ICS 35.080
CCS L 77

团　　体　　标　　准

T/DGAG 040—2025

数字政府统一基础运维规范
第 7 部分：政务外网网络安全服务实施

Specification for digital government unified basic operation maintenance
—Part 7: Implementation for government external network security services

2025－12－12 发布　　2026－01－01 实施

广东省数字政务协会　　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。

《数字政府统一基础运维规范》分为7个部分：

——第 1 部分：总则；（已以 DB4401/T 294.1—2024 发布）

——第 2 部分：信息基础设施服务要求；（已以 DB4401/T 294.2—2024 发布）

——第 3 部分：政务云服务要求；（已以 DB4401/T 294.3—2024 发布）

——第 4 部分：政务外网网络安全服务要求；

——第 5 部分：信息基础设施服务实施；

——第 6 部分：政务云服务实施；

——第 7 部分：政务外网网络安全服务实施。

本文件是《数字政府统一基础运维规范》的第7部分。

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。

本文件由广东省数字政务协会归口。

本文件起草单位：广州市数字政府运营中心、中国联合网络通信有限公司广州市分公司、广州市标准化研究院、联通（广东）产业互联网有限公司、联通数字科技有限公司、深信服科技股份有限公司、广州安恒智慧城市网络安全技术有限公司、广州方集信息科技有限公司、广东省数字政务协会、广州市信息安全测评中心、赛讯数科（广东）技术有限公司、中网讯信息科技（广州）有限公司、广州尚古网络科技有限公司、云仓库（广东）信息科技有限公司。

本文件主要起草人：苏勇、吴培庆、廖盛辉、穆斌、陈刚、周绍午、陈楠、何帅、汪旭、巫晔浩、徐振兴、钟志鸿、刘春林、曾剑锋、郝敬宁、宛仕程、林兵、许文彬、苏轶、李娜、林晓、马之宇、廖奘龙、斯鹏、于代典、刘瑞婷、李昀辉、崔杨、曾金杯、吴伟雄、董耀艺、叶将发、刘曦、杨小庆、陈文俊。

引　言

广州市为提升网络安全保障能力和基础设施运维管理能力，构建集约管理、安全可信、权责清晰、资源共享、高效有序的广州市数字政府统一基础运维管理体系，广州市政务服务和数据管理局通过开展数字政府统一基础运维，整合全市各部门现有基础运维资源，将原分散、各自负责的基础运维工作进行一体化服务。

目前，广州市数字政府统一基础运维主要针对信息基础设施、政务云和政务外网网络安全三个方面。为规范广州市数字政府统一基础运维服务，提高服务质量，2023年广州市政务服务和数据管理局提出建立一整套的服务标准。本标准依据广州市数字政府统一基础运维的实际实施情况，将标准分为7个部分。

其中，第1部分总则，主要说明统一基础运维的主要内容和范围，并为其余部分的编制提供依据；第2、3、4部分主要从管理方和使用方的角度，分别对信息基础设施、政务云和政务外网网络安全的服务内容与效果提出要求；第5、6、7部分则主要对服务方提供信息基础设施、政务云和政务外网网络安全服务的实施过程进行规范。

《数字政府统一基础运维规范》第1、2、3部分已以地方标准的形式发布，其第4、5、6、7部分以团体标准的形式发布。

本文件是《数字政府统一基础运维规范》的第7部分。该部分旨在指导服务方服务实施，确保服务方达到第1部分统一基础运维的总体工作要求，以及第4部分政务外网网络安全服务要求。

数字政府统一基础运维规范
第 7 部分：政务外网网络安全服务实施

1 范围

本文件规定了数字政府统一基础运维中政务外网网络安全运维（含运营）服务的总体规范、服务机构与人员、实施技术、实施过程、评价与改进的要求。

本文件适用于广州市数字政府统一基础运维中政务外网网络安全的运维（含运营）服务实施工作，其他网络安全运维（含运营）可参考。

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 20986—2023 信息安全技术 网络安全事件分类分级指南
GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
GB/T 28458—2020 信息安全技术 网络安全漏洞标识与描述规范
GB/T 28827.1－2022 信息技术服务 运行维护 第1部分：通用要求
GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
GB/T 45940—2025 网络安全技术 网络安全运维实施指南
DB4401/T 294.1—2024 数字政府统一基础运维规范 第1部分：总则
T/DGAG 037—2025 数字政府统一基础运维规范 第4部分：政务外网网络安全服务要求

3 术语和定义

DB4401/T 294.1—2024界定的以及下列术语和定义适用于本文件。

3.1

网络安全运维 cybersecurity operation and maintenance

组织为抵御网络空间安全威胁，控制网络安全风险，确保业务持续、稳定运行，保证业务以及承载数据的保密性、完整性和可用性，统筹技术、流程、人员等要素，持续开展管理、识别、防护、监测分析、事件处置、协同等工作的一种网络安全服务方式。

[来源：GB/T 45940—2025，3.1]

4 实施概述

服务方应从服务机构与人员、实施技术、实施过程和评价改进方面进行服务实施规范管理及持续提升服务能力，并符合DB4401/T 294.1—2024和T/DGAG 037—2025的规定。

a) 服务机构与人员：具备满足政务外网网络安全服务要求的服务能力、服务工具、服务场地、服务制度和服务人员。
b) 实施技术：采用调查收集、管理平台、监控工具或可视化工具等多样化的技术手段保障政务外网网络安全服务质量。
c) 实施过程：具备政务外网网络安全运营服务的过程管理能力，规范政务外网网络安全服务的实施过程。

d) 评价改进：通过实施过程和结果的监控和测量、服务满意度调查、内部审核、管理评审等方式开展服务质量自我评价，并根据管理方、使用方、监理方在服务全过程中反馈问题和评价结果，制定并落实改进措施，以持续改进服务质量。

5 服务机构与人员

5.1 服务机构

5.1.1 综合能力

服务方按照GB/T 28827.1—2022中5的规定进行能力建设，具备能力包括但不限于：

a) 服务活动策划和管理能力；
b) 建立完善的政务外网网络安全服务管理制度和服务规范的能力；
c) 提供满足服务要求的政务外网网络安全服务资源的能力；
d) 提供满足服务要求的政务外网网络安全服务技术的能力；
e) 建设满足服务要求的专业政务外网网络安全服务实施团队的能力；
f) 建立完善的安全防护管理体系的能力；
g) 应急响应能力。

5.1.2 服务工具

服务方提供保障服务质量符合服务要求的安全运营平台，平台应符合GB/T 22239—2019中第三级安全要求的规定。平台具备功能包括但不限于：

a) 资产管理功能：资产全生命周期管理；
b) 漏洞运营管理功能：扫描工具及任务管理、漏洞全生命周期管理、漏洞情报管理；
c) 安全告警及事件管理功能：安全告警聚合、研判，安全事件处置管理；
d) 指挥调度管理功能：工单管理、通告下发；
e) 安全服务管理功能：渗透测试、上线检测、应急演练、APP 检测、钓鱼测试、安全意识培训、安全重保服务管理；
f) 评价考核管理功能：服务评价考核；
g) 数据可视化功能：多维度数据概况展示。

5.1.3 服务台

服务方根据使用方服务场景特点建立满足接收服务请求或事件、信息交互、资源调度、服务过程管控等需求服务台。服务台具备7×24小时热线、站内消息、即时通讯等多种渠道的支持能力，同时提供业务咨询反馈、服务申请及报障引导响应。

5.1.4 服务保障场地

服务方根据管理方和使用方的要求设立政务外网网络安全服务保障场所。保障场所配备满足服务需求的软硬件，具备指挥调度、应急管理、资源调配和服务支持等功能，保证政务外网网络安全服务的质量。

5.1.5 制度建设

服务方根据政务外网网络安全服务的总体要求，建立并完善服务管理制度和体系，确保各项工作的标准化、规范化和有序管理。服务管理制度目录内容见附录A。

5.2 人员

5.2.1 人员配置

服务方根据政务外网网络安全服务的总体需求，结合管理方和使用方不同服务场景的实际需要配置岗位合理和数量充足的服务人员。岗位配置应至少包括管理类、技术类和操作类。

5.2.2 人员能力

5.2.2.1 管理类

管理类服务人员具备从事政务外网网络安全服务管理所需的专业知识、技能和经验，包括但不限于：

a) 能够组织建立完善政务外网网络安全服务各类体系制度、标准规范和工作流程并推进执行；
b) 能够制定政务外网网络安全服务计划，进行资源整体统筹调配；
c) 能够监督管控政务外网网络安全服务的各个过程，确保达到管理方和使用方要求；
d) 能够进行政务外网网络安全服务整体沟通协调；
e) 能够进行应急管理，处理政务外网网络安全服务中的突发事件；
f) 能够提供建设性意见，协助管理方优化工作机制或流程。

5.2.2.2 技术类

技术类服务人员具备从事政务外网网络安全服务技术支持所需的专业知识、技能和经验，包括但不限于：

a) 能够结合使用方不同服务场景中的服务需求，提供针对性技术方案和技术支持；
b) 能够完成政务外网网络安全服务相关的研发及技术实现，推进成果应用；
c) 能够识别政务外网网络安全服务中的风险，分析问题原因，提出改进措施；
d) 能够提供政务外网网络安全服务相关的技术培训。

5.2.2.3 操作类

操作类服务人员具备从事政务外网网络安全服务实施操作执行所需的专业知识、技能和经验，包括但不限于：

a) 能够完成政务外网网络安全服务日常操作的实施；
b) 能够根据规范、手册等执行服务操作，并对操作结果负责。

5.2.3 人员管理

5.2.3.1 服务方对服务人员的储备、资质、培训、绩效管理、能力评价应符合 GB/T 28827.1—2022 中 6 的规定。

5.2.3.2 服务人员在涉及信息安全的服务实施过程中应符合 GB/T 22239—2019、GB/T 39786—2021 和 GB/T 45940—2025 的规定。

6 实施技术

服务方应具备提供政务外网网络安全服务的基本技术和方法，并持续改进，以适应技术发展和业务场景变化。政务外网网络安全服务主要技术和方法及对应服务项见表1。

表 1 技术和方法表

序号	技术和方法	说明	对应服务项
1	调查收集	通过访谈、检查、盘点、巡检、监控等方式收集政务外网网络安全服务相关信息	安全咨询、安全评估、资产管理、安全培训、安全监测、应急演练
2	安全运营平台	具备统一运营数据分析、可视化展示、工单调度等功能的运营服务平台	全部安全服务项
3	安全策略及监控工具	根据安全要求部署安全策略管控工具，并抓取网络流量，识别异常流量模式并提供异常流量的监控和告警	边界安全、WEB安全、主机安全、终端安全、高级威胁分析、访问控制、态势感知
4	入侵检测及防御工具	通过部署检测引擎，收集和处理整个网络中的通信信息，分析其是否构成对网络或主机造成危害的入侵攻击事件，生成相应的告警信息且可以在必要时进行主动防御的系统	安全防护类服务项、应急响应

表1　技术和方法表（续）

序号	技术和方法	说明	对应服务项
5	日志分析工具	用于记录系统、设备、应用程序、终端和个人等产生的网络日志，分析网络安全现状，协助审计及合规管理等人员进行尽责调查和合规性检查	日志及审计、安全评估
6	漏洞检测工具	通过远程或现场的方式，对网络安全隐患进行探测、检查和分析，发现目标系统在设计、实现、配置和运行等过程中，有意或无意产生的脆弱性或后门，并提出一定的防范和补救措施建议	应用检测、漏洞扫描、渗透测试、安全通告、安全评估
7	应用安全检测工具	通过模拟恶意攻击者的技术和手段，来评估计算机系统、网络、应用程序或其他信息技术基础设施安全性的服务	全部安全服务项
8	配置核查工具	基于安全配置要求实现对资产（如服务器、网络设备、安全产品、操作系统、数据库和应用系统等）的安全配置检测和合规性分析，生成安全配置建议和合规性报告	主机安全、终端安全、策略管理、安全咨询、安全评估
9	资产信息收集和管理工具	对网络空间中的资产进行全面、细致地识别和测绘，形成资产清单和分布图，发现管理视角外的未知资产，并进行安全管理和防护	资产管理、安全评估
10	应急支持	辅助客户建立、优化应急响应流程及制度；出现安全事件时提供安全告警、辅助排查	应急响应、应急演练、安全评估
11	其他新技术工具	通过使用云计算、大数据、人工智能、物联网等，实现智能派单、事件分析、性能调优、智能决策	根据实际应用场景确定具体服务项

7　实施过程

7.1　概述

使用方提出T/DGAG 037—2025中5的相关服务内容时，服务方服务人员应按照本章节对应服务项实施，符合T/DGAG 037—2025中6的规定。

7.2　安全防护

7.2.1　边界安全

7.2.1.1　与使用方确认边界安全的需求，内容包括但不限于防护范围、防护对象和访问控制规则。
7.2.1.2　根据需求制定边界安全实施方案，内容包括但不限于防护策略、访问控制和访问规则，明确安全设备配置参数及开通计划。
7.2.1.3　组织相关方对边界安全实施方案进行评审，并获取授权。
7.2.1.4　根据通过评审的方案开通和配置安全防护组件，在边界安全设备配置访问策略、病毒库、入侵规则和 VPN 通道，启用监测功能。
7.2.1.5　通过网络准入控制设备对非授权设备私自联到内部网络的行为及内部用户非授权联到外部网络的行为进行检查或限制。
7.2.1.6　与管理方和使用方确认边界安全实施情况，如业务受到影响采取回退措施。
7.2.1.7　记录服务过程和结果，提供资产信息台账更新记录。

7.2.2　访问控制

7.2.2.1　与使用方确认访问控制的需求，内容包括但不限于控制范围和访问主体。
7.2.2.2　根据需求制定访问控制方案，内容包括但不限于访问策略、统一身份管理规则、精细化权限分配模型和零信任架构。
7.2.2.3　根据方案实施访问控制，接入零信任安全，部署并启用零信任网关，实现应用级隐身、终端环境实时信任评估、建立安全访问通道。
7.2.2.4　配置资源精细化访问权限，依据策略方案，在访问代理/API 网关上设置应用和数据的细粒度访问控制策略，关闭默认开放权限，实施最小权限原则。
7.2.2.5　记录服务过程和结果，提供访问控制审计报告、合规性评估报告和信息台账更新记录。

7.2.3　WEB 安全

7.2.3.1　与使用方确认 WEB 应用和业务应用安全的需求，内容包括但不限于防护范围和防护要求。
7.2.3.2　根据需求制定 WEB 防护方案，内容包括但不限于防护对象和防护策略。
7.2.3.3　组织相关方对防护方案进行评审，并获取授权。
7.2.3.4　根据通过评审的方案部署防护设备，配置 WAF 规则和防护策略，启用监测功能。
7.2.3.5　与管理方和使用方确认 WEB 安全实施情况，如业务受到影响采取回退措施。
7.2.3.6　记录服务过程和结果，提供资产信息台账更新记录。

7.2.4　主机安全

7.2.4.1　与使用方确认主机防护的需求，内容包括但不限于防护范围和安全要求。
7.2.4.2　根据需求制定主机防护方案，内容包括但不限于防护策略、资产清点和流量监控。
7.2.4.3　组织相关方对主机安全方案进行评审，并获取授权。
7.2.4.4　根据通过评审的方案备份主机关键信息，部署安全防护代理，对接安全运营平台，配置安全防护策略，启用监测功能。
7.2.4.5　与使用方确认主机安全实施情况，如业务受到影响采取回退措施。
7.2.4.6　记录服务过程和结果，提供资产信息台账更新记录。
7.2.4.7　收集使用方需求，定期下发病毒查杀和基线检查等任务，提供相关检查报告。

7.2.5　终端安全

7.2.5.1　与使用方确认终端防护的需求，内容包括但不限于终端范围和安全要求。
7.2.5.2　根据需求制定终端防护方案，内容包括但不限于资产探测、防病毒管理、漏洞补丁管理、终端准入、终端外设管理和数据保护。
7.2.5.3　组织相关方对终端安全方案进行评审，并获取授权。
7.2.5.4　根据通过评审的方案备份终端关键信息，部署安全客户端，对接安全运营平台，配置端防护和病毒扫描等策略，启用监测功能。
7.2.5.5　与使用方确认终端安全实施情况，如业务受到影响采取回退措施。
7.2.5.6　记录服务过程和结果，提供资产信息台账更新记录。
7.2.5.7　收集使用方需求，定期下发病毒查杀和基线检查等任务，提供相关检查报告。

7.2.6　日志及审计

7.2.6.1　与使用方确认日志及审计的需求，内容包括但不限于日志采集范围、保存时限和审计要求。
7.2.6.2　根据需求制定审计方案，内容包括但不限于日志分析结果、审计记录、威胁分析和合规评估。
7.2.6.3　组织相关方对审计方案进行评审，并获取授权。
7.2.6.4　根据通过评审的方案部署日志采集组件，安装日志采集代理或配置转发。
7.2.6.5　配置审计分析策略，启用实时日志分析引擎。
7.2.6.6　执行安全审计，审计账号操作、配置变更等安全行为，标记高风险操作并提供处置建议。
7.2.6.7　检查日志信息和审计记录保存时间是否不少于 1 年，记录服务过程和结果，每季度提供日志审计报告。

7.2.7　蜜罐

7.2.7.1　与使用方确认蜜罐服务的需求，内容包括但不限于蜜罐部署区域和伪装类型。

7.2.7.2　根据需求制定蜜罐部署方案，内容包括但不限于诱饵架构、攻击引流策略和伪装规则。
7.2.7.3　根据方案部署蜜罐节点，配置攻击诱饵节点，配置伪装代理和流量牵引策略。
7.2.7.4　启用攻击诱捕监测，开启攻击行为自动捕获，监控扫描探测、漏洞利用、恶意载荷投递等动作，屏蔽蜜罐对真实业务的影响。
7.2.7.5　蜜罐产生告警时主动溯源攻击者 IP、工具链及意图，关联威胁情报库，评估攻击危害等级，执行威胁处置与响应，内容包括但不限于联动阻断攻击源 IP、分析攻击行为轨迹、上报攻击威胁情报。
7.2.7.6　记录服务过程和结果，提供蜜罐运行报告和威胁分析报告。

7.2.8　高级威胁分析

7.2.8.1　与使用方确认高级威胁分析的需求，内容包括但不限于分析范围、情报定制要求和溯源深度。
7.2.8.2　根据需求制定高级威胁分析方案，内容包括但不限于探针部署策略、分析规则配置和情报交付机制。
7.2.8.3　根据方案部署威胁监测探针，按需部署流量探针，配置日志采集策略，建立云端威胁分析通道。
7.2.8.4　执行云端关联分析，追踪恶意 IP/域名轨迹，测绘受害目标资产分布，还原攻击链和溯源攻击者。
7.2.8.5　根据分析结果，阻断攻击路径，更新检测模型，同步防御策略至防护体系。
7.2.8.6　记录服务过程和结果，推送有针对性的威胁情报，提供高级威胁分析报告。

7.2.9　态势感知

7.2.9.1　与使用方确认态势感知的需求，内容包括但不限于监控资产范围、情报共享接口要求和预测分析目标。
7.2.9.2　根据需求制定态势感知方案，内容包括但不限于资产发现机制、流量采集点规划和共享接口策略。
7.2.9.3　根据态势感知方案采集资产与风险状态，启用监测功能，实时发现政务外网主机、服务、网站、域名等资产，动态扫描漏洞及配置风险等级。
7.2.9.4　根据态势感知方案接入网络流量，识别恶意连接、异常行为、入侵攻击链，关联威胁情报库实时告警。
7.2.9.5　关联分析资产风险、攻击事件、威胁情报，识别攻击链模式，预测威胁发展趋势，生成实时态势视图和预警指标。
7.2.9.6　记录服务过程和结果，提供安全态势报告。

7.3　咨询评估

7.3.1　安全咨询

7.3.1.1　通过咨询电话、网络、安全运营平台等多种渠道接收安全咨询需求。
7.3.1.2　服务台在响应时限内接听热线或响应平台安全咨询工单，记录安全咨询请求或事件的详细信息。
7.3.1.3　优先利用知识库处理工单。
7.3.1.4　服务台无法处理解决的，将工单分配给相应的安全专家进行处理与回复，安全专家提供对应的安全服务、技术支持、报告内容等。
7.3.1.5　记录服务过程和结果。

7.3.2　安全评估

7.3.2.1　与使用方确认安全评估的需求，内容包括但不限于资产范围、实施时间和实施地点。
7.3.2.2　根据安全评估需求，向相关网络安全主管部门报备，向相关方获取授权。
7.3.2.3　安全风险评估方法符合 GB/T 20984—2022 和 GB/T 22239—2019 的规定。
7.3.2.4　采用漏洞检测、基线检查、弱口令检查、渗透测试等方法实施评估。量化风险等级，通过检测工具与人工排查的方式全面发现评估对象脆弱性。
7.3.2.5　根据符合性验证和安全风险评估结果，提供安全评估报告和安全加固建议报告。

7.3.3 应用检测

7.3.3.1 与使用方确认应用检测的需求，内容包括但不限于检测范围、实施时间和实施地点。
7.3.3.2 根据应用检测需求，向相关网络安全主管部门报备，向相关方获取授权。
7.3.3.3 采用漏洞扫描、基线检查、弱口令检测、移动端检测、代码审计等自动化工具，对政务外网移动客户端和服务器端的应用进行安全检测。
7.3.3.4 采用人工排查的方式，进行漏洞可利用性验证、逻辑漏洞挖掘、隐蔽通道检测、第三方组件风险等安全验证。
7.3.3.5 结合自动化工具和人工排查的方式全面发现应用系统脆弱性，并提供应用检测报告及安全加固建议报告。

7.3.4 漏洞扫描

7.3.4.1 与使用方确认漏洞扫描的需求，内容包括但不限于扫描范围、实施时间和实施地点。
7.3.4.2 根据漏洞扫描需求，向相关网络安全主管部门报备，向相关方获取授权。
7.3.4.3 采用漏洞扫描工具检测与人工排查相结合的方式进行扫描，提供漏洞检测报告和安全加固建议报告。
7.3.4.4 使用方安全加固完成后，可对修复的成果再次进行漏洞扫描复查，对加固修复的结果进行检验，确保修复结果的有效性，并提供系统漏洞扫描复测报告。

7.3.5 渗透测试

7.3.5.1 与使用方确认渗透测试的需求，内容包括但不限于测试范围、实施时间和实施地点。
7.3.5.2 根据渗透测试需求，向相关网络安全主管部门报备，向相关方获取授权。
7.3.5.3 通过信息收集、扫描技术、验证技术、口令破解、脚本测试、溢出攻击、提权技术等方法进行测试，并提供渗透测试报告和安全加固建议报告。
7.3.5.4 使用方安全加固完成后，可对修复的成果再次进行渗透测试复查，对加固修复的结果进行检验，确保修复结果的有效性，并提供渗透测试复测报告。

7.4 优化改善

7.4.1 资产管理

7.4.1.1 与使用方确认资产管理的需求，内容包括但不限于资产范围和资产类型。
7.4.1.2 根据管理需求，全量纳管政务外网和互联网暴露面资产，如域名、网站、APP、公众号等，实施资产信息报备工作的指导、管理和监督。
7.4.1.3 建立资产信息台账，检查各使用方的资产信息报备准确情况，随资产生命周期变化及时更新定级备案、IP/ICP 备案，及时督办更新资产信息。
7.4.1.4 采用自动化工具和人工排查等方式，每季度扫描检测，发现未知资产并跟踪处理。
7.4.1.5 每季度清查资产子域名/端口的使用情况，如系统已下线，需确保子域名已取消解析，端口已关闭，进行资产回收下线登记。
7.4.1.6 资产发生变更时，及时在安全运营平台上更新 IP/域名/应用资产信息。
7.4.1.7 记录服务过程和结果，提供资产信息台账更新记录。

7.4.2 漏洞管理

7.4.2.1 根据业务系统的重要性，评估扫描范围和涉及的网络风险，制定漏洞扫描方案。
7.4.2.2 按照 GB/T 30279—2020 的规定，对漏洞进行分类分级。
7.4.2.3 按照 GB/T 28458—2020 和 GB/T 30276—2020 的规定，对漏洞的发现和报告、接收、验证、处置、发布、跟踪进行全生命周期管理。
7.4.2.4 对漏洞扫描结果进行验证确认，必要时进行漏洞复测，排除误报情况，并调整漏洞扫描器和安全运营平台的漏洞列表数据，以免下次重复出现。
7.4.2.5 漏洞无法及时修复时，采用缓解措施对漏洞起到规避风险的作用并需持续监控和评估其有效性。

7.4.3 策略管理

7.4.3.1 与管理方和使用方确认策略管理的需求，内容包括但不限于具体策略要求，策略维护更新要求、特定场景需求等。
7.4.3.2 根据策略管理需求，结合政务外网网络安全整体要求制定安全策略基线。
7.4.3.3 协助各使用方基于统一的安全策略基线，配置符合各使用方业务场景的政务外网接入边界、业务系统、办公终端及主机等安全防护策略。
7.4.3.4 针对不同使用方对政务外网稳定性、可用性及安全性等具体安全需求，每季度对安全策略进行测试验证，确保其有效性。
7.4.3.5 根据每季度测试与验证结果，结合新威胁、业务变更、缺陷等对网络安全策略基线进行优化和迭代。

7.4.4 安全监测

7.4.4.1 与使用方确认安全监测的需求，内容包括但不限于监测范围、监测频率和监测指标。
7.4.4.2 根据监测需求，统一采集安全运营平台对政务外网内安全设备、安全组件和安全服务产生的安全数据，配置实时数据分析、批量数据分析和智能关联分析。
7.4.4.3 结合服务要求设定监测项和巡检计划，监测项参考 T/DGAG 037—2025 附录 B。
7.4.4.4 在权限受控或有监督的环境下，通过远程监控工具和人工巡检对政务外网全网安全数据进行汇聚和集中分析，结合实时更新的威胁情报及时发现安全事件。
7.4.4.5 对防护互联网、各使用方接入政务外网边界、办公终端、系统主机等安全设备进行周期性的状态检查并提交巡检报告及安全建议，对发现的安全隐患进行修复，保障系统、设备的安全性和可用性。
7.4.4.6 将监测发现的各类网络信息安全威胁或隐患告知相关方并协助处理。
7.4.4.7 结合巡检结果与实时监测，对异常设备进行安全监控和记录，包括筛选过滤告警日志，记录统计告警信息，及时发现内部失陷主机、外部攻击、违规外联等安全事件，经研判后，若为安全事件进行上报，同时根据应急预案启动应急响应服务流程。
7.4.4.8 每月提供安全态势报告，内容包括但不限于对漏洞和威胁的发现、分析和统计，并提出修复建议，对受影响资产整改情况进行统计分析，对安全防护能力的建设和配置更改进行说明。

7.4.5 安全通告

7.4.5.1 与管理方和使用方确认安全通告信息沟通渠道。
7.4.5.2 根据 GB/T 43557—2023 制定安全通告，内容包括但不限于信息类型和信息要素。
a) 实时提供网络安全通告，内容包括安全监测结果、威胁情报、行业重大安全事件以及高危漏洞预警等。
b) 每月提供安全态势通告，内容包括高危漏洞、安全热点及威胁情报解读。
7.4.5.3 对重大安全漏洞和安全威胁，跟踪控制措施，预防自身安全事件隐患的发生。

7.4.6 安全培训

7.4.6.1 与管理方和使用方确认培训需求，内容包括但不限于培训主题、培训形式、培训目标。
7.4.6.2 根据需求制定培训方案或计划，内容包括但不限于培训内容、培训方式和讲师。
7.4.6.3 根据培训方案或计划，开展相应的线上、线下培训。
7.4.6.4 进行技术交流，收集培训人员对培训内容、形式、效果等的反馈。
7.4.6.5 根据培训结果和反馈意见，优化调整培训方式和内容。
7.4.6.6 记录服务过程和结果，提供培训报告。

7.5 应急管理

7.5.1 应急响应

7.5.1.1 收集政务外网资产基本信息，确定风险评估目标。
7.5.1.2 按照 GB/T 20986—2023 中 6.2 的规定，结合政务外网资产的重要程度、安全事件发生的概率、可能造成的影响和损失进行评估，确定网络安全事件的级别。
7.5.1.3 根据不同级别的网络安全事件制定应急响应预案，每年对预案进行评审和改进。

7.5.1.4 预案经评审确认后进行发布，并对所有相关参与应急响应的部门和人员进行宣贯和培训，确保发生网络安全事件时，服务人员按照预案进行应急响应及事件处置。
7.5.1.5 通过巡检监控、用户反馈、热线支持或其他渠道接收网络安全事件信息，内容包括但不限于事件现象、影响范围、已采取的措施，为后续的分析和处理提供依据。
7.5.1.6 分析评估事件情况，并按照 T/DGAG 037—2025 中 5.4.1 的规定对事件进行分级。
7.5.1.7 调配相关资源，根据应急预案启动应急响应流程，按对应的事件级别及指标要求提供服务。
7.5.1.8 通过现场控制、远程值守、后备支持等方式实施应急响应，减少业务中断和事件影响，响应指标符合 T/DGAG 037—2025 中 5.4.1.5 的规定：

a) 对需要现场处理的事件，派遣服务人员到达现场，进行现场控制，防止事件影响扩大；
b) 对需要持续观察、随时响应的事件，根据使用方需求及事件情况提供现场或远程服务，并组织后备支持；
c) 在实施过程中及时向所有相关方通报事件进展，协调跨部门和跨单位之间的行动，确保应急响应行动的一致性和有效性。

7.5.1.9 记录应急处理过程中的所有活动，包括采取措施、效果评估和相关人员的行动，为后续的总结和改进提供数据支持。
7.5.1.10 根据记录编制并提交应急响应报告，确保相关方及时、全面了解事件处理进展和结果。
7.5.1.11 根据应急事件处理结果和报告反馈意见，对应急预案和响应流程进行必要的优化改进，以提高应急处理能力。

7.5.2 应急演练

7.5.2.1 根据预案内容，制定演练方案或计划，内容包括但不限于时间、参与人员、演练场景。
7.5.2.2 对参与演练的人员进行培训，确保相关人员了解演练的目的、流程和职责。
7.5.2.3 按照演练方案或计划实施应急演练。
7.5.2.4 记录演练过程和结果，收集相关方的反馈意见。
7.5.2.5 演练结束后，编制并提交应急演练报告，内容包括但不限于演练内容、演练结果，存在问题和改进措施。
7.5.2.6 根据演练报告和反馈意见，对应急预案进行优化和调整，提高预案的实用性和有效性。

8 评价与改进

8.1 评价

8.1.1 评价方式

评价方式包括但不限于：

a) 通过问卷调查、电话回访、走访调研、安全运营平台等方式收集相关方的评价并进行分析；
b) 接受相关方的日常监督和定期考核评价，根据监督考核结果调整优化政务外网网络安全服务；
c) 建立内部评估体系，基于相关方考核指标进行自我考核和内部评价，确保服务符合标准和满足服务需求。

8.1.2 评价内容

服务方按照T/DGAG 037—2025中7.4的规定对服务人员及整体服务方开展全面评价，评价内容见附录B。

8.1.3 评价周期

根据相关方管理要求，定期或不定期进行服务评价：

a) 定期评价：根据服务要求进行周期性总结、评价，形成相应的考核评分表或报告，为服务改进提供依据；
b) 不定期评价：根据特定情况或需求，包括但不限于发生重大安全事件、客户投诉或反馈等，开展服务评价。

8.2 改进

根据评价结果，服务方应采取以下措施对整体服务机制、体系和流程等进行全面优化改进，包括但不限于：

a) 制定具体的改进计划，包括目标、时间表、整改措施和预期成果；
b) 加强服务人员的技术培训，提升技术能力，提高服务效率；
c) 根据服务情况和相关方的反馈，调整服务内容，优化服务流程，提高服务满意度；
d) 应用自动化和数字化手段，提高服务效率；
e) 加强与相关方的沟通，深化与相关方的协同合作；
f) 持续监督改进效果，实现改进目标。

附 录 A
（资料性）
服务管理制度目录表

A.1 常用政务外网网络安全服务方管理制度见表 A.1，在不同使用方、服务场景下，内容可能存在差异，服务方可根据实际情况进行调整。

表 A.1 服务管理制度目录表

序号	管理制度名称
1	网络安全管理办法
2	人员安全与保密管理制度
3	信息资产管理规范
4	终端安全管理规范
5	机房及基础设施安全管理规范
6	软件开发与测试安全管理规范
7	网络安全事件管理规范
8	供应链安全风险管理规范
9	办公环境安全管理规范
10	漏洞全生命周期管理规范
11	安全设备上线管理规范
12	安全设备割接管理规范
13	安全设备故障应急处理规范
14	安全设备策略变更管理规范
15	第三方工具与平台安全管理规范
16	网络安全监测与分析管理规范
17	现场服务标准化规范
18	互联网暴露面动态监测规范
19	安全配置基线管理规范

附 录 B
（资料性）
评价内容表

B.1 服务人员评价

常用服务人员评价内容见表B.1，在不同使用方、服务场景下，内容可能存在差异，服务方可根据实际情况进行调整。

表 B.1 服务人员评价内容表

序号	评价项	评价内容	适用岗位
1	体系构建能力	是否建立且完善政务外网网络安全服务管理制度、标准规范及工作流程，并有效监督执行	管理类
2	资源统筹能力	资源调配是否高效、合理，能否满足多场景需求	
3	过程管控能力	是否对政务外网网络安全服务进行全过程监督管控，是否达到管理方和使用方要求	
4	应急管理能力	突发事件处理流程的规范性、响应速度及事后总结改进的落实情况	
5	创新改进能力	是否提出有效改进建议，协助优化工作机制或流程	
6	技术方案能力	提供的技术方案是否结合场景需求，实施后是否达成预期目标	技术类
7	研发实现能力	能否完成政务外网网络安全服务技术研发及达成相关成果实际应用，提升服务效率	
8	风险管控能力	对政务外网网络安全服务风险预判的准确性，问题根本原因分析的深入性及改进措施的有效性	
9	技术培训能力	培训内容的覆盖度、参训人员反馈满意度及知识传递的实用性	
10	操作规范性	是否严格按规范、手册执行操作，记录是否完整	操作类
11	任务完成效率	日常操作是否能按时完成，操作后是否达成预期结果	
12	问题上报时效	异常情况上报是否及时，工单响应速度及操作规范性	
13	数据记录质量	操作日志是否完整	
14	合规性	是否遵守安全规范或操作流程	管理类、技术类、操作类
15	沟通能力	工作汇报内容是否完整、清晰，是否能实现跨部门协作	
16	服务满意度	使用方对服务态度、响应速度及问题解决效果的综合评价	

B.2 整体评价

常用整体评价内容见表B.2，在不同使用方、服务场景下，内容可能存在差异，服务方可根据实际情况进行调整。

表 B.2 整体评价内容表

序号	评价项	评价内容
1	服务规范性	制度流程执行是否符合规范、操作手册执行是否符合规范
2	服务时效性	应急响应时效（从上报到处置）、日常任务按时完成率
3	技术有效性	漏洞修复率、系统可用性（故障率）
4	风险管理	风险识别与整改完成率
5	用户满意度	客户投诉解决满意度、服务需求匹配度
6	创新与改进	优化建议采纳数、效率提升率
7	培训与能力	人员培训覆盖率、培训考核合格率
8	合规性	安全合规检查通过率

参 考 文 献

[1] GB/T 28827.3 信息技术服务 运行维护 第3部分：应急响应规范
[2] GB/T 32914 信息安全技术 网络安全服务能力要求
[3] GB/T 35273 信息安全技术 个人信息安全规范
[4] GB/T 36074.2 信息技术服务 服务管理 第2部分：实施指南
[5] GB/T 37961 信息技术服务 服务基本要求
[6] GB/T 42461 信息安全技术 网络安全服务成本度量指南
[7] SJ/T 11691 信息技术服务 服务级别协议指南
[8] ITSS.1 信息技术服务 运行维护服务能力成熟度模型
[9] ISO/IEC 20000-1 信息技术 服务管理 第1部分：服务管理体系要求
[10] ISO/IEC 20000-2 信息技术 服务管理 第2部分：服务管理体系应用指南