善业务网、政务外网（互联网）等网络之间的安全互联策略；
b） 对不同局域网之间远程通信时应采取安全防护措施，如虚拟专用网（VPN）、防火墙等；
c） 应保持同一用户其用户身份和访问控制策略等在不同网络区域中的一致性；
d） 应对未授权设备进行动态发现及管控，只允许通过运营者授权的软硬件运行；
e） 应采用无线接入网关设备接入有线网络与无线网络边界之间的访问和数据流；
f） 应采用边界设备提供的受控接口进行跨越边界的访问和数据流通信；
g） 应对非授权设备或内部用户非授权联到内部和外部网络的行为进行检查或限制，如堡垒机、终端安全管理系统。

7.2.3 访问控制

访问控制应符合以下要求：

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，默认情况下除允许通信外受控接口拒绝所有通信；
b) 应删除多余或无效的访问控制规则，优化访问控制列表；
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) 应根据会话状态信息为进出数据流提供允许、拒绝访问的措施；
e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。

7.2.4 入侵防范

入侵防范应符合以下要求：
a) 应在关键网络节点处检测、防止或限制从内部、外部发起的网络攻击行为；
b) 应在关键网络节点处对恶意代码、垃圾邮件进行检测、清除和防护，并维护恶意代码防护机制、垃圾邮件的升级和更新；
c) 应对网络行为进行分析，实现对新型网络攻击行为的分析，并记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应及时上报主管部门。

7.2.5 安全审计

安全审计应符合以下要求：
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安全事件进行审计；
b) 应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) 应采取网络审计措施，监测、记录系统运行状态、日常操作、故障维护、远程运维等，留存日志数据不少于 12 个月；
d) 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。

7.3 主机安全

7.3.1 身份鉴别

身份鉴别应符合以下要求：
a) 应对主机登录的用户进行身份标识和鉴别，身份标识具有唯一性；
b) 应对主机制定统一的安全配置基线；
c) 应具有主机登录失败处理功能，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措施；
d) 应采用技术措施对主机进行远程管理，如堡垒机、虚拟专用网（VPN）等；
e) 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（第三级以上）。

7.3.2 访问控制

访问控制应符合以下要求：
a) 应依据最小权限的原则，为默认用户预置针对主机的访问控制策略；
b) 在用户访问主机上的受控资源或功能时，应依据设置的控制策略进行授权和访问控制；
c) 针对主机的访问控制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；
d) 应删除多余或无效的主机访问控制规则。

7.3.3 入侵防范

入侵防范应符合以下要求：
a) 应按照最小安装的原则，仅安装主机需要的组件和应用程序，关闭不需要的系统服务、默认共享和高危端口；
b) 应定期开展漏洞扫描，至少每半年开展一次；

c） 应能发现已知主机漏洞，并在经过充分测试评估后，及时修补漏洞；
d） 应至少每个季度更新一次病毒库、漏洞规则库等；
e） 应采取技术手段检测主机被入侵的行为并及时阻断，同时进行实时告警；
f） 关键信息基础设施运营单位应采取技术手段，提高对高级可持续威胁（APT）等网络攻击行为的入侵防范能力。

7.3.4 安全审计

安全审计应符合以下要求：
a） 应启用针对主机用户行为的安全审计功能，审计覆盖到每个主机用户，对重要的用户行为和重要安全事件进行审计，应对主机审计进程进行保护，防止未经授权的中断；
b） 主机审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c） 应对主机审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

7.4 应用安全

7.4.1 身份鉴别

身份鉴别应符合以下要求：
a） 应在用户登录应用系统时，进行身份标识与鉴别；
b） 应具备登录失败处理、会话结束、非法登录次数限制及超时自动退出等安全功能；
c） 应采用至少两种鉴别技术（如口令、密码、生物技术），并至少使用 1 种密码技术（第三级以上）。

7.4.2 访问权限

访问权限应符合以下要求：
a） 应对登录用户分配专属账户和权限，禁用或重命名默认账户并修改其默认口令；
b） 应定期清理和停用多余、过期账户，避免共享账户的存在；
c） 应授予管理用户最小必要权限，实现权限分离；
d） 应由授权主体制定访问控制策略，规定用户或进程对文件、数据库表的访问规则，实现访问控制；
e） 应对重要主体和客体设置安全标记，并严格控制对有标记资源的访问权限。

7.4.3 数据接口

数据接口应符合以下要求：
a） 应采用密码技术保障数据接口传输数据的机密性和完整性；
b） 应采用数据签名、多因素等技术提供身份鉴别和访问控制；应根据数据应用方唯一标识进行应用身份鉴别、状态校验和权限控制等，对数据接口进行安全管理；
c） 应采用数据接口参数过滤、限制等措施，防止接口特殊参数注入；
d） 应对数据接口调用日志进行分析，从访问用户、访问频率、访问时间、访问数据量等维度进行数据接口调用行为分析画像，通过告警和阻断机制对异常事件进行实时通知和阻断；
e） 应规定使用数据接口的安全限制条件和安全控制措施，如授权策略、访问控制、数字签名、时间戳、安全协议、白名单制等；
f） 应对数据接口实施版本管理，以便在引入新功能或修复安全漏洞时能够平滑过渡。

7.4.4 安全审计

安全审计应符合以下要求：
a） 应启用针对应用系统用户行为的安全审计功能，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；
b） 应对会话标识符的生成、存储和传输过程进行审计，以及会话超时和注销进行审计；

c） 应对应用系统是否记录了关键的安全事件和操作日志，如用户登录、敏感操作等进行审计。

7.4.5 安全编程

安全编程应按照GB/T 38674、GB/T 42884的要求进行防护。

7.5 数据安全

7.5.1 数据收集

数据收集应符合以下要求：

a） 应根据国家要求与标准制定数据收集标准；
b） 应参照主管部门制定的数据收集标准完成数据收集工作；
c） 应具备数据分类分级、数据加密存储、数据源身份鉴别、数据完整性校验、数据收集过程审计等能力，满足数据收集安全性要求；
d） 数据收集过程中，应当根据数据安全级别采取相应的安全措施，重要数据和核心数据收集生产人员、设备的管理，并对收集来源、时间、类型、数量、精度、区域、频度、流向等进行记录；
e） 应定期评估数据收集的范围、流程、频次、渠道、方式等。

7.5.2 数据存储

数据存储应符合以下要求：

a） 应明确数据存储设施的安全存储保护措施，如数据加密存储、数据存储实施安全访问策略等；
b） 应建立数据存储设施操作的安全控制机制，包括统一身份认证、账号权限最小配置、数据脱敏、操作日志记录与审计等；
c） 数据存储设施应根据存储数据的类别和级别，基于密码技术提供数据的机密性保护，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；
d） 数据存储设施应根据存储数据的类别和级别，基于密码技术提供数据的完整性保护，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
e） 应对存有鉴别信息或存有敏感数据的存储空间被释放或重新分配前进行完全清除；
f） 数据应存储于中华人民共和国境内，确需出境应符合国家法律、行政法规和有关规定要求；
g） 数据存储设施应对汇聚后形成规模或体量的数据重新定级，并根据相应级别采取安全防护措施；
h） 关键信息基础设施运营单位应提供重要数据处理系统的热冗余，提供重要数据的本地数据备份与恢复与异地实施备份功能，利用通信网络将重要数据实时备份至备份场地，关键信息基础设施一旦被破坏，可及时进行恢复和补救。

7.5.3 数据使用与加工

数据使用与加工的应符合以下要求：

a） 应当采取访问控制、数据防泄露、操作审计等管控措施；
b） 应明确数据使用与加工的流程，包括处理目的、处理方式、应用场景等，并对数据使用与加工流程进行存证，实现数据处理全过程审计；
c） 应对数据处理过程进行日志记录。

7.5.4 数据传输

数据传输应符合以下要求：

a） 应具备断点续传、超时重新连接等能力；
b） 应对数据传输过程进行日志记录。

7.5.5 数据提供

数据提供应符合以下要求：

a) 数据提供前应对数据提供双方进行身份鉴别；
b) 应根据政务数据的类别和级别,执行相应的数据安全保护措施；
c) 应具备身份鉴别、权限控制、日志审计和数据加密等安全措施；
d) 应对数据提供过程进行日志记录,符合数据提供过程可审计和可追溯需求；
e) 数据共享应符合 GB/T39477 的规定。

7.5.6 数据公开

数据公开应符合以下要求：

a) 应在数据公开前对待公开数据进行内容检查,及时识别并停止涉及重要数据和敏感个人信息的政务数据公开；
b) 应对数据公开过程进行日志记录,符合数据公开过程可审计和可追溯需求。

7.5.7 数据销毁

数据销毁应符合以下要求：

a) 应建立不可逆数据删除机制,配置必要的数据删除工具,能根据业务场景需求以不可逆方式删除的数据及其衍生的数据，如设备报废、存储介质迁移、系统升级或迁移、科研或测试、个人隐私保护、国家安全与涉密信息等场景；
b) 应具有物理删除和逻辑删除的数据删除方法,明确不同类别和级别的数据删除方式和安全；
c) 应对数据销毁过程进行日志记录,包括时间发生的日期和时间、事件主体、事件客体、事件描述、事件成功或失败等，符合数据销毁过程可审计和可追溯需求。

7.5.8 数据备份及恢复

数据备份及恢复应符合以下要求：

a) 应制定备份策略，包括对象、时间、方式、介质、模式、优先级等；
b) 应根据数据特点和业务需要，采用全量备份、增量备份或差量备份方式；
c) 应根据数据的更新频率和业务需要，确定备份频率；
d) 应选择可扩展的存储介质进行数据备份；
e) 应定期开展数据备份恢复演练，制定备份恢复计划，包括恢复步骤、所需时间、恢复后的验证及测试等。

7.6 终端安全

7.6.1 安全检查

安全检查应符合以下要求：

a) 应采用免受恶意代码攻击的技术措施，包括防病毒系统、集中式终端安全管理系统或主动免疫可信验证机制及时识别入侵和病毒行为，将其有效阻断；
b) 应能检测识别或阻断非授权访问、权限异常变化、恶意软件安装等恶意行为；
c) 应对终端接入网络之前，检查防病毒软件、弱口令账户、未修复的高危漏洞，不符合要求的终端不允许接入网络。

7.6.2 身份鉴别

身份鉴别应符合以下要求：

a) 应对终端登录的用户进行身份标识和鉴别；
b) 应对终端配置登录失败处理策略；
c) 应对终端接入网络采用口令认证、密码技术、生物技术或 MAC 认证等鉴别技术对用户进行认证。

7.6.3 访问控制

应对终端的接口进行使用控制，包括光驱、WLAN、蓝牙、USB接口等接口。

7.6.4 入侵防范

入侵防范应符合以下要求：

a) 应对终端关闭不需要的系统服务、默认共享和高危端口；
b) 应对终端采取主动防护技术手段，及时识别并阻断入侵和病毒行为，并对高级可持续威胁（APT）进行识别防护。

7.6.5 传输加密

应采用密码技术鉴别数据、重要业务数据和重要个人信息等。

7.6.6 安全审计

安全设审计应符合以下要求：

a) 应具备安全审计能力，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；
b) 应对审计记录进行定期备份。

7.7 云计算安全

7.7.1 网络架构

网络架构应符合以下要求：

a) 自然资源云不应承载高于其安全保护等级的业务应用系统；
b) 应实现不同虚拟网络之间的隔离；
c) 应根据业务需求提供通信传输、边界防护、入侵防范等安全能力；
d) 应根据业务需求自主设置安全策略，包括定义访问路径、选择安全组件、配置安全策略。

7.7.2 访问控制

访问控制应符合以下要求：

a) 应设置不同虚拟机之间、容器之间的访问控制策略；
b) 应对容器镜像仓库设置访问控制策略；
c) 应对云管理平台实现基于角色的访问控制，支持设定不同用户对管理平台内各类资源和容器镜像资源的权限控制。

7.7.3 入侵防范

入侵防范应符合以下要求：

a) 应检测虚拟机之间、容器之间的资源隔离状态，并进行告警；
b) 应检测非授权新建或者重新启用虚拟机、容器，并进行告警；
c) 应检测恶意代码在虚拟机间、容器间感染及情况，并进行告警。

7.7.4 身份鉴别

身份鉴别应符合以下要求：

a) 当远程管理自然资源云中设备时，管理终端和自然资源云之间应建立双向身份验证机制；
b) 应对云管理平台、容器镜像仓库、容器实例的访问请求进行身份标识和鉴别，并使用安全协议连接。

7.7.5 镜像和快照保护

镜像和快照保护应符合以下要求：

a) 应针对重要业务系统提供安全加固操作，如基线配置核查等；
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；
c) 应采取密码技术或其他技术手段防止虚拟机镜像、快照中敏感资源被非法访问。

7.7.6 安全审计

安全审计应符合以下要求：

a) 应对远程管理时执行的特权命令进行审计，包括但不限于虚拟机删除、虚拟机重启等；
b) 应审计容器镜像使用情况，包括镜像上传、镜像下载事件，记录访问源 IP 等；
c) 应审计容器实例事件，包括进程、文件、网络等事件。

7.8 物联网安全

7.8.1 感知终端

感知终端应符合以下要求：

a) 应要求感知终端接入网络中具有唯一网络身份标识，对操作系统用户进行身份鉴别，只有授权的感知终端可以接入；
b) 感知终端应能自检出已定义的设备故障并进行告警，确保设备未受故障影响部分的功能正常；
c) 应能为操作系统事件生成审计记录，审计记录应包括日期、时间、操作用户、操作类型等信息。

7.8.2 感知层网关

感知层网关应符合以下要求：

a) 应能够控制感知终端访问数量，能够对接入的感知终端进行认证；
b) 应能够对接入设备设置访问控制策略，防止资源被非法访问和非法使用；
c) 应能够对身份鉴别、协议转换、审计记录操作、修改安全属性、访问请求等操作行为进行记录并生成审计记录，审计记录应至少包括事件发生时间、类型和主体身份，能够对审计记录访问进行限制和查询。

7.8.3 感知层接入

感知层接入应符合以下要求：

a) 接入系统应具备感知层接入实体与自然资源“一张网”之间的隔离防护功能，应支持逻辑隔离或物理隔离；
b) 接入系统应对接入自然资源“一张网”的感知层接入实体进行鉴别；
c) 接入系统应支持感知层接入实体对自然资源“一张网”的访问控制机制和安全策略，支持应用指定的通信协议和数据内容格式检查的数据包过滤；
d) 接入系统应具备对与感知层接入实体通信的密钥管理功能；
e) 接入系统应对感知层接入实体的接入安全事件进行日志审计。

7.8.4 物联网（IOT）数据传输

物联网（IOT）数据传输应符合以下要求：

a) 应支持通信延时和中断处理功能，配合终端进行完整性保证；
b) 应保障数据的及时性，对所接收的历史数据或超出时限的数据进行识别，包括数据来源于系统采用统一时间分配，矫正机制，数据中宜包含时间标识等；
c) 应保障数据的准确性，在数据存在可接受的误差时，建立容错集中保障系统的正常运行；
d) 应建立数据安全传输策略、程序和控制措施，以保护通信设施传输的所有类型信息的安全，应明确可明文传输信息类别和范围；
e) 应对数据传输建立成功与失败、传输设备在线监测异常与告警事件、恶意程序入侵警报事件、管理员/非管理员造成的配置修改操作等安全失效事件记录日志和进行审计，日志内容至少包括时间、事件类型、事件主体、事件描述、成功/失败信息等。

7.9 供应链安全

7.9.1 软件开发

软件开发应符合以下要求：

a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
b) 应要求供应链建立研发、测试工具和设备白名单，采用安全检测、正版授权验证、官方完整性校验等措施进行白名单准入控制，并记录风险信息；
c) 应要求供应链对其研发、测试工具提供安全替代方案，在断供、停止服务等情况下不影响开发、测试工作；
d) 应在软件开发过程中对安全性进行测试，在软件安装前对恶意代码进行检测；
e) 应要求开发单位提供软件源代码，自行或委托第三方网络安全服务机构对定制开发的软件进行源代码安全检测，或由供应方提供第三方网络安全服务机构出具的代码安全检测报告；
f) 应掌握软件技术资料，包括中文版运行维护、二次开发、软件使用的场景和条件、权限和授权机制、软件设计文档、建设过程文档、软件使用说明书及测试报告等技术资料。

7.9.2 软件运维

软件运维应符合以下要求：

a) 应确定运维方案，包括运维团队、运维内容和范围、运维流程等内容；
b) 应明确运维人员的访问权限级别，对其访问范围和授权期限进行严格区分，确定不同权限人员尤其是厂商、外包等非自有维护人员，开展软件运维的内容和边界；
c) 应协调软件原厂、供应商、集成商等共同开展软件运维工作；
d) 应禁止向未授权者提供运维相关数据，或将相关数据用于运维以外的目的。

7.9.3 风险评估

风险评估应符合以下要求：

a) 应每年开展一次供应链风险评估工作，针对风险评估发现的问题及时整改；
b) 应保存供应链风险评估文档，包括风险评估过程文档、评估报告、整改方案、整改报告等，留档备查。

7.9.4 安全检查

安全检查应符合以下要求：

a) 应制定供应链检查方案，每年开展不少于 1 次的供应链安全检查工作，完善供应链安全管理工作；
b) 应在主管部门制定的供应链检查方案基础上进行修订与完善，形成本单位的供应链检查方案；
c) 应开展常态化供应链安全自查工作，每年不少于 1 次，应根据检查结果进行整改，记录整改过程，留档备查。

8 安全运营要求

8.1 运营活动

网络安全运营活动包括资产识别与更新、安全检测与加固、安全监测与预警、事件处置与应急、安全攻防演练五个部分。主管部门制定总体安全运营活动流程，明确各单位的工作内容，依托统一监测预警平台，组织协同开展安全运营工作，相关示例见附录A。

8.2 资产识别与更新

8.2.1 资产识别

资产识别应符合以下要求：

a) 应通过人工梳理或自动化技术对保护对象的资产进行识别，建立资产台账；
b) 资产识别范围应包括但不限于：域名、IP、端口、中间件、数据库、操作系统等 ，识别后应对资产信息进行分类管理。

8.2.2 资产更新

资产更新应符合以下要求：

a) 应定期对资产信息进行识别，持续动态更新管理资产台账；
b) 应在资产发生改建、扩建、所有人变更等较大变化时，重新识别资产信息，更新资产信息；
c) 应根据安全检测、监测预警、响应处置中发现的安全隐患或发生的安全事件，以及处置结果，并结合安全威胁和风险变化情况开展评估，必要时重新开展资产信息更新工作。

8.3 安全检测与加固

8.3.1 安全检测

安全检测应符合以下要求：

a) 应自行或者委托网络安全服务机构通过渗透测试、风险评估等安全服务识别保护对象安全风险，每年进行至少一次安全检测；
b) 在安全检测工作中，应配合提供网络安全管理制度、网络拓扑图、重要资产清单、关键业务链、网络日志等必要的资料和技术支持，针对安全检测工作中发现的安全隐患和风险建立清单；
c) 应对安全检测结果进行留存，应将安全检测报告上报至主管部门；
d) 应将发现的资产漏洞信息按照要求进行上报，主管部门应对资产漏洞进行统一管理。

8.3.2 安全加固

安全加固应符合以下要求：

a) 应制定详细的安全加固方案，包括安装时间、步骤、回退计划以及应急措施；
b) 应在非生产环境对安全加固方案进行测试，验证加固后对业务产生的潜在影响进行评估，确定对系统的运行不会造成影响后方可加固；
c) 应验证安全加固后，系统的功能完整性、性能表现以及安全漏洞是否已被修复等；
d) 应将加固并验证后的报告上报到主管部门。

8.4 安全监测与预警

8.4.1 安全监测

安全监测应符合以下要求：

a) 主管部门组织建设自然资源网络安全统一监测预警平台，各单位应按照标准接口将安全日志上传；
b) 应采用自动化机制，对关键业务所涉及的系统的所有监测信息进行整合分析，监测指标至少包含资产、脆弱性、威胁等维度；
c) 应对网络安全共享信息、威胁情报、报警信息等进行综合分析、研判，发现网络安全事件；
d) 主管部门对网络安全事件统一采集并监测分析，展示网络安全态势。

8.4.2 安全预警

安全预警应符合以下要求：

a) 主管部门对造成较大影响的安全事件向相关单位发起预警通告；
b) 预警信息的内容应为：基本情况描述、能产生的危害及程度、可能影响的用户及范围、宜采取的应对措施等。

8.5 事件处置与应急

8.5.1 事件处置

事件处置应符合以下要求：

a) 当发生有可能危害关键业务的安全事件时，应及时向主管部门报告，并组织研判，形成事件报告；
b) 应按照网络安全事件和数据安全事件应急预案进行事件处理，恢复关键业务和信息系统；

c） 主管部门应及时将安全事件及处置情况通报到受影响的单位和人员。

8.5.2 应急演练

应急演练应符合以下要求：

a） 应在国家和主管部门应急预案的框架下，制定网络安全事件应急预案；
b） 应急预案应至少包括总则、组织机构与职责、监测与预警、应急处置等内容；
c） 应每年至少组织开展 1 次应急演练。

8.6 安全攻防演练

8.6.1 演练方案

演练方案应符合以下要求：

a） 应围绕关键业务的可持续运行制定演练方案，方案包括演练目标、演练范围、演练时间、演练人员等；
b） 在不适合开展实网攻防演练场景下，应采取沙盘推演的方式进行攻防演练；
c） 关键信息基础设施运营单位应每年至少开展 1 次攻防演练工作。

8.6.2 演练结果

演练结果应符合以下要求：

a） 应在攻防演练工作结束后，形成攻防演练总结报告，针对攻防演练中发现的安全问题和风险开展安全整改工作，支撑安全防护体系优化；
b） 应对攻防演练整改工作进行安全技术验证，消除安全风险；
c） 应将攻防演练的总结报告上报到主管部门。

附 录 A
（资料性）
安全运营流程实例

A.1 为确保自然资源领域信息系统的安全稳定，需按照系统化、全面化的安全运营流程，该流程涵盖资产识别与更新、安全检测与加固、安全监测与预警、事件处理与应急、安全攻防演练等关键环节，流程示例见图A.1。

A.2 建立完整资产台账，定期识别更新资产信息，为安全检测提供数据基础。

A.3 全面检测信息系统，及时发现漏洞并制定加固方案，提升系统防护能力。

A.4 构建安全监测体系，实时监测预警潜在威胁，提高响应速度。

A.5 制定应急预案并定期组织演练，确保安全事件得到迅速有效处理。

A.6 常态化组织攻防演练，模拟真实攻击场景，检验防护措施和应急流程，持续优化提升安全防护能力。

A.7 在整个安全运营过程中，强调各环节协同操作和数据共享，建立数据上报接收机制，确保信息及时传递反馈，形成完整安全运营体系，为安全运营工作的持续改进和优化提供有力支撑，不断提升自然资源领域的安全管理水平。

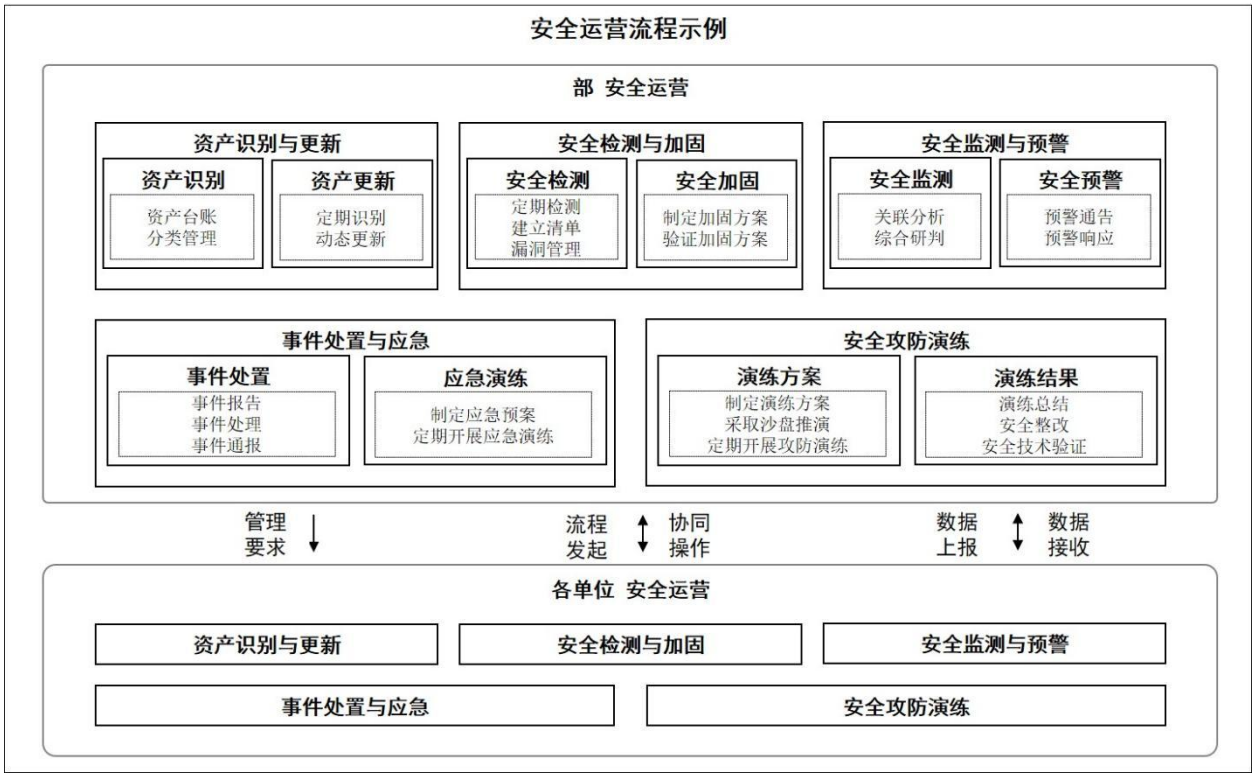

图 A.1 安全运营流程示例

参 考 文 献

[1] GB/T 20984—2022 信息安全技术 信息安全风险评估方法
[2] GB/T 20986—2023 信息安全技术 网络安全事件分类分级指南
[3] GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范
[4] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
[5] GB/T 25069—2022 信息安全技术 术语
[6] GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求
[7] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
[8] GB/T 32924—2016 信息安全技术 网络安全预警指南
[9] GB/T 35273—2020 信息安全技术 个人信息安全规范
[10] GB/T 36635—2018 信息安全技术 网络安全监测基本要求与实施指南
[11] GB/T 36951—2018 信息安全技术 物联网感知终端应用安全技术要求
[12] GB/T 37025—2018 信息安全技术 物联网数据传输安全技术要求
[13] GB/T 37044—2018 信息安全技术 物联网安全参考模型及通用要求
[14] GB/T 37093—2018 信息安全技术 物联网感知层接入通信网的安全要求
[15] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
[16] GB/T 38645—2020 信息安全技术 网络安全事件应急演练指南
[17] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
[18] GB/T 43698—2024 网络安全技术 软件供应链安全要求
[19] GB/T 45396—2025 数据安全技术 政务数据安全处理要求
[20] YD/T 4208—2023 面向云计算的安全运营中心能力要求
[21] 《自然资源数字化治理能力提升总体方案》 （自然资发〔2024〕33号）
[22] 《自然资源领域数据安全管理办法》 （自然资发〔2024〕57号）