ICS 35.020
L 70

团　　体　　标　　准

T/DSAG 003-2025

数字政府政务系统安全监测体系运营标准

Operation Standard for Security Monitoring System of Digital Government Administration System

2025 - 01 - 01 发布　　2025 - 01 - 01 实施

广东省数字安全协会　　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。

本文件由广东省数字安全协会归口管理。

本文件起草单位：深信服科技股份有限公司、广东省信息安全测评中心、天翼安全科技有限公司、北京梆梆安全科技有限公司、中孚安全技术有限公司、北京天融信网络安全技术有限公司、奇安信网神信息技术(北京)股份有限公司、广东科城信服信息技术有限公司、深圳市常行科技有限公司。

本文件主要起草人：常晓宇、王文佳、方冬茹、张廷伦、高勇、刘懋东、郑灿丹、黄福印、庄严、曾磊、赵阳、邓思贤、李新亮、杜江波、刘康权、刘启超。

信息安全技术 数字政府政务系统安全监测体系运营标准

1 范围

本文件规定了广东省政务网络安全监测系统建设的总体要求和技术规范，以及通过安全监测系统开展安全运营的工作要求。

本文件适用于指导广东省各级电子政务外网主管单位开展安全监测系统设计、建设、运维及运营工作。

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/Z 20986 信息安全技术 信息安全事件分类分级指南

GB/T 25069 信息安全技术 术语

GB/T 32924 信息安全技术 网络安全预警指南

GB/T 36635 信息安全技术 网络安全监测基本要求与实施指南

GB/T 36643 信息安全技术 网络安全威胁信息格式规范

GW0203-2014 国家电子政务外网安全监测体系技术规范与实施指南

GW0204-2014 国家电子政务外网安全管理系统技术要求与接口规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

政务网络 government network

运行政务部门非涉密业务应用的专用网络。

注：包含基础网络、以及部署在基础网络之上的政务云、政务应用和政务数据等信息技术设施和资源，主要划分为政务广域网、政务城域网和政务局域网。

3.2

政务城域网 government metropolitan area network

同城各政务部门间实现互联互通的政务网络。

3.3

政务广域网 government wide area network

连接不同地区政务局域网或政务城域网，实现远程通信的政务网络。

3.4

安全监测系统 security monitoring system

通过对网络流量、安全日志、威胁情报等数据进行实时采集、监测和分析，动态识别网络风险，发现攻击威胁、资产脆弱性以及安全事件，并进行通报预警和可视化展示的系统。

3.5

脆弱性 Vulnerability

信息技术、信息产品、信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷，这些缺陷以不同形式存在于信息系统的各个层次和环节中，一旦被恶意主体所利用，就会对信息系统的安全造成损害，从而影响构建与信息系统之上正常服务的运行，危害信息系统及信息的安全。脆弱性又称为安全漏洞。

3.6

告警 alert

对网络安全要素进行分析，发现攻击或入侵时，自动向相关人员发出的通知。

3.7

预警 warning

针对即将发生或正在发生的网络安全事件或威胁，提前或及时发出的安全警示。
[来源:GB/T 32924 3.5]

3.8

探针 probe

从被观察的信息系统中，通过感知、监测等收集事态数据的一种部件或代理。
[来源:GB/T 25069 2.2.1.27]

3.9

数据总线 data bus

实现系统中数据采集探针、存储、分析、展示与应用等各模块之间，以及与第三方平台之间数据共享和交换的功能模块。

3.10

威胁情报 threat intelligence

一种基于证据的知识，用于描述网络威胁信息、研判安全态势，支持安全事件响应和处置决策。

3.11

遥测数据 telemetry

经过最小化处理的数据，可以明确表明特定行为发生并且和特定的攻击机制相关。

4 符号与缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

CPU：中央处理器（Central Processing Unit）

DGA：域名生成算法（Domain Generation Algorithm）

DNS：域名系统（Domain Name System）

GIS：地理信息系统（Geographic Information System）

IP：网际协议（Internet Protocol）

SMTP：简单邮件传输协议（Simple Mail Transfer Protocol）

URL：统一资源定位系统（Uniform Resource Locator）

VPC：虚拟私有云（Virtual Private Cloud）

5 概述

5.1 系统技术架构

政务网络安全监测系统包括数据采集与预处理、数据存储、数据总线、数据分析、展示与应用、威胁情报、安全管理等基本功能模块，其技术架构如图1所示。

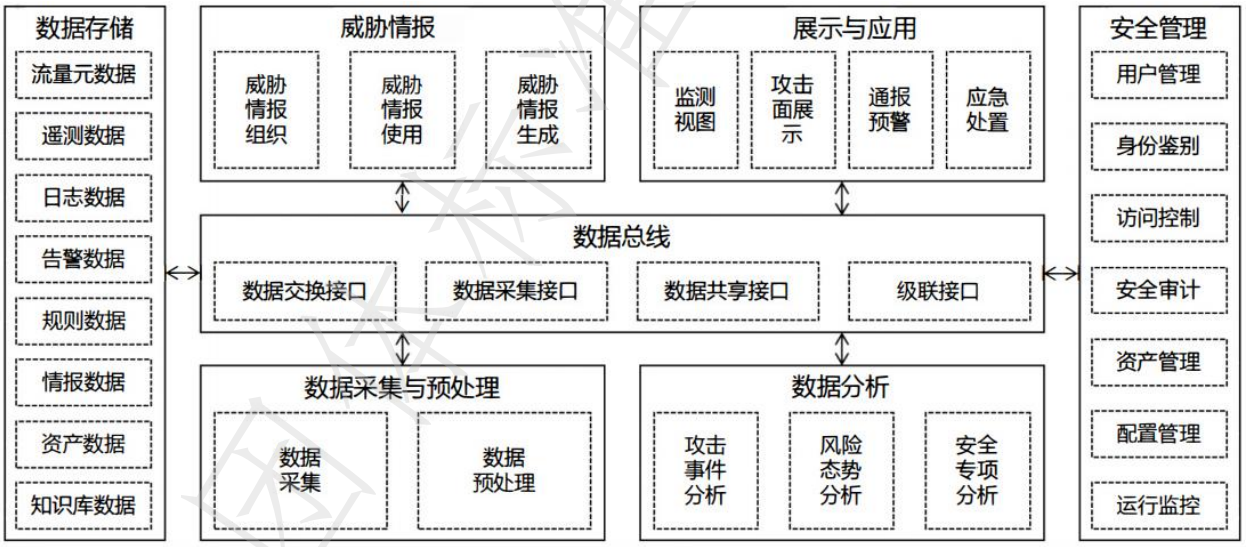

图 1 政务网络安全监测系统技术架构图

a) 数据采集与预处理：根据政务网络安全监测系统的监测范围和监测对象确定数据采集范围、采集对象和采集方式，并对采集的数据进行解析预处理，以进一步数据关联分析；

b) 数据存储：对系统中不同类型和结构的安全数据进行存储；

c) 数据总线：实现系统各功能模块之间，以及与第三方平台之间的数据共享和交换；

d) 数据分析：通过关联分析、模式匹配、特征匹配、机器学习等数据分析技术识别网络攻击行为，分析安全风险态势；

e) 展示与应用：根据决策层、管理层、执行层等不同层级人员的需求和关注重点，进行多维度的态势展示，并且支持通报预警和应急处置；

f) 威胁情报：为安全事件检测、事件调查、研判分析、追踪溯源提供外部情报数据支撑；

g) 安全管理：提供基础的用户管理、配置管理、运行监控、安全审计等功能，强化系统自身的安全性。

5.2 系统监测范围和对象

广东省电子政务外网主要承载广东省各级政务部门的办公类应用、公众服务类应用，以及跨地区、跨部门业务协同和数据共享类应用。广东省电子政务外网一般包含如下网络区域：

a) 广域网：各级政务部门实现上下互联互通的网络。各级电子政务外网通过接入设备接入广域骨干网链路；

b) 城域网：同级政务部门实现互联互通的网络。各政务部门通过接入设备接入城域网链路；

c) 政务云平台区：包含互联网区数据中心和公用网络区数据中心，两个数据中心通过逻辑隔离技术实现安全隔离；

d) 互联网区数据中心：是政务部门安全接入、开展社会化服务的网络区域，满足政务部门利用互联网开展公共服务、社会管理、经济调节和市场监管的电子政务业务需要；

e) 公用网络区数据中心：是各部门、各地区互联互通的网络区域，为政务部门公共服务及开展跨部门、跨地区的业务应用、协同和数据共享提供支撑；

f) 互联网出口区：同级政务部门实现统一互联网资源访问的逻辑功能区域；

g) 安管网管区：承担电子政务外网统一认证、安全审计、网络监控、运维管理的逻辑功能区域。

政务网络安全监测系统的监测范围应涵盖上述网络区域，并以各地市、区县落地路由为各级责任边界。监测的对象包括基础网络，以及部署在上述网络区域的政务云平台、政务应用和政务数据。当政务网络的边界或结构发生变化时，应及时调整监测范围和监测系统的部署。

5.3 系统部署要求

5.3.1 总体部署架构

政务网络安全监测系统采用省、地市、区县三级架构，省级和地市级单独建设安全监测系统，具备完整的数据采集与预处理、数据存储、数据总线、数据分析、展示与应用、威胁情报、安全管理和安全运营保障等功能。省级单位电子政务外网应部署监测探针，把监测数据接入省级政务网络安全监测系统，市级单位的监测探针数据接入市级平台系统，区县级根据实际情况可不单独建设安全监测系统，通过部署安全监测探针实现安全监测能力。需要进行级联对接的上级系统和下级系统通过数据总线接口规范实现总体态势、告警日志、威胁情报、认证、报表等数据的级联对接。政务安全监测系统的部署架构如图2所示。

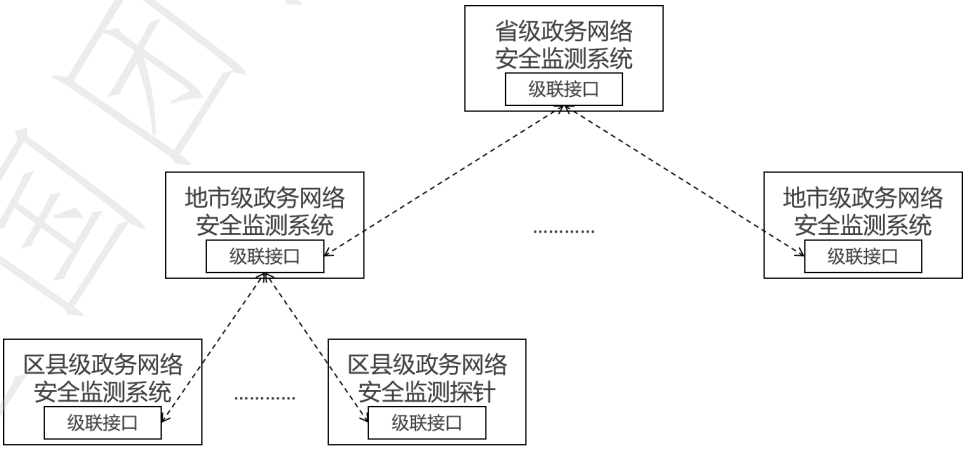

图 2 政务网络安全监测系统部署架构图

5.3.2 省级系统部署

省级政务网络安全监测系统应部署在省级电子政务外网，主要对地市级广域网接入、城域网接入、政务云平台等区域进行流量、日志等维度信息的数据采集处理。

5.3.3 地市级系统部署

地市级政务网络安全监测系统应部署在市级电子政务外网，主要对区县级广域网接入、城域网接入、政务云平台等区域进行流量、日志等维度信息的数据采集处理。

地市级政务安全监测系统应按照要求和省级政务安全监测系统进行数据的级联对接。

5.3.4 区县级系统部署

区县级根据实际情况可不单独建设安全监测系统，可以通过部署安全监测探针实现针对区县城域网接入、政务云平台等区域进行流量、日志等维度信息的数据采集预处理。

区县级安全探针应按要求和地市级安全监测系统进行数据的级联对接。

5.4 运营管理要求

依托政务网络安全监测系统能力，各级部门需要履行网络安全管理职能，规范开展电子政务外网主动防控，监测预警、研判分析、通报处置、应急响应等运营管理工作，有效保障电子政务外网网络安全。

6 安全监测总体要求

6.1 数据采集与预处理

6.1.1 数据采集

本项要求包括：

a) 采集范围应覆盖监测范围内的通信网络、区域边界以及计算环境。采集点部署在核心交换节点、核心汇聚节点和移动接入点等关键节点。如果监测范围包括政务广域网或政务城域网，数据采集点应部署在政务广域网和政务城域网的核心交换节点、核心汇聚节点等关键节点；

b) 采集对象宜包括：网络流量、资产信息、威胁情报、脆弱性信息、知识案例数据、安全设备告警、安全日志、遥测数据等；

c) 系统应支持通过不同的方式采集流量、日志、资产、威胁情报等信息：

1) 应支持部署流量探针，通过流量镜像的方式获取被监测的流量；
2) 应支持主动或被动采集日志；
3) 应支持主动扫描或网络流量检测方式发现资产，并支持手动或第三方导入、补全资产信息；
4) 应支持通过级联接口或数据共享接口采集第三方平台数据；
5) 应支持主动扫描、手动或第三方导入，获取资产的脆弱性信息；
6) 应支持接口更新或第三方导入威胁情报数据；
7) 应支持采集政务云的边界区域、VPC 内部、VPC 之间和管理区的流量，流量采集对计算节点及带宽资源的占用应以不影响云上政务业务系统的正常运行为基准；
8) 应支持通过采集流量、日志、资产、威胁情报等信息采集方法或对接政务云安全管理平台采集政务云的日志、资产等数据；
9) 应支持在政务云计算节点上部署探针，进行计算节点流量或日志数据的采集；
10) 应支持在邮件系统出入口处部署邮件监测探针，进行 SMTP 等流量数据采集；
11) 应支持部署网站专用探针，进行网站安全数据采集；
12) 应支持主动或被动采集业务系统安全日志数据；
13) 应支持在关键节点部署流量探针，进行政务数据流量采集；
14) 应支持采用主动或被动方式采集数据库安全审计日志、数据安全设备日志等。

6.1.2 数据预处理

本项要求包括：

a) 应具备数据解析规则、过滤规则和补全规则等，用于过滤、富化日志信息；

b) 应支持对邮件系统的采集数据进行 SMTP 等流量数据预处理；

c) 应支持对网站的采集数据进行网站安全数据预处理；

d) 应支持自定义数据预处理规则。

6.2 数据存储

本项要求包括：

a) 应支持对系统采集以及处理产生的数据进行分类存储，包括但不限于流量元数据、资产信息、日志数据、遥测数据、安全告警、威胁情报、安全事件、案例知识库等数据；

b) 应支持对结构化数据、半结构化数据和非结构化数据进行存储；

c) 应支持自定义数据存储时间；

d) 应支持对身份鉴别、数据分析结果等重要数据进行加密存储；

e) 应支持配置数据保护策略，防止数据遭受未经授权的读取、删除或修改；

f) 应支持数据迁移、数据的备份及恢复；

g) 应支持数据存储节点扩展和负载均衡；

h) 应支持当数据存储达到阈值时，发出报警信息。

6.3 数据总线

6.3.1 数据类型

应支持根据数据类型定义数据格式、数据协议和接口调用。数据类型包括但不限于流量元数据、日志数据、遥测数据、资产信息、安全告警、威胁情报、安全事件、工单报表等。

6.3.2 数据交换接口

应支持系统内部基本功能模块之间，通过接口进行数据调用、存储、分析、展示与应用。

6.3.3 数据采集接口

应支持从不同类型的数据采集探针采集流量元数据、日志数据、遥测数据、资产信息、威胁情报等数据。

6.3.4 数据共享接口

宜支持向第三方平台发送/接收数据，包括但不限于：安全告警、安全事件、预警信息、威胁情报等。

6.3.5 级联接口

具有上下级联关系的系统之间通过级联接口进行数据共享和交换，本项要求包括：

a) 数据交互内容包括但不限于安全告警、预警信息、安全事件、威胁情报、工单报表、统计数据、知识案例等；

b) 接口类型包括但不限于级联注册接口、数据上传接口、数据下发接口和数据查询接口等；

c) 应支持在数据传输过程中采用密码技术保证数据的完整性和保密性。

6.4 数据分析

6.4.1 攻击行为分析

本项要求包括：

a) 应支持特征码匹配分析，能够识别恶意流量特征、恶意文件特征、恶意代码特征等；

b) 应支持场景化分析，包括但不限于资产违规外连、账号异地登录、弱口令、数据库敏感操作等典型场景；

c) 宜支持基于攻击阶段、攻击特征相似度等维度的关联分析；

d) 应支持通过机器学习算法进行数据分析；

e) 应支持对多源异构的安全大数据进行聚合或关联分析，发现攻击行为；

f) 宜支持利用沙箱对可疑文件及 URL 进行静态或动态的分析检测；

g) 宜支持关联威胁情报进行网络攻击行为特征分析和溯源分析；

h) 宜支持 DNS 威胁检测，包括但不限于 DNS 协议漏洞检测、恶意域名解析检测、DGA 域名检测、DNS 隐蔽通道检测等；

i) 应支持对政务云边界区域和管理区的南北向流量的攻击行为分析；

j) 应支持对政务云 VPC 内部、VPC 之间的东西向流量的攻击行为分析。

6.4.2 风险态势分析

本项要求包括：

a) 应支持基于资产、威胁和脆弱性监测数据，对网络的整体安全态势进行分析；

b) 应支持基于安全事件的威胁态势分析，安全事件包括但不限于有害程序事件、网络攻击事件、数据攻击事件、违规操作事件等；

c) 应支持基于资产的类型、分布、重要程度、资产脆弱性等信息，综合分析资产安全态势；

d) 应支持对政务云边界区域和管理区的南北向流量的风险态势分析；

e) 应支持对政务云 VPC 内部、VPC 之间的东西向流量的风险态势分析。

6.4.3 安全专项分析

网站监测分析要求包括：

a) 应支持对网站可用性进行监测分析；

b) 应支持对网站 DNS 解析服务进行监测，及时发现域名劫持，域名解析失败等问题；

c) 应支持对网站攻击行为进行分析，包括但不限于网页篡改、网页挂马、敏感信息泄露等事件；

d) 应支持定期对网站系统漏洞进行扫描分析。

业务系统分析要求包括：

a) 应支持业务行为分析，包括敏感信息页面调用异常、查询数据异常、账号使用异常等行为；

b) 应支持操作行为分析，包括同一业务高频操作、异常时间操作、数据库异常操作等行为；

c) 应支持访问行为分析，包括异常 IP 地址登录、非正常时间段登录、短时多 IP 登录、异常端口访问等行为；

d) 应支持资产变动分析，对业务系统资产的端口或服务变化情况进行监测分析。

政务数据分析要求包括：

a) 应支持数据资产识别分析，包括自动发现数据资产、数据分类分级标记等；

b) 应支持数据异常行为分析，包括对数据库异常访问、异常操作行为、接口异常调用等进行分析；

c) 应支持数据接口脆弱性分析，包括参数可遍历、接口未鉴权、登录弱口令、口令明文传输等；

d) 应支持个人信息泄露分析，对个人信息泄露情况进行识别和分析；

e) 应支持对数据泄露情况进行溯源分析和取证。

6.5 展示与应用

6.5.1 监测视图

本项要求包括：

a) 应支持对网络整体安全态势的展示，展示方式包括 GIS 地图、雷达图、拓扑图、路径等至少两种表现形式；

b) 应支持基于威胁类型、攻击次数、威胁来源、威胁目标、攻击路径等信息的威胁视图展示；

c) 应支持基于资产类型、分布、资产脆弱性、相关攻击事件等信息的资产安全视图展示；

d) 应支持基于事件类型、源 IP、目的 IP、受攻击资产、威胁等级、处置情况等信息的安全事件视图展示；

e) 应支持基于统计信息、实时信息、历史信息和变化趋势的展示方式，以及分角色展示方式；

f) 应支持基于政务云平台维度、云服务客户维度和 VPC 维度的态势展示；

g) 应支持政务云边界区域、VPC 内容、VPC 之间和管理区的威胁态势和资产安全态势展示；

h) 应支持对数据安全态势的展示，包括威胁统计、资产统计和脆弱性统计等；

i) 宜支持对数据流转或数据访问关系的展示；

j) 应支持对数据安全事件的告警，内容包括但不限于告警类型、告警级别、受影响数据资产信息等；

k) 应支持根据数据分析结果进行实时告警，告警内容包括但不限于告警类型、告警级别、受威胁的业务资产信息、网站标识、网站地址等。

6.5.2 攻击面展示

本项要求包括：

a) 应支持在重要或特殊时期通过安全探测等方式对网络资产进行持续发现、盘点、分类、排序和监控；

b) 应支持对重要资产的攻击面信息进行详细展示，包括但不限于：各类已知资产、未知资产、影子资产等安全漏洞、系统组件、开放端口、应用程序、API 接口等；

c) 应支持以图形化的方式展现网络中各类重要资产的分布状况、相互关系、潜在攻击路径等。

6.5.3 通报预警

本项要求包括：

a) 应支持基于数据分析结构和告警规则，实时产生分级别安全告警；

b) 应支持按照设定的预警级别和预警流程发布预警信息，预警内容包括但不限于：预警类型、预警级别、威胁方式、涉及对象、影响程度、防范对策等；

c) 应支持按照设定的安全事件通报流程进行事件通报，通报内容包括但不限于事件类型、攻击源 IP、目标 IP、事件级别、事件分析、影响程度和处置建议等；

d) 应支持平台、邮件、短信、即时通讯、文件等两种及以上预警和通报方式。

6.5.4 应急处置

本项要求包括：

a) 应支持将安全告警或安全事件形成处置任务，并进行记录、跟踪和归档；

b) 应支持对安全告警或安全事件进行调查取证，包含告警溯源信息和关联的原始日志；

c) 应支持与第三方设备或平台联动，根据监测结果，协助实施动态访问控制等安全处置行动；

d) 应支持与政务云安全设备或云安全服务组件进行联动，自动完成应急处置任务。

6.6 威胁情报

6.6.1 威胁情报格式

应符合 GB/T 36643-2018 中对于情报格式的定义。

6.6.2 威胁情报组织

本项要求包括：

a) 应支持威胁情报分类存储和情报置信度评价分级，分类包括但不限于域名类、IP 类、文件类等；

b) 应支持威胁情报数据手动更新或者在线更新，更新频率不超过 24 小时。

6.6.3 威胁情报共享和使用

本项要求包括：

a) 应支持提供威胁情报数据查询和比对接口，供数据实时分析和批量查询；

b) 应支持通过接口方式或文件导入/导出方式，实现与第三方平台的威胁情报共享交换和使用。

6.6.4 威胁情报生成

本项要求包括:

a) 应支持获取原始样本或数据，并对其进行归类、分析、加工、处理后生成威胁情报；

b) 应支持自定义威胁情报标签；

c) 应支持手动增加或删除威胁情报。

6.7 安全管理

6.7.1 用户管理

本项要求包括:

a) 应支持用户、用户组的增加、删除、修改、查询及分组管理；

b) 应支持划分不同的角色，并为不同角色分配权限。

6.7.2 身份鉴别

本项要求包括：

a) 应对系统登录用户进行身份鉴别，身份鉴别信息应具有复杂度和定期更换要求；

b) 应采用密码技术保证身份鉴别信息在传输过程中的完整性和保密性；

c) 应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中至少一种鉴别技术应使用密码技术来实现。

6.7.3 访问控制

本项要求包括：

a) 应向授权用户提供配置、查询和修改各种安全策略的功能；

b) 应向授权用户提供管理日志的功能，包括日志的存储、导出和备份等；

c) 应支持在用户远程管理方式下，限定远程管理端 IP 地址范围，并采取措施保证管理端与系统之间数据传输的保密性。

6.7.4 安全审计

本项要求包括：

a) 应支持对每个用户的操作行为进行安全审计，包括但不限于：

1) 管理员的登录成功和失败；
2) 因身份鉴别尝试失败次数达到设定值导致的会话连接终止；
3) 对安全策略进行配置的操作；
4) 对管理用户进行增加、删除和属性修改的操作。

b) 审计记录应至少包括事件发生日期、时间、用户标识、事件类型、操作结果等信息。日期应精确到日，时间应精确到秒；

c) 应对审计记录进行保护，避免受到删除、修改或覆盖。

6.7.5 资产管理

本项要求包括:

a) 应支持记录资产的属性信息包括但不限于资产名称、资产类型、资产 IP、所属业务系统、部署位置、资产负责人等信息；

b) 应支持按照类型、部署位置、所属业务系统等属性对资产进行分组管理；

c) 应支持资产信息的增加、删除、查询、标记；

d) 应支持资产信息的批量导入、导出。

6.7.6 配置管理

本项要求包括:

a) 应支持对用户账号和口令的配置管理，包括初次登录口令修改、账号锁定时间、口令有效期、登录尝试次数、口令长度和复杂度限制等；

b) 应支持系统各基本功能模块与唯一确定时钟进行自动同步，每天至少同步一次；

c) 应支持对系统的安全策略、特征库、补丁等进行升级。

6.7.7 运行监控

应支持实时监控系统设备运行状态，包括但不限于 CPU 使用率、内存使用情况、磁盘使用情况、网络流量情况、设备产生的异常报警等。

7 运营管理具体要求

7.1 总体要求

运营管理工作主要包括：

a) 定期核对及时更新电子政务外网平台资产和 IP 地址对应信息；

b) 做好安全监测、威胁检测、平台对接、通报预警等工作；

c) 组织运营例会，总结运营情况，编制运营报告；

d) 对安全威胁预警及事件工单处置管理，承担安全通报支撑保障工作；

e) 制定应急预案，组织开展应急演练及攻防演练，承担应急值守与响应处置，强化重点时期安全保障；

f) 方案编制、规范制定、安全培训、绩效考核等技术支撑工作。

7.2 运营人员要求

主要包括：

a) 政务网络安全运营人员应具备专业安全技术能力及安全管理经验。

b) 由外部企业性质单位对政务网络开展安全运营，应与企业签订保密协议，并核验企业与相关人

员的保密协议。且对接入政务网络进行运营的自带终端应进行接入管控，防止政务数据泄漏。

c) 电子政务外网安全运营人员应专职专岗。

7.3 日常工作要求

7.3.1 资产梳理

主要包括：

a) 将所监测范围的政务网络相关 IP 资产信息、网络拓扑及相关责任人信息，并录入监测系统资产管理系统，并定期巡检更新。

b) 在网络及安全设备接入电子政务外网前，应进行安全性及有效性评估。

7.3.2 通报预警

主要包括：

a) 对安全监测系统采集的政务网络相关 IP 资产安全漏洞、安全事件及威胁情报等安全威胁进行人工分析验证，准确研判安全威胁及事件；

b) 对分析研判发现的安全威胁，利用监测系统通报预警模块向相关 IP 资产管理单位及联络人及时下发安全预警通告，同时做好通告问题整改督促及复测；

c) 配合做好本级安全监测系统与上下级安全监测系统对接工作。

7.3.3 定期检查

主要包括：

a) 利用包括但不限于渗透测试、漏洞扫描等主动检查方式，对电子政务外网及重要业务系统定期进行全面安全检查，验证全网所面临的威胁、风险、隐患、弱点等安全漏洞，全面分析政务网络安全的薄弱环节，及时提出整改建议，督促整改落实，并验证安全监测系统攻击特征库、威胁情报等检测能力。

7.3.4 月度汇报

主要包括：

a) 按月综合政务网络监测告警、漏洞风险、工单处置及安全事件等方面情况，划分区域及单位，评估电子政务外网风险情况、安全防护短板及受控程度，形成月度总体安全态势报告，通过安全监测系统向各单位进行发布以及存档，并记录跟踪各单位整改情况。

7.4 专项保障要求

7.4.1 安全整改

主要包括：

a) 加强与省网信、省公安及国家电子政务外网管理中心等网络安全监管部门工作协同，针对所发布大安全隐患、典型安全问题及时组织开展专项安全检查，结合安全监测情况，做好相关专项安全问题以查促改、及时反馈形成分析总结报告存档。

7.4.2 攻防演练

主要包括：

a) 协助制定攻防演练方案，开展电子政务外网安全自查工作；

b) 依托政务网络监测能力及防护能力，做好演练期间的技术安全保障工作；

c) 及时处置安全监测系统监测的安全事件或攻击行为，督促被攻击应用系统责任单位整改；

d) 总结攻防演练工作，包括但不限于从组织能力、检验安全监测系统监测预警、联动防护及人员

技术能力等角度总结，形成总结报告存档。

e) 协助电子政务外网安全合规管理，协助开展电子政务外网的网络安全等级保护测评、商用密码应用安全性评估及渗透测试等年度合规性测评工作，并将结果录入安全监测系统或形成报告存档。

7.5 重要时期保障要求

在特定重要时期启动重保工作模式，强化安全保障能力，主要包括：

a) 重保前期应做好人员值班值守安排，下发重保工作通知，开展安全检查工作,并对发现的问题进行通告发布，督促整改并复测，记录存档；

b) 重保期间应 7*24 小时应急值守，强化主动防控措施，及时阻断安全威胁，快速处置安全风险，按要求做好日重保情况信息报送；

c) 重保结束后及时进行复盘，形成重保工作总结存档。

7.6 培训与考核

应制定安全运营培训计划和考核指标，提升相关人员技术知识水平，实现安全运营能力持续提升，主要包括：

a) 制定安全技能和安全意识培训计划，对专业技术人员提供专项提升培训和考核，掌握前沿技术、产品应用等内容，提升相关人员技术知识水平；

b) 结合安全运营的目标和现状制定安全运营考核指标，指标应包括安全管理指标、安全建设指标、运行能力指标和安全态势指标，并每年至少开展一次考核工作。

7.7 应急响应要求

主要包括：

a) 制定本级政务网络总体应急预案，包括但不限于事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应应急处置措施，同时明确应急响应工作组织架构、职责分工及 7*24 小时应急响应机制，每年至少更新一次；

b) 发生重大安全事件或收到安全监管部门安全通报时，启动应急预案，依照事件类别及等级，组织开展安全事件分析与排查，督促或协助整改，做好事件处置总结归档，并更新应急预案；

c) 每年协助开展应急演练，演练结束后更新应急预案。