ICS 35.240
CCS L 67

T/GDEIIA

团　体　标　准

T/GDEIIA XX—2024

湾区通办政务自助服务平台运维管理规范

Operation and Maintenance Management Specification for the Bay Area Inter-city Self-service Government Platform

（征求意见稿）

2024 –xx – xx 发布　　2024 – xx – xx 实施

广东省电子信息行业协会　　发 布

目　　次

前　言

本文件按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》给出的规则起草。

本文件由广东金赋科技股份有限公司提出。

本文件由广东省电子信息行业协会归口。

本文件主要起草单位：

本文件主要起草人：

本文件为首次制定。

湾区通办政务自助服务平台运维管理规范

1 范围

本文件规定了湾区通办政务自助服务平台运维管理规范的总体结构、平台系统服务管理、自助终端服务管理、平台系统监控管理、自助终端监控管理、安全管理等运维要求及内容。

本文件适用于湾区通办政务自助服务平台的运维服务管理。

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 22239-2019 信息安全技术 网络安全等级保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

湾区通办政务自助服务平台 Bay Area Unified Government Self-service Platform

统一湾区自助服务平台应用业务接入，面向各湾区部门、政务单位和其他组织提供湾区政务便民服务事项的平台。

3.2

终端设备 terminal device

连接到网络的最终用户设备，即政务自助终端设备，是用户与湾区通办政务自助服务平台互动的设备。

3.3

管理系统 management system

湾区通办政务自助服务平台在终端设备管理、设备运行监控等方面的后台管理系统。

3.4

智能运维服务管理 intelligent operation and maintenance service management

基于移动互联技术，打造一站式智能运维服务管理平台，实现“码上报”、无感报障、服务审计、服务同步、权限管理、服务预判、部件维修、在线知识库、在线绩效考核等，精细化管控运维全局，有效整合需求与资源，调用人员积极性，提高运维效能，降低工作成本，实现“指尖上”的微运维。

4 缩略语

下列符号与缩略语适用于本文件。

PM：预防性维护(Preventive Maintenance)

SP：升级包(Service Pack)

5 总体结构

湾区通办政务自助服务平台由自助服务终端和自助服务平台构成，其运维管理围绕终端和平台两个对象进行，总体结构由服务管理、监控管理、安全管理三部分组成，其总体结构如图1。

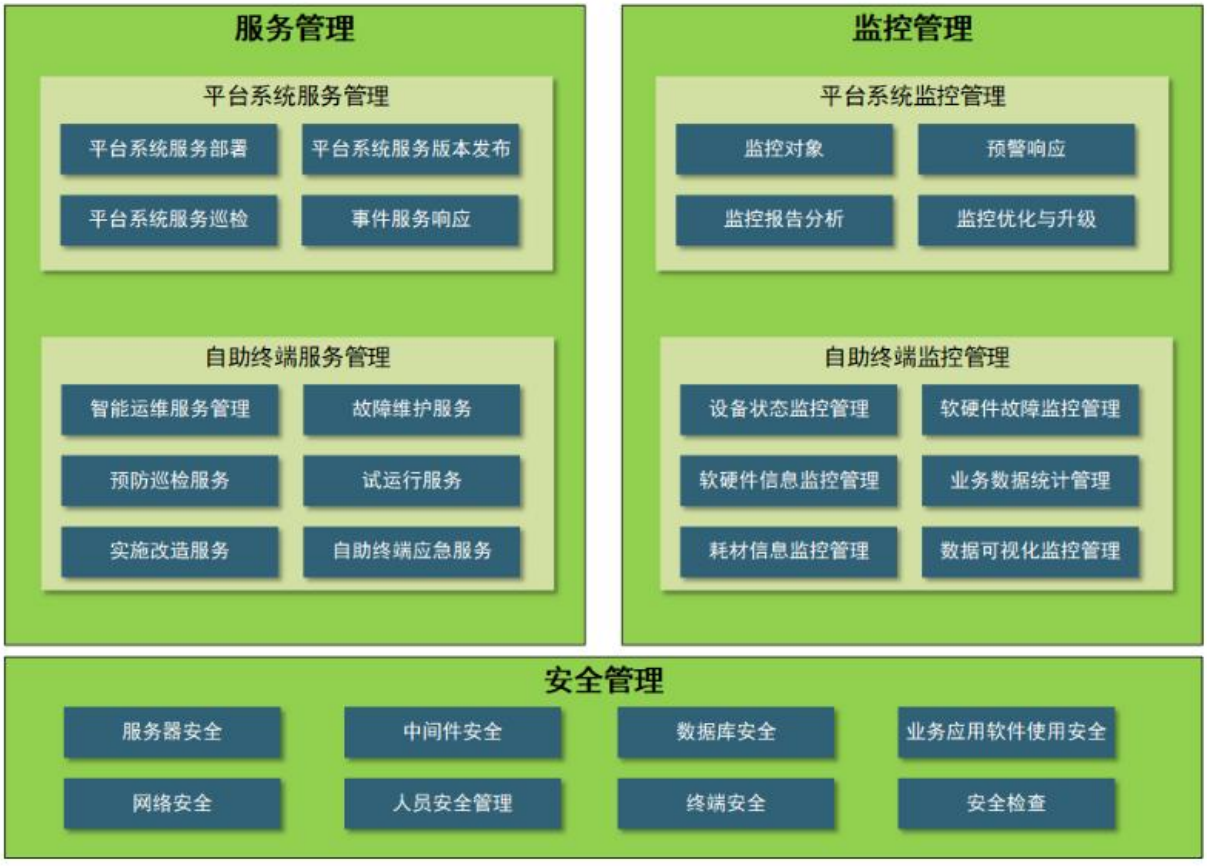

图 1　湾区通办政务自助服务平台运维管理规范结构示意图

6 平台系统服务管理

6.1 服务部署

6.1.1 服务器部署

6.1.1.1 服务器配置要求

应用服务器、数据库服务器、中间件服务器均应至少配备两台，采用主备架构，且配置均应至少满足 CPU 4 核，内存 16 GB，系统盘 50 GB，数据库存储空间 100 GB，其中数据库服务器数据库存储空间应大于 200 GB。

6.1.1.2 基础设置与工具安装要求包括：

a）磁盘划分。应根据业务需求合理分配系统盘、数据盘，并逻辑划分数据盘。

b）网络设置。应配置稳定至少百兆带宽的网络连接。

c）交换分区设置。应根据服务器内存大小，当内存 8GB~64GB，设置 swap 至少 8G。

d）用户组与用户创建。应根据业务需求创建运维、开发、审计用户，并为每个用户分配适当的权限。

e）系统运维工具。应安装指定的系统运维工具，包括 sysstat、lsof、iotop、iftop、nc、mtr、tcping 等。

f）监控软件。应安装指定的监控软件，包括 zabbix。

6.1.1.3 运维团队应调整 TCP 连接数、文件打开限制和进程数量等关键系统参数，并配置命令历史记录以显示操作时间，以满足业务需求并优化系统性能。

6.1.2 中间件部署

6.1.2.1 软件安装与配置应满足如下要求：

a）安装主备 2 套中间件软件，包括分发服务、消息队列、缓存系统等。

b）根据根据业务需求进行初始化配置，包括网络端口、日志管理等。

c）根据业务需求创建运维、开发、审计用户，并为每个用户分配适当的权限。

d）配置中间件的安全设置，包括密码策略、启用 SSL/TLS 加密、设置访问控制列表、实施身份认证和授权等。

6.1.2.2 运维团队应根据业务需求对中间件进行性能调优，包括内存大小、连接池大小、线程数、超时设置等。

6.1.3 数据库部署

6.1.3.1 软件安装与配置应满足如下要求：

a）安装主从架构的数据库软件，要求实现秒级同步数据。

b）根据业务需求进行初始化配置，包括字符集、时区和日志管理设置等。

c）合理划分数据库的逻辑和物理存储结构，包括不限于表空间、数据文件和索引文件。

d）根据业务需求创建运维、开发、审计用户，并为其分配所需的最小权限。应设置运维用户负责系统监控、日志查看、网络管理等；开发用户拥有代码库访问、开发环境管理等权限；审计用户则负责日志审计、合规性检查等。

e）配置安全设置。应对数据库实施严格的安全设置，包括访问控制、密码策略和加密通信等，以确保数据的机密性和完整性。

6.1.3.2 数据库和 SQL 性能调优应基于业务需求，包括内存管理、并发控制、连接数、索引优化及分区策略等方面。

6.1.3.3 数据库备份

运维团队应设置异机备份的策略，包括物理备份和逻辑备份，并每月对备份数据进行恢复操作验证

备份的有效性，周期为 1 天/次。

6.1.4 应用程序部署

应用程序安装与配置时应根据业务需求部署应用程序，如设置内存、线程等关键参数。

6.2 平台系统服务巡检

运维团对应建立周度巡检流程，覆盖服务器、中间件、数据库及应用程序，以识别潜在风险，采取预防措施，提升系统可靠性。

6.2.1 服务器巡检

6.2.1.1 资源使用情况检查应满足以下要求：

a) CPU 使用情况。检查 CPU 的占用率和负载情况，确保使用率未超过 80%。
b) 内存使用情况。检查内存的使用率和交换空间的使用情况，确保使用率未超过 80%。
c) 磁盘存储空间情况。检查各分区的磁盘空间使用情况，确保使用率未超过 80%。
d) 磁盘 IO 情况。检查磁盘的读写速率、IO 等待时间以及 IO 利用率，确保 IO 性能良好且未出现严重的读写瓶颈。

6.2.1.2 运维团队应检查网络连接的稳定性,确保平均延迟时间不超过 50 毫秒且确保丢包率低于 0.5%周期宜为 1 天/次。

6.2.1.3 运维团队应定期审查系统更新及补丁应用情况和系统日志，以确保系统安全性及及时识别潜在问题，周期宜为 1 周/次。

6.2.2 中间件巡检

6.2.2.1 中间件 CPU 与内存使用应不超过分配资源的 80%，连接数应保持在配置的最大值的 80%以下。

6.2.2.2 运维团队应评估中间件处理请求的响应时间及备用系统的可用性，定期检查中间件版本更新及补丁应用情况，分析日志文件识别和修复安全漏洞及性能问题，周期宜为半年/次。

6.2.3 数据库巡检

6.2.3.1 运维团队应检查数据库内存不超过为其分配的内存资源的 80%，数据库的连接数不超过中间件配置的最大连接数的 80%。

6.2.3.2 运维团队应审查数据库性能与可用性，审查指标包括分析吞吐量、事务处理速度及错误率等，并主从数据库间同步时间差应最小化。

6.2.3.3 运维团队应定期验证数据库版本与补丁更新，修补安全漏洞与性能缺陷，应通过分析日志文件识别及预防潜在的安全威胁与性能瓶颈，周期宜为 1 周/次。

6.2.3.4 运维团队应审查数据库备份策略，验证备份数据的完整性与可恢复性。

6.2.4 应用程序的 CPU 与内存使用率均应不超过其分配资源的 80%。

6.3 平台系统服务版本发布

平台系统服务版本发布流程包括：

a) 版本接收与审核：运维团队接收开发团队提交并已通过测试的软件版本，并审核其完整性。若版本不完整，需退回开发团队重新修正。

b）发布通知与准备：在收到项目经理的版本发布通知后，软件运维团队应详细阅读部署说明、版本说明、测试报告与操作说明。如发现问题，需立即与项目经理沟通并获得明确答复。

c）评审与计划制定：评审通过后，软件运维团队需制定详细的版本发布计划。发布流程与试运行：软件运维团队需提起发布流程，并安排试运行工作。试运行期间，应密切监控系统的稳定性和性能。

d）部署与验证测试：在试运行通过后，软件运维团队需执行版本部署工作，并进行后期的验证测试，确保所有功能正常运行且无新的 BUG 产生。

e）备份与归档：按照版本发布事件的要求备份新旧两个程序包，并将所有相关资料进行归档。

6.4 事件服务响应

软件运维应提供 5*8 小时的现场支持，7*24 小时的远程支持（如电话和站内短信），指定紧急联系人、责任部门快速响应处理问题，运维团队应通过故障事件数据库记录故障事件的分类、原因分析、处理结果等，并应制定预防措施及详细的灾难恢复步骤和计划，包括远程数据备份、定期灾备演练等。

7 自助终端服务管理

7.1 智能运维服务管理

智能运维服务管理要求包括：

a）码上报：通过手机微信扫终端上的二维码，获取终端的基本信息，并填写故障内容进行报修。

b）无感报障：利用终端监控技术，对终端上的硬件和软件进行监控，一旦发现异常，进行智能分析，由系统判断并自动化下发运维工单到相应的运维人员，通过系统安排运维人员上门解决故障。

c）服务审计：系统根据既定服务协议和规定制定监控策略，对巡检时效、维护时效、档案规范进行监控预警，并输出审计结果。

d）轨迹管控：运维人员在执行运维任务时，对每个工作地点进行 GPS 定位，并记录运维轨迹，系统提供运维轨迹数据分析，方便核实运维工作的的合规性和合理性。

e）数据分析：基于运维数据，从服务时效、终端故障率、故障类型、客户满意度等维度进行智能化数据分析，并提供指导性建议。

7.2 预防巡检服务

运维团队应建立季度性的政务自助服务终端预防巡检制度，识别并解决运行中的问题，减少故障发生率并提升稳定性。巡检内容及要求参见表 1。

表 1 巡检内容及要求

巡检部件	**巡检点**	**巡检要求及内容**
机柜	机柜外观	是否存在破损、脱漆的位置，并描述损坏严重程度。
	门锁	连续开、关锁 5 次没有卡阻情况，前门面板可正常支起不下。
	出纸口	测试打印 3 张纸张，是否发生不能送出出纸口的情况。
	功放	不存在杂音，能正常调节音量。
	散热风扇	顺畅运转，清理表面积尘。
	灯管	亮度是否正常，有否闪烁。
	标签	是否贴在正确位置，是否有翘起、脱胶现象。

	电缆线路	检查各个配件电源、数据线是否有破损。
	机柜环境	不能存在多余五金件等其它杂物、打印机、主机表面无积。
	导轨	拉入拉出 2 次无阻滞。
	指示灯	测试指示灯能否正常发光、熄灭。
触摸屏	显示	屏幕是否变色，是否有水波纹、亮点。
	灵敏度	触摸反应灵敏，在触摸屏上滑动，不可有中断现象。
	定位	触摸屏定位是否准确，测试 3 次，不可出现指针飘忽不定，不准确则较准。
	表面	触摸屏表面无破损、污迹。距离屏幕 30cm，从各个角度看，触摸屏表面不可有明显刮伤。
二代证阅读器	读取速度	使用测试程序测试 3 次，平均能在 3s 内读取二代身份证。
	读取内容	自助业务系统能正确使用二代身份证。
3 合 1 电动读卡器	传动	使用测试程序测试 3 次，可正常吸卡、吐卡。
	读取内容	可读取银行卡信息。
热敏打印机	打印	测试打印小票内容字体清晰、能切断票、不卡票。
激光打印机	打印	是否正常打印测试页，连续打印 5 张测试页是否出现卡纸现象，打印字迹是否清晰、有无墨迹。
金属键盘	输入	测试是否能正常输入数字，取消、确认、更正功能按键正常使用。
扫描枪	识别	是否正常识别测试用一维码、二维码。
工控主机	环境	清理机内及散热风扇积尘，检查内存等是否插接牢固。
	操作系统	查杀木马、病毒。
软件	业务功能	测试各业务功能是否正常使用，是否符合相关业务规则。

7.3 实施部署服务

运维工程师应在约定期限内上门，现场实施部署产品，并进行调试验证，最终满足客户对产品的使用需求。具体阶段如下：

a）实施准备阶段。业务部门应与客户达成一致，确定具体的执行时间和地点，并向实施团队传达详细要求，准备必需的资源和人员。

b）条件确认阶段。实施团队的负责人在收到任务后应在 2 个工作日内与客户联系，确认终端设备到货状态、预定的上门时间、以及现场的电源和网络条件，保证所有先决条件都已就绪。

c）现场实施阶段。实施人员应在现场安全开展设备的摆放、开箱、安装及配置工作，对设备进行正常工作测试，对客户的操作人员使用培训和指导。

d）终端验收交付阶段。终端设备完成部署后，实施人员应与客户进行终端设备的功能测试，完成客户验收、配件交付等全套部署服务。

7.4 故障维护服务

现场运维工程师在接收到故障工单后，应上门为客户提供运行维护服务，故障处理流程应遵守以下要求和流程：

a）准备与协调阶段。接收故障工单后运维工程师应携带完备的维修工具，并与客户协调确定服务时间。对不明确的故障描述，应提前与报障人沟通，获取详细信息，以便高效、精确地进行故障排查。

b）现场服务执行。运维工程师应按约定时间准时到达，进行现场服务。详细了解故障情况后进行系统的故障排查与修复，并验证系统恢复正常。应由客户签字确认服务完成并将谷物过程及结果上传至服务系统。

c）服务时效与响应。接收到故障报运维团队应在 30 分钟内响应，安排 24 小时内上门服务。一般故障目标应在 2 小时内解决，严重故障则争取 24 小时内修复。如需更换设备或部件，运维团对应在新设备到达后 24 小时内完成更换。

7.5 试运行服务

产品试运行是确保产品发布后达到预期应用效果的重要阶段，试运行过程中应密切关注产品的实际运行及使用情况，发现问题应立即反馈。试运行过程应遵循以下流程和要求：

a）试运行前准备。试运行启动前运营团队应了解业务背景，如详细的硬件规格和软件版本信息；应掌握产品部署的具体步骤，获取相关的安装和调试指南；应与业务部门紧密合作，明确试运行的目标、要求、时间安排、内容以及所需资源。

b）试运行执行。执行阶段应在指定环境中安装并调试硬件与软件，确保所有产品功能按照设计标准正常运行；应实施全面的数据收集和监控，包括通过用户反馈、终端管理员的观察以及实地监控。

c）试运行总结。试运行结束后，运维团队应编写详尽的试运行报告，包括执行过程、观察结果和出现问题的详细记录，发送给项目发起部门。

7.6 自助终端应急服务

7.6.1 应急管理机构与职责

应自助终端运维应急小组，设置组长和组员，组员应具备专业技术。小组的主要职责包括：

a）制定针对突发事件的应急技术保障方案，确保在紧急情况下能够迅速响应；

b）提供技术保障手段，为突发事件的解决提供有力支持；

c）攻克其他突发事件中遇到的技术难题，保障项目顺利进行；

d）对突发事件处理结果进行深入分析，并形成详尽的书面报告，为今后的应急工作提供参考。

7.6.2 应急要求

在事故发生后，坚持安全第一的原则，迅速响应，最大限度降低事故影响，阻断故障源，防止二次事故发生，保持通讯畅通，随时掌握事故动态；同时，迅速调集救助技术力量，控制事态发展。

7.6.3 应急处理基本流程

应急处理基本流程包括：

a）报告接收与上报。一旦运维工程师接收到突发事件报告，应立即上报给业主方和项目经理，并整理成详细的问题报告单。业主方和项目经理会迅速组织项目组，对事件进行初步分析和处理。

b）进展跟踪与反馈。在处理过程中，运维工程师需持续跟踪事件的进展情况，并及时向项目经理、项目组及事件提交人反馈处理结果。同时，详细记录每一步的处理过程。

c）事件总结与预防。当事件处理完毕后，业主方和项目经理应共同总结本次事件的经验教训，分析事件原因，并制定相应的预防措施，以避免类似事件再次发生。

8 平台系统监控管理

8.1 监控对象

监控对象的内容包括：

a）网络监控：覆盖网络设备（交换机、路由器、防火墙）的状态监控，DNS 解析的正确性，网络链路的稳定性，以及服务器的连通性。

b）操作系统监控：针对 Linux、Windows 等操作系统，监控 CPU 使用率、内存使用率、磁盘空间使用率、网络流量等关键指标。

c）数据库监控：涵盖 Oracle、MySQL、Redis、MongoDB 等主流数据库的连接状态、表空间使用率、缓存命中率等性能指标。

d）业务系统监控：根据业务系统的特点，定制监控内容，包括但不限于内存使用、线程池状态、业务使用情况等。

e）第三方接口监控：针对第三方接口的请求与响应报文，监控调用响应时间、返回值内容。日志内容监控：基于系统、应用等日志的规范输出，实施关键字监控，以发现潜在问题。

8.2 预警响应

运维团队应根据严重程度设置 P1-P3 三级预警，P1 预警应在 30 分钟内响应，P2 预警应在 1 小时内响应，P3 预警应在 2 小时内响应，应严格遵循每级预警的响应人员和时间要求。

8.3 监控报告分析

运维团队应形成监控报告，汇总并分析监控数据，为业务系统的优化和升级改造提供决策依据，周期宜为 1 周/次。

8.4 监控优化与升级

运维团队应根据业务需求和技术发展，不断优化监控策略并按月度维护并不断升级监控系统。

9 自助终端监控管理

9.1 设备状态监控管理

设备状态监控管理，实现对自助终端进行实时监控，对设备的基本信息、终端状态等重要指标进行监控管理，从而保证终端设备服务的连续性和可靠性，具体包括：

a）终端信息，包括于终端编号、终端名称、终端管理号、所属项目、所属机构、所属区域、所属布点、业务类型、设备名称、设备状态。

b）设备信息，如设备名称、设备状态。

c）监控管理，通过设备管理器将设备状态传到终端助手，最后回流至政务服务管理云平台。

9.2 软硬件信息监控管理

软硬件信息监控管理能够实现对自助终端进行硬件信息和软件信息管理，确保设备的配置与业务需求相匹配，避免因配置不当导致的性能问题。具体内容包括：

a）硬件信息如硬件类型、硬件厂家、启停状态。

b）软件信息如软件代码、软件名称、文件相对路径、基础路径。

c）监控管理。支持对软硬件信息进行增删改查操作。

9.3 耗材信息监控管理

耗材信息监控管理，实现对自助终端设备耗材管理，确保有效管理各设备耗材数量。具体内容包括：

a）耗材信息管理，包括但不限于耗材类型、关联设备、设备 ID、状态、可用数量、耗材预警值、启停状态。

b）监控管理，通过设备管理器将设备耗材状态传到终端助手，最后回流至政务服务管理云平台。

9.4 软硬件故障监控管理

软硬件故障监控管理，实现对自助终端软硬件运行状态实时监控，确保进行快速定位故障，采取相应的修复或更换措施。具体内容包括：

a）故障监控管理包括但不限于终端编号、终端名称、设备名称、设备类型、设备状态、状态持续时间、所属布点

b）监控管控，通过设备管理器将设备状态传到终端助手，最后回流至政务服务管理云平台。

9.5 业务数据统计管理

业务数据统计管理，涵盖业务量统计、点击量统计、开关机统计、终端分布统计和故障报警统计，实现对业务数据的深挖和分析。具体内容包括：

a）业务量统计：支持通过图表和列表的形式，展示各终端的业务量数据，包括但不限于业务量统计信息、各终端业务量的详细信息以及跨城业务量的办理情况。

b）点击量统计：实现通过图表和列表的方式，全面统计各终端的点击量数据，包括但不限于点击量统计信息、各终端点击量的详细信息以及跨城点击量的办理情况。

c）开关机统计：支持图表和列表的形式，精确统计各终端的开关机数据，展示各终端的开关机情况，为用户提供了终端运行状态的实时监控。

d）终端分布统计：支持图表和列表的形式，分别统计终端数量、各摆放点各种状态终端数的占比等终端分布情况。

e）故障报警统计：支持图示和列表方式展示各摆放点的终端故障报警数占比、故障类型占比、故障数及故障率。

f）监控管理：通过数据助手收集数据至终端助手，最后回流至政务服务管理云平台。

9.6 数据可视化监控管理

数据可视化监控管理，实现对业务各项数据的实时采集、处理与监控，以可视化的图表形式呈现，具体内容包括：

a）数据可视化信息管理：支持通过可视化图标形式展示包括但不限于终端数量、用户总数、终端预计个数、型号总数、今日终端趋势、今日终端状态情况。

b）监控管理：通过数据助手收集数据至终端助手，最后回流至政务服务管理云平台。

10 安全管理

10.1 概述

政务自助终端系统建设应按照国家关于信息安全等级保护三级系统保护要求进行系统安全体系设计，满足 GB/T 22239—2019 《信息安全技术 网络安全等级保护基本要求》中三级系统的防护要求。

10.2 服务器安全

服务器安全保障措施包括：

a）应安装并使用正版操作系统和最新的安全补丁。

b）应安装局方推荐的防病毒软件，并每月更新病毒库。

c）应强化用户安全策略，实施访问控制策略、强密码策略、密码过期策略、登录超时登出策略、输错密码锁定策略等，以增强用户账户的安全性。同时，禁用无用的账号，限制 root 用户的远程登录，并禁止 wheel 组用户免密切换 root 用户。

d）应配置 umask 值为 027，控制新创建文件和目录的默认权限。

e）应修改 SSH 的 Banner 信息与警告信息，向用户展示自定义的安全提示和合规性声明。

f）应禁用或限制潜在的高危服务，包括不限于 23、135、137、138、139、445 等端口。

g）应开启审计功能。

h）全面渗透测试及系统大更新或重大变更后的即时测试，使用包括 OWASP ZAP、Metasploit 在内的行业标准工具进行外部和内部漏洞探测，周期为半年/次。

i）应采用自动化工具如 Nessus、Qualys 进行漏洞自测，辅以手动检查，撰写漏洞详情、修复建议和后续验证结果的综合报告，周期为 3 个月/次。

10.3 网络安全

10.3.1 湾区通办政务自助服务网络开通应经过正式申请流程。

10.3.2 湾区通办政务自助服务网络开通前应经过严格审计。

10.4 中间件安全

中间件安全保障措施包括：

a）应安装并使用正版中间件软件。

b）应配置中间件的安全设置，包括不限于密码策略、启用 SSL/TLS 加密、设置访问控制列表、实施身份认证和授权等。

c）中间件管理员和审计员角色应由不同的人员担任。

d）应开启审计功能。

10.5 数据库安全

数据库安全保障措施包括：

a）应安装并使用正版数据库软件。

b）应配置中间件的安全设置，包括访问控制、密码策略和加密通信等。

c）应按照三权分立原则创建和管理数据库用户，实现权限的分离和制衡。

d）应设置每天异机备份的策略，并每月验证备份的可恢复性。

e）应开启审计功能。

10.6 业务应用软件使用安全

业务应用软件使用安全保障措施包括：

a）业务应用软件应完善自身的安全性和稳定性；

b）业务应用软件不应将所接入的局端业务系统的用户界面暴露给用户进行操作；

c）管理系统系统管理员、业务管理员、审计员角色应严格区分，分由不同人员担任；

d）政务自助终端应具备限制主机操作行为能力，屏蔽常见的危险操作；具备网络访问控制能力，只能访问与政务自助终端相关的网站和系统；具备病毒、木马防护能力，避免遭受病毒、木马程序的攻击；

e）政务自助终端应具备软件运行保护与限制机制，对于重点和关键的业务应用软件应对其运行进程加以保护，防止崩溃；对于未授权的软件进程应该禁止运行；

f）当终端业务应用软件处于维护或异常状态时，应设有适当的屏幕保护遮罩，防止非终端管理员

用户操作系统级别功能和系统文件。终端管理员用户需经过授权或密码校验后才可退出屏幕保护遮罩。

10.7 终端安全

10.7.1 终端硬件安全

自助终端需符合国标《GB/T 23647-2009 自助服务终端通用规范》规范中有关安全性要求：

a）终端整机采用厚度 1.5～2mm 的冷轧钢板，具有较好的刚度和强度，能防止由于空间变动、部件松动或移位造成的终端内部零部件损坏，防止部件发生电击和人身伤害，并且机身内部零部件紧固无松动，活动部件的动作灵活可靠，外部采用静电喷涂工艺，机身表面耐腐蚀、易清洁、不褪色。

b）终端机柜前后门均采用安全锁（非通配锁），防止强力开启机柜或越权开启机柜，可以有效提高抗破坏能力以及安全管理强度，确保终端内部设备和耗材的安全。

c）机柜的所有开口均设计具有适当的位置、大小、形状，以防止未经授权人员接触终端机柜内部的设备模块；

d）自助终端外部网络接口、电源接口设在终端机柜内部，且网线在终端内部有固定装置，在打开终端机柜后才能插拔网线；

e）终端提供独立的接地端子，所有外露的金属部件以及所有在使用或维护时可接触到的金属部件都与通过接地线与接地端子连接。

f）自助终端配置的金属密码键盘仅用于在业务操作过程中输入数字密码、数量、金额等业务信息，不提供与输入业务信息无关的操作功能，对触摸屏等操作设备则禁用了这些设备与输入业务信息无关功能，如鼠标右键功能；

g）终端外置的 USB 接口采用移动存储介质安全读写模块进行控制，而不是直接连接到终端工控主机，可防止通过外部接口侵入系统或将恶意程序引入系统。

10.7.2 终端系统安全

终端系统安全保障措施包括：

a）操作系统使用过程应稳定，无卡顿、死机等问题。

b）操作系统具备基本的安全防护功能，每月更新系统安全补丁，修复已知安全漏洞，并安装局方指定的防病毒软件，每月更新病毒库

c）终端应采取措施保护存储在其中的数据，包括加密敏感信息、实施访问控制等。同时，还需要遵守相关的隐私保护法规，确保用户数据的安全和合规性。

d）终端系统确保只有经过授权的用户能够访问终端设备及其存储的信息，采用强密码、生物识别等多因素身份认证方式，提高认证的安全性。

e）终端系统应备安全审计功能，能够记录用户操作、系统事件等关键信息，以便于后续的安全分析和溯源。

10.8 人员管理安全

人员管理安全保障措施包括：

a）运维人员应保守客户单位的机密，务必妥善保管所持有的文件。

b）运维人员未经许可，严禁对外提供密级文件、技术配置、工艺以及其他未经公开的经营情况、业务数据等。

c）严格遵守业务方驻场工作的规章制度，所有驻场工作的相关电子设备、计算机或电子介质等（如 U 盘、光盘等）应经过业主方许可方可接入网络并按照业主方规章制度进行管理。

d）未经业主方许可，禁止将任何设备接入业主方设备与网络。

e）禁止使用内网计算机连接手机、移动 WIFI 或无线上网卡等设备

f）未经业主方许可，禁止把内网计算机拿到业务单位以外地方维修

g）未经业主方许可，禁止把移动存储介质在内外网中互用

h）未经业主方许可，内网禁止使用无线路由，笔记本接入内网须关闭 WIFI

i）未经业主方许可，内网计算机禁止擅自接入互联网

j）存储介质接入内网时，应使用业主方认可的杀毒软件进行扫描杀毒

k）严格遵守驻场工作的工作流程规范，未经业主方许可，禁止擅自变更工作流程。

l）未经业主方许可，严禁擅自使用、挪动或拆卸业主方的设备（包括终端机、计算机、打印机、复印机、传真机等）或接入业主方网络。

m）未经业主方许可，严禁擅自变更接入网络的方式。

n）未经他方许可，不得随意翻看他人办公资料物品。应保密的资料，资料持有人应按规定保存。

o）未经业主方许可，严禁进行工作规范约定之外的任何操作。

p）涉及数据信息安全风险的操作，需业主方许可并由操作人员记录操作并签名、审核人审核操作并签名记录。

q）业主方提供的账号与密码等信息，严禁外泄，接触人员需承担由于自身管理原因导致账号外泄的一切责任。

r）个人计算机应设置一定复杂程度的密码，人离开应锁屏。

s）个人计算机禁止擅自交给他人使用。

10.9 安全检查

运维团队应定期组织系统渗透测试，以评估系统的安全性，发现并修复潜在的安全漏洞；应组织系统的攻防演练，通过模拟真实攻击场景，检验和提升系统的安全防护能力，周期均宜为一年/次。

参 考 文 献

[1] GB/T 16784 工业产品售后服务 总则
[2] GB/T 18789.1 信息技术 自动柜员机通用规范 第1部分:设备
[3] GB/T 18789.3 信息技术自动柜员机通用规范 第3部分:服务
[4] GB/T 20986-2023 信息安全技术 网络安全事件分类分级指南
[5] GB/T 23647-2009 自助服务终端通用规范
[6] SW/T 9-2014 自助办税终端系统技术规范