ICS 35.240.50
CCS L 67

T/STIC

团　　体　　标　　准

T/STIC 120076—2023

桌面及外围设备运维服务规范

Operation and maintenance Service specification for desktop teminal and peripheral

2023－08－10 发布　　2023－08－20 实施

上海市检验检测认证协会　　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。

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。

本文件由上海市检验检测认证协会提出并归口。

本文件起草单位：上海蓝盟网络技术有限公司、上海蓝盟信息技术有限公司、上海市计算机行业协会、上海微恺信息技术有限公司、上海欧测认证服务有限公司、上海添唯认证技术有限公司。

本文件主要起草人：夏立成、吴威巍、裘维东、佘灏程、陆凌云、谢柯、王栋、孙学刚、蒋文骏、王统、欧阳树生、黄惠杰。

首批承诺执行单位：上海蓝盟网络技术有限公司、上海蓝盟信息技术有限公司、上海市计算机行业协会、上海微恺信息技术有限公司、上海欧测认证服务有限公司。

桌面及外围设备运维服务规范

1 范围

本文件规定了桌面及外围设备运行维护服务在服务设施，服务人员，服务要求等方面的要求。
本文件适用于桌面及外围设备运行维护服务的设计、建设与管理工作。

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/T 28827.1-2022 信息技术服务 运行维护 第1部分：通用要求
SJ/T 11564.5-2017 信息技术服务 运行维护 第5部分：桌面及外围设备规范

3 术语和定义

GB/T 28827.1-2022界定的以及下列术语和定义适用于本文件。

3.1
桌面及外围设备 desktop termainal and peripheral
直接面向用户，具备计算、输入输出、数据通信、数据存储中一项或多项功能，用于使用或管理信息系统应用的终端设备。
[来源：SJ/T 11564.5-2017，3.1]

3.2
服务级别协议 service level agreement：SLA
运行维护服务组织与需求方之间定义服务和服务指标所形成的文件。
[来源：GB/T 28827.1-2022，2.8]

3.3
定期检查 routine check
根据既定的运行维护计划，以固定的频率对设备进行状态检查或信息记录。
[来源：SJ/T 11564.5-2017，3.8]

3.4
日常维护 daily maintenance
为了提高设备的使用效能和使用寿命,降低安全风险和成本浪费,供方对设备进行的主动服务操作。
[来源：SJ/T 11564.5-2017，3.9]

3.5
组织 organization
提供桌面及外围设备运行维护服务的实体或虚拟团队。

4 缩略语

下列缩略语适用于本文件。
AP: （网络）接入点（Access Point)
BIOS: （计算机）基本输入输出系统（Basic Input Output System)
DHCP： 动态主机设置协议（Dynamic Host Configuration Protocol)
DMZ： 隔离区CDeMilitarized Zone)
DNS： 网域名称系统（Domain Name System)
IIS应用： 联网信息服务(Internet Information Services)

IP： 互联网协议（Internet Protocol）
LPT：并行打印口（Line Print Terminal）
UPS： 不间断电源（Uninterruptible Power System）
USB： 通用串行总线（Universal Serial BUS）
WAN：广域网（Wide Area Network）

5 服务设施

5.1 信息化管理

组织应制定信息化建设发展规划，基于信息化管理体系，建立信息化管理平台，确保组织管理与项目运行管理协同，应包括以下功能：

a） 集成相关信息系统，实现组织管理与主营业务的信息化，推进组织管理信息系统中项目业务管理和财务管理的信息系统深度集成；
b） 集成知识库，实现知识的共享，充分挖掘和利用知识的价值，支撑智慧组织建设；
c） 集成监控工具，具备 IT 系统运行状况实时监视、故障预警告知以及远程支持的服务能力；
d） 集成服务台，包括服务请求的接收、记录、跟踪和反馈等流程，实现服务流程在线化；
e） 网络安全自查、巡检、风险评估及安全整改，并持续优化网络安全；
f） 容灾备份，具有灾难恢复系统、防病毒、防篡改、防泄漏系统。

5.2 备件管理

组织应具备并有效管理运行维护服务活动所需的备件资源的能力，包括但不限于：

a） 建立供应商选择和评价管理，规范备件的采购过程；
b） 建立备件出入库管理制度，规范入库备件的标识、使用、核销和账务管理；
c） 采用信息化工具对备件库管理，确保备件库信息真实有效；
d） 管理备件状态，以确保其功能满足运行维护需求。

5.3 智能运维工具

组织应根据运行维护服务的不同场景需求，规划和建设智能运维能力，结合人工智能、大数据、云计算等技术，开发或集成相应的运维工具，提高服务效率和质量。

a） 识别智能运维场景，分析运维场景的需求，目标，特征，可行性，形成设计方案；
b） 选择适宜的技术手段，构建实现能力，满足实时性，有效性，可靠性，安全性等技术需求；
c） 明确场景数据需求，对实现过程进行评审，优化和变更管控；
d） 使用数据建模工具，完成数据模型的定义、设计和开发；
e） 在数据存储，数据加密，数据压缩，队列调度等关键处理中采用相适宜的算法，满足元数据管理的需要；
f） 配置适当的资源满足智能运维工具的运行要求，包括计算，网络，存储等。
g） 建立评估机制，定期进行效果评估，制定改进措施，持续改进，快速迭代。
h） 覆盖服务的主要场景，包括并不限于软件分发，终端漏洞检测，终端日常巡检自动化，终端威胁 IP 检测，运维知识库智能应用，访问控制审核等，能力要求参考附录 D。

5.4 资产管理

组织应具备对软硬件资产进行管理的能力，包括但不限于服务器、工作站、虚拟桌面、网络设备、存储设备，以及各种操作系统、数据库、应用软件等。

a） 应识别和记录所有资产的状态和位置，以便于进行有效的管理和维护，满足资产管理的实时性和准确性需求；
b） 建立有效的通知机制，对未纳入管理的设备进行实时通知，提高设备管理的全面性；
c） 管理软件许可证，类别和合规性；
d） 统计特定软件的使用情况详细信息，例如使用次数，总使用时间，具有特定软件的系统等；
e） 在网络中检测，阻止和自动卸载禁止的软件；

f） 具有设备锁定功能，以保证设备的安全性和数据的完整性；
g） 按使用期限，磁盘使用情况，类型进行资产排序。；
h） 针对许可证数量及终端安装数量进行统计，当许可不足或过多时报警。
i） 支持将报告导出为 PDF 或 CSV 格式；
j） 资产管理统计效率达到 100 台/人天。

6 服务人员

6.1 基本要求

组织应对服务人员进行管理，包括但不限于：
a） 识别运行维护服务有关人员的分类，明确其职责、权限以及与岗位相适应的能力要求，如教育程度、专业技能、工作经验等。
b） 根据服务要求配备适合的管理和作业人员，特殊岗位按规定要求持证上岗。
c） 识别培训需求，制定并实施员工培训计划，做好员工上岗前和在岗中的培训。
d） 建立员工绩效考核管理制度，规定考核内容、标准，并将考核结果作为人力资源管理评价和质量管理改进的依据。
e） 建立和实施人才梯队培育制度，并定期评价培育规划的充分性、适宜性和有效性。

6.2 团队建设

组织应确定并配置满足服务所需的人员，包括：
a） 满足一线提供运维服务所需的人员，即在保持高绩效的同时具备良好的服务意识、职业素养以及运行维护基本知识和技能的人员；
b） 满足二线提供支持服务和服务管理所需的高潜人才，即在保持高绩效的同时具备领导意愿、取得成功的能力以及对组织有着更高敬业度的人才；
c） 在相应的行业领域和专业范围内配置满足战略发展需求的战略性人才；
d） 考虑行业未来发展趋势配置满足组织技术创新需要的研发人才。

6.3 行为监督

a） 组织应制定、实施能够体现组织文化并被全体员工认同和遵守的服务人员基本行为准则和日常行为规范；
b） 组织应依据基本行为准则和日常行为规范建立服务人员行为监督管理机制，监督、评价、分析、改进服务人员行为及其后续的工作内容与工作方式。

6.4 人员培训

组织应建立培训管理体系，包括：
a） 组织应依据理论、实训与实践相结合的培训组织体系以及相应的管理和激励；
b） 组织应有专门的部门进行培训的实施和管理，培训教育过程和结果应保留记录；
c） 组织应针对运行维护服务常见问题的描述、分析和解决方法建立相关的知识库，并利用信息化工具进行知识的收集、共享以及生命周期管理；
d） 组织应建立技能培训平台，并配置至少包括防火墙、无线网络、sd-wan 、网上行为管理设备在内的 IT 网络相关的主流厂商设备，以及虚拟化服务器平台和虚拟桌面平台部署环境；
e） 组织应至少每半年开展一次技能更新培训，培训内容至少应包括：windows 系统、exchange 邮件系统、文件系统、域环境、vsphere 虚拟化环境部署、主流虚拟桌面部署、交换机、路由器、防火墙、VPN 设备常规操作技能等；
f） 组织应设置专业技术人员和技术管理人员技术分级标准、培训及考核方案，定期评价培育规划的充分性、适宜性和有效性，相关人员应经培训并通过考核才能上岗。

7 服务要求

7.1 基本要求

7.1.1 服务要求

7.1.1.1 组织应根据客户需求提供包括但不限于电话支持，远程协助，应急服务，驻场服务，AI 服务，定期巡检等多种服务模式。

7.1.1.2 提供服务时服务人员应遵守以下共同要求：

a) 提供相应的服务前应征得客户同意，遇到需方提出额外要求时，服务人员应得到上级授权后再做处理；
b) 服务人员应确保个人联系方式畅通，表达准确，注意仪表和礼仪，在客户现场应遵守客户管理制度；
c) 运维工程师若不能按要求到场则需要在第一时间向组织说明，由组织安排其他运维工程师提供应急服务；
d) 对客户交代的每件事情要有始有终，跟进过程要及时汇报；
e) 事件完成时限应符合附录 A 的要求，处理及时率 ≥ 95%，服务可用性 ≥ 99.6%。
f) 应根据客户需求，制定数据灾备管理方案，参照附录 B。
g) 服务过程中应注重 IT 系统故障处理的规范性，尽量减低因操作不慎带来的风险，操作流程可参照附录 C。

注：服务可用性 =（ 1 - 故障时间/服务时间）×100%，故障时间和服务时间按年度平均值计算。

7.1.2 跨平台支持

组织应具备跨平台技术服务能力，支持管理多种主流操作系统，包括Windows，Mac，Linux，iOS,Android，tvOS，ChromesOS。

a) 开发统一的管理平台或接口，用以监控和管理多种操作系统上的资产，确保无论资产处于何种操作系统，均能够被有效地管理；
b) 提供自动化配置和部署工具，支持在多种操作系统上快速部署和配置软件及服务；
c) 实施跨平台的监控系统，用于实时收集多种操作系统的性能数据，并生成统一的报告，以便于运维人员分析和决策；
d) 定期进行兼容性测试，确保运维工具和应用在多种操作系统上都能够稳定工作，且具备良好的用户体验；
e) 建立灵活的访问控制策略，确保用户能够根据权限在多种操作系统上访问相应的资源和服务；
f) 制定统一的安全策略，确保在多种操作系统上都能执行相同的安全标准和措施；
g) 实现数据的跨平台同步与备份，保证数据的一致性和可恢复性；
h) 管理多种操作系统间的兼容性和依赖性问题，确保跨平台应用的连续性和稳定性；
i) 提供全面的技术支持，确保在多种操作系统上，用户都能获得及时有效的帮助；
j) 应覆盖主流操作系统 80%以上。

7.1.3 操作系统及应用补丁更新

组织应监控其所管理的所有系统和应用运行状态，及时发现并修复安全漏洞，缩短更新周期，保障IT环境的稳定和安全。

a) 建立实时监控机制，对所有管理的操作系统和应用的运行状态进行监控，以便及时发现异常或潜在的安全漏洞，并通过警报系统快速通知运维团队；
b) 对发现的安全漏洞进行评估，根据漏洞的严重性和对业务的影响程度，为补丁更新制定优先级，确保关键系统的安全性最先得到加强；
c) 采用自动化工具来管理补丁的下载、测试和部署过程，减少人为操作的错误，提高补丁管理的效率和准确性；
d) 对补丁部署后的系统和应用进行验证，确保补丁正确应用且不影响系统的正常运行；
e) 在进行补丁更新前，确保有完整的备份，以便在更新出现问题时能够快速回滚到稳定状态；
f) 更新周期应在补丁发布后的 45 天内完成。

7.1.4 终端软件自动部署

组织应采取自动化和批量化的方式对终端软件进行部署，包括新软件部署，软件更新与补丁应用，配置变更，软件许可证管理，应急响应，硬件更换或升级，遵从性和审计，远程办公支持等场景，提高准确性和部署效率，提升运维效率。

a) 明确组织的需求，包括需要部署的软件类型、目标终端的数量和类型、预期的部署时间等；
b) 根据需求分析的结果，选择合适的自动化部署工具。工具的选择应考虑其是否支持跨平台部署、是否具有丰富的功能、是否易于使用和管理等因素；
c) 对工具进行合理配置。包括设置部署策略、定义部署流程、配置软件仓库等；
d) 在少量终端上进行测试部署，验证配置的正确性和部署的效果，测试部署的结果将为实际部署提供参考；
e) 测试部署成功后，在所有目标终端上进行实施部署。在部署过程中，需要密切监控部署的进度和结果，及时发现并解决问题；
f) 部署完成后，需要进行后续的管理，包括监控软件的运行状态、更新软件和补丁、管理软件许可证等，根据实际运行情况，调整部署策略和流程，以提高部署的效果；
g) 自动化和批量化应覆盖 90%以上的部署场景。

7.1.5 终端自动运维操作

组织应采取自动化和批量化的方式执行常规运维操作，包括系统监控，日志管理，用户账户管理，安全管理，备份与恢复，网络配置，资产管理，故障响应等场景，降低出错率，提升运维效率。

a) 对运维流程进行彻底的审查和评估，确定可自动化的操作。制定全面的自动化策略，包括目标、时间表、预算和资源分配；
b) 根据自动化需求选择合适的工具和平台，包括监控工具、日志分析器、配置管理系统、安全扫描工具、备份软件等，确保工具可集成并协同工作，提供统一的自动化解决方案；
c) 准备必要的基础设施，包括服务器、存储和网络资源，以支持自动化工具的部署和运行，确保有足够的容量来处理监控数据、日志文件、备份集等；
d) 开发自动化脚本和流程，以执行常规任务，如监控性能指标、收集和分析日志、管理用户账户、安装和更新软件、维护系统配置、执行安全扫描、管理网络设置、跟踪资产和故障响应；
e) 在控制环境中对自动化脚本和流程进行测试，应确保按预期工作，不会干扰现有的业务流程，验证自动化操作是否符合安全标准和合规要求；
f) 测试完成后，逐步部署自动化解决方案到生产环境。监控部署过程，确保自动化操作不会导致服务中断或其他问题；
g) 应持续监督性能和效率，收集反馈，根据实际运行情况不断改进自动化流程，确保覆盖率达到目标，对于无法自动化的特殊情况，应制定手动处理策略；
h) 应为运维团队编制完整的操作文档，说明自动化系统的工作原理和操作方法。对团队成员进行培训，确保能够有效地使用自动化工具和处理异常情况；
i) 定期进行安全审计和合规性检查，以确保自动化操作不会引入新的安全风险，并且符合行业标准和法规要求；
j) 应进行持续的监控和维护，以应对基础设施变化、新的安全威胁、软件更新和其他可能影响自动化效率的因素；
k) 自动化和批量化应覆盖 90%以上的运维操作场景。

7.2 电话支持

7.2.1 电话支持是指通过电话指导客户快速解决问题，适用于简单易操作，可在 10 min 内排除的故障类故障，采用电话支持前应与客户进行沟通，判断客户针对相关问题的操作能力是否适合采用电话支持。

7.2.2 电话支持服务应至少符合以下要求：

a) 操作过程描述清晰，并和客户确认每一步操作显示的窗口和现象；
b) 如果某些步骤等待时间比较长，提前向客户说明；
c) 如果尝试过一两种方法，故障仍不能解决，向顾客建议改由运维工程师上门服务。

7.3 远程协助

7.3.1 远程协助是指通过远程控制软件登陆客户桌面协助客户解决问题，仅适用于网络正常情况下的

桌面类的故障。

7.3.2 远程协助服务应至少符合以下要求：

a) 远程报修需要记录客户名称、联系人、联系方式、报修问题；
b) 远程连接后，先让客户操作确认故障现象，并提醒客户自行保存文档，再按照常流程处理；
c) 结束服务时由客户先断开远程后，服务人员才能断远程；
d) 如果尝试过两种或以上方法，故障仍不能解决，向顾客建议改由运维工程师上门服务。

7.4 应急服务

7.4.1 应急服务是指接到客户报修后，派遣运维工程师进行上门服务，适用于比较复杂，需要全面地排查，预估处理比较长的故障。应急服务的范围包含所有在 SLA 范围内的故障内容。

7.4.2 应急服务应至少符合以下要求：

a) 组织应根据服务规模配置相应的运维工程师，密度比应至少达到 1:18（运维工程师 ： 客户数量）；
b) 应及时响应客户需求，并初步确认故障原因及处理方式，响应时间 ≤ 5 min；
c) 应急事件需要记录客户信息、联系人信息、处理事务、预约到场时间、服务地址；
d) 运维工程师出发前应检查确认所携带的工具、服务单、系统盘，人员到场时间 ≤ 2 h；
e) 运维工程师现场进行的所操作都应在工单上进行记录，内容至少包括工作内容，服务标签、耗时、处理过程、是否解决；
f) 对复杂或存在风险的工作做好预案，经审核后实施，如现场碰到 30min 内无法处理问题直接进行问题升级；
g) 工单完成后客户签字确认，该项目服务经理审核工单关闭服务事件。

7.5 驻场服务

7.5.1 驻场服务是指派出运维工程师驻扎在客户现场进行服务，适用于对可用性和连续性要求比较高的项目，可及时响应客户需求，服务的范围应包含所有在 SLA 范围内的故障内容。

7.5.2 驻场服务应至少符合以下要求：

a) 应自备工具、服务单、系统盘；
b) 应按客户方上班时间准时上下班并按组织要求做考勤记录；
c) 按标准的工作清单提供服务并填写工单，内容包括工作内容，服务标签、耗时、处理过程、是否解决；
d) 工单完成后客户签字确认，该项目服务经理审核工单关闭服务事件
e) 服务中如果碰到无法解决的技术问题，应提交问题升级；
f) 应主动询问客户负责人是否有其他工作安排，主动帮助客户员工。

注：驻场人员如需请假或调休，应按组织人事管理制度执行，并提前至少一天告知客户，同时组织应为客户提供临时代班的驻场人员。

7.6 AI 服务

7.6.1 AI 服务是指在服务过程中利用人工智能技术，为客户提供交互式服务的智能服务系统，替代人工进行客户服务，实现信息的智能化处理。

7.6.2 AI 服务应至少符合以下要求：

a) 宜实现对声音的实时采集和识别，自动将语音处理成自然文本；
b) 宜集成人工智能技术驱动的自然语言处理工具，具有语言理解和文本生成能力；
c) 宜集成组织知识库，并训练运维工程师模型，根据客户输入的关键词，进行检索查询，可回复或处理技术问题；
d) 宜利用大数据建模和算法实现，处理客户日常运维数据，用于加速服务报告生成和服务需求预测。

7.7 定期巡检

7.7.1 定期巡检是指对电脑（硬件或者虚拟桌面）、服务器、网络设备、打印机等设备在运行一定时限后进行定期检查，提前建议客户进行备件更换或者设备扩容，有助于预防问题的发生，服务的范围应

包含所有在 SLA 范围内的巡检内容。

7.7.2 定期巡检应至少符合以下要求：

a) 按照 SLA 约定制定巡检计划，内容包括巡检项目，巡检周期，巡检要求；
b) 执行巡检任务前应提前征得客户同意，运维工程师按时抵达现场根据巡检工单进行巡检；
c) 巡检完成后客户签字确认，一周内提交巡检报告；
d) 针对巡检中发现的问题，按照 SLA 约定的方案进行处理。

8 信息安全

应符合GB/T 28827.1-2022 中7.12 的要求，无因组织管理不当导致的泄密事故发生。

9 持续改进

应符合GB/T 28827.1-2022 中5.3.4的要求。

10 评价要求

10.1 评价准则

10.1.1 第 5，6，7，8，9 章给出了桌面及外围设备运维的服务要求，其评价应依据附录 E 表 E.1 给出的评价工具实施。

10.1.2 评价人员基于表 E.1 实施桌面及外围设备运维的服务要求评价：

a) 表 E.1 是根据第 5，6，7，8，9 章的要求，赋权量化构建的服务要求评价表，设定满分值为 100 分;
b) 给出基于李克特 5 点式量表的评价内容体验系数 α ,如下：
c) 远低于预期：0≤ α ≤0.2；
d) 低于预期：0.2＜ α ≤0.4；
e) 符合预期：0.4＜ α ≤0.6；
f) 高于预期：0.6＜ α ≤0.8；
g) 远高于预期：0.8＜ α ≤1.0。
h) 用表 E.1 中给定的每一项评价内容的分值乘以该项的体验系数 α 后求和，得出服务要求评价得分。

10.2 评价结果

桌面及外围设备运维服务评价结果分为通过、不通过。其中：

a) 通过是指服务要求评价达到 80 分（含）以上；
b) 当桌面及外围设备运维服务评价发生下列任一情况时，评价结果为不通过：
c) 服务要求评价低于 80 分；
d) 评价期间组织因重大违法违规行为而受到行政处罚；
e) 评价期间组织提供的服务发生重大安全或舆情事故，社会影响恶劣。

附 录 A
（规范性）
运维服务级别及完成时限

A.1 驻场运维服务级别及完成时限

驻场运维服务分类，服务项，服务可用时段，服务响应时限，服务完成时限，以及服务优先级要求应符合表A.1。

表A.1 驻场运维服务级别及完成时限

服务大类	服务小类	服务项	服务可用时段	服务响应时限	服务完成时限	服务优先级
桌面终端维护	PC硬件	PC端内存、硬盘等配置升级	工作日	1 d	3 d	4
		PC电脑硬件安装或更换（不含采购时间）		20 min	1 h	4
	虚拟桌面终端硬件	终端硬件固件更新		1 h	2 h	4
		终端硬件部署和安装（不含采购时间）		20 min	40 min	4
	办公软件	新电脑操作系统或非标软件安装、操作系统修复或优化		20 min	1 h	4
		办公标准软件安装		10 min	30 min	3
		办公软件应用维护、软件使用咨询		20 min	2 h	3
	数据备份	移动存储数据备份		1 h	4 h	4
		备份软件备份数据		30 min	2 d	4
	电话服务	电话安装、功能变更		20 min	1 h	3
		话机移动		20 min	1 h	4
	电子邮件服务	员工邮箱或公共邮箱或邮箱组建改删		20 min	1 h	3
		邮件客户端设置（设置OUTLOOK邮箱配置）		30 min	1 h	3
		邮件客户端排错		30 min	2 h	3
		邮箱数据恢复，容量扩容		20 min	2 h	4
	互联网服务	访问权限设置、使用权限开通、无法访问排错		30 min	1 h	4
	打印/传真服务	打印机安装、共享打印机设置		20 min	30 min	3
		传真、电子传真号码申请，传真移机		20 min	2 h	4
	文件共享	共享目录设置、共享目录历史文件恢复		20 min	2 h	4
		共享目录权限更改、共享目录扩容		20 min	1 h	3
		部门文件发布		30 min	2 h	4
	特殊办公支持	电话会议申请、无限卡申请及交付		20 min	1 h	4
		专用网连接、移动网卡安装		1 h	4 h	4
		会议室网络环境支持		10 min	30 min	3
	域账号	员工域账号建改删（密码重置）		20 min	1 h	3
		VPN权限建改删		20 min	4 h	3
	员工桌面配置（PC硬件）	包括：安装桌面电脑、安装标准办公软件、分配并配置个人邮箱、安装或连接相应的打印机。		30 min	3 h	5
	员工桌面配置（虚拟桌面终端硬件）	包括：安装桌面电脑、安装标准办公软件、分配并配置个人邮箱、安装或连接相应的打印机。		30 min	2 h	5

表 A.1 驻场运维服务级别及完成时限（续）

服务大类	服务小类	服务项	服务可用时段	服务响应时限	服务完成时限	服务优先级
	员工异动权限改删	包括：域账号、邮箱、应用系统、上网权限的改动或清除		20 min	1 h	3
	工位变动支持服务	办公桌面移动，包括：重要数据备份、设备拆除、搬移、安装、打印机服务配置变更、电话服务变更等。		1 h	1 d	5
	特殊环境服务	用户培训环境、特殊安全环境构建与拆除		1 h	2 d	5
	电脑巡检服务	PC电脑及虚拟桌面运行状态的巡检工作		20 min	1 d	5
业务支持	应用支持	业务系统全局性服务完全中断故障	所有日期	即时	1 h	1
		业务系统片区域部分线上或线下订单处理关键业务服务中断故障		即时	2 h	2
		业务系统单点部分线上或线下订单处理等关键业务服务中断故障		20 min	4 h	3
		业务系统部分线上或线下订单处理等非关键业务服务中断故障	工作日	20 min	8 h	4
		业务系统使用咨询		5 min	30 min	4
		业务数据提取、差错数据修改		1 h	2 d	4
	IT资源	应用系统账户建改删、呼叫中心话务配置、配置发放回收、密码重置		1 h	8 h	4
		配置账单提供		2 h	2 d	5
	通报	重大故障通报、内外部维护通报、最新业务通报	所有日期	即时	20 min	1
信息安全管理	安全支持	特殊环境数据导入/导出	工作日	1 h	8 h	2
		访问控制权限管理	所有日期	1 h	5 d	4
	安全服务	技术环境安全评估、应急预案及应急演练	-	-	1 次 /2 月	3
		病毒防护系统维护	所有日期	-	1次/天	3
		安全设备性能巡检		-	3次/天	4
		电脑病毒查杀	工作日	3 0min	2 h	4
基础环境维护	机房物理环境维护	空调制冷设备、消费系统、环境监控系统、安防系统、防雷接地、温湿度、UPS设备、柴油发电机设备、线缆的标识和标签巡检	所有日期	-	3次/天	4
	IT基础环境日常维护	网络设备性能、网络线路带宽流量、服务器设备性能、操作系统运行环境、虚拟化环境监控		-	实时	3
		客户端月度例行巡检		-	10台电脑/h	4
技术支持	办公室自动化支持	AD域、企业邮箱、ITSM应用、电话系统维护		20 min	4 h	3
		财务、人力、审计专用系统技术支持	工作日	20 min	4 h	3
	业务类技术支持	研发相关系统环境需求分析		1 h	3 d	3
		研发相关系统环境搭建		1 h	-	3
		硬件设备选型与测试、容量规划管理	-	-	-	3
	其他	用户培训	工作日	5 d	7 d	4
		IT行政事务		2 h	3 d	4

表 A.1 驻场运维服务级别及完成时限（续）

服务大类	服务小类	服务项	服务可用时段	服务响应时限	服务完成时限	服务优先级
事件处理	安全事件支持	安全事件处理	所有日期	即时	8 h	1
	办公环境故障支持	旧电脑操作系统重装、业务办公软件故障处理	工作日	20 min	2 h	3
		PC电脑硬件故障送修		20 min	-	4
		互联网线路、电话线路、传真机、公告打印机故障处理		20 min	4 h	3
	基础环境故障支持	基础环境故障处理		即时	2 h	1
运维报表	服务报告	服务台关键KPI、客户服务月报		-	次月第一个工作日	2
	基础环境报告	基础环境运行分析月报		-		2
	运维报告（客户自行选择，可单选或多选）	运维月报		-		2
		运维周报		-	次周首日	2
		运维日报		-	次日上午10点	2

注1：服务优先级共分1级-5级，优先服务等级依次递减。
注2：所列运维服务级别内容不包括以下自然灾害、外因或规划性事情。
——地震、台风、洪水等自然灾害；
——战争、罢工、停电、政府行为等；
——政府电力部门或电信部门的行为；
——电信线路被人为破坏或骨干网线路、设备因调试、扩容所引起的中断；
——互联网公网阻塞或其他通路（如访问目的地的服务器响应速度）问题；
——外部人为破坏因素引起的， 超过设备的承载能力；
——第三方服务提供商因素引起的；
——业务操作人员在没有技术人员的指导下或私自操作造成服务中断的；
——因业务发展的需要在正常上班时期进行服务维护的；
——因规划需要，计划内的维护。

A.2 远程运维服务级别及完成时限

远程运维服务分类，服务项，服务可用时段，服务响应时限，服务完成时限，以及服务优先级要求应符合表A.12。

表A.2 远程运维服务级别及完成时限

服务大类	服务小类	服务项	服务可用时间段	服务响应时限	服务完成时限	服务优先级
桌面类远程	办公软件	办公标准软件安装	工作时间	10 min	30 min	3
		非标准软件安装	工作时间	10 min	1 h	4
		办公软件应用维护	工作时间	10 min	30 min	3
		办公软件使用咨询	工作时间	10 min	30 min	3
	电子邮件服务	员工邮箱新建修改删除	工作时间	10 min	20 min	3
		公共邮箱新建修改删除	工作时间	10 min	20 min	3
		邮箱组新建修改删除	工作时间	10 min	20 min	3
		邮箱归档，收发软件设置&排错	工作时间	10 min	30 min	3

表 A.2 远程运维服务级别及完成时限（续）

服务大类	服务小类	服务项	服务可用时间段	服务响应时限	服务完成时限	服务优先级
	互联网服务	互联网访问权限设置	工作时间	10 min	30 min	4
		网络使用权限开通	工作时间	10 min	30 min	4
	打印机服务	打印机安装	工作时间	10 min	15 min	3
		共享打印机设置	工作时间	10 min	30 min	3
		打印机排错	工作时间	10 min	30 min	3
	共享盘问题处理	共享目录设置（局域网共享）	工作时间	10 min	1 h	4
		共享目录权限修改	工作时间	10 min	1 h	3
		共享目录历史文件恢复	工作时间	10 min	2 h	4
	域环境	员工域账号新建修改删除（密码重置）	工作时间	10 min	15 min	3
		客户端加域退域	工作时间	10 min	30 min	3
注：服务优先级共分1级-5级，优先服务等级依次递减。						

附 录 B
（资料性）
数据灾备管理

B.1 数据丢失和应用中断因素

组织应根据客户需求，制定数据备份与恢复的机制、策略、规范、流程和应急保障措施，满足客户不同级别数据的存储安全保护要求。数据备份和恢复应保障数据存储过程的保密性、完整性、可用性和可追溯性。数据丢失和应用中断因素见表B.1。

表B.1 数据丢失和应用中断因素

序号	类别	内容
1	自然因素	地震、火灾、雷电、 洪水、 腮风、 工业事故等。
2	人为因素	盗窃、蓄意破坏、 病毒、缺乏经验造成的误操作、 压力和恐慌造成的误操作等。
3	硬件故障	硬盘损伤、 服务器岩机、 电源故障、 存储器故障等。
4	软件故障	数据库设计缺陷、 应用软件故障、 操作系统故障等。
5	网络故障	络连接问题、 网卡和驱动程序故障等。

B.2 数据安全风险

B.2.1 单服务器运行风险

若不对单机架构的应用服务器数据采取有效的数据安全保护措施，应用系统面对人为误操作、病毒、网络攻击、软硬件故障、自然灾害等意外事件时缺少必要的安全保护，极易造成数据丢失，甚至将严重影响到业务的正常开展，带来巨大的经济损失以及负面影响。另外，操作系统也需要进行保护，否则重大故障发生时，需要先重新安装操作系统、重装所有应用程序，然后才能恢复数据，耗费相当长的时间才能够重新恢复应用。

B.2.2 手工备份弊端

采用手工方式进行备份将无法避免会出现漏备、 误备等情况， 备份的数据也难以管理。

B.2.3 本地数据中心损毁风险

本地信息化安全措施无法防范水灾、地震等重大灾难对本地机房的整体性摧毁，因此需要建设更高安全保护等级的灾备系统，如异地数据灾备系统。异地数据灾备要求在异地保存与本地一致的备份数据，灾难发生后， 当无法从本地恢复时，可以从异地恢复系统和数据，确保用户原有的数据不会丢失或遭到破坏。

B.3 数据备份方案

数据备份方案见表B.2。

表B.2 数据备份方案

方式	描述	优点	缺点
普通双机热备	两台服务器通过磁盘阵列实现双机热备，在一台服务器出现问题的时候，可以马上切换到另外一台服务器继续运行。但如果磁盘阵列出现问题，整个系统将不能正常运行。	在主机出现故障，比如电源、内存、硬盘等硬件设备出现故障，另外一台服务器可以马上代替工作。	磁盘阵列是整个系统的瓶颈，磁盘阵列出现故障后，需要专业人员进行数据恢复，并且存在数据丢失与完全无法恢复的可能。

表 B.2 数据备份方案（续）

方式	描述	优点	缺点
全冗余双机热备	由两台服务器、两套磁盘阵列再加上专用磁盘阵列同步软件以及相关连接设备构成。	服务器或磁盘阵列任何单个设备出现问题，备份设备可以及时代替工作。	系统复杂程度高，除了双套设备之外，还有许多连接设备及软件，导致系统维护成本高。由于存在着数据同步的过程，因此整体运行性能较低且造假高。
NBS备份	在局域网内设置一个专用存储服务器，通过FTP等通知协议继续定期数据备份。	备份机制独立，系统维护起来简单。 支持异地备份， 可 以避免机房发生火灾等严重损害时，可以保证数据不丢失，数据恢复容易，成本低。	不能实现实时备份，一般备份周期为一h或者一天。

B.4 数据备份策略

B.4.1 数据库备份策略

数据库备份策略见表B.3。

表B.3 数据库备份策略

实时策略	关键应用的数据库采用实时备份： 设置数据库为在线 CDP 持续监控备份， 保留 3 个月的连续性各份数据，保证数据趋于 0 丢失。
定时策略	非关键应用数据库：建议每周至少做 1次欠完全备份，周末进行；每天做 1 次增量备份，每 4 h做 1 次归档日志备份（勾选 “删除已备份的本地归档日志 ” ）。保留三个月的完全备份版本数目。
	数据库访问非常频繁：若只能容忍半h或 10 min的数据丢失，则应加大各种各份的频率。应每周备份 2次～3 次全备份，每天至少备份 2次增量备份、每半h进行 1 次归档日志备份。
	用户数据库非常大：则备份需要消耗更长时间，应按照最佳备份策略进行备份。
	用户数据库数据非常重要，需要经常恢复到某个时间点，则应加大归档日志备份频率， 应每0.5 h进行一次归档日志备份。保留更多完全备份版本。

B.4.2 文件备份策略

文件备份策略见表B.4。

表B.4 文件备份策略

实时策略	重要文件资料设置为对全盘所有文件进行实时监控，默认排除类型：tmp、 temp、exe、rmvb、rar、 MP3。同一个文件的实时备份间隔为连续，每个文件保留500个版本。对超过200M前文件，实时各份间隔为1h，每个文件保留10个版本。
定时策略	非关键性资料采用定时备份：初始为完全备份，每天做1次差异备份；保留 1个月的备份版本数目（即备份保留版本数为30个）。
LAN-Free备份策略	大数据LAN-Free备份：针对服务器数据量大的文件数据，采用LAN-Free方式备份，晚间进行。

B.4.3 操作系统备份策略

操作系统备份策略见表B.5。

表B.5 操作系统备份策略

在线热备策略（定时）	操作系统（含应用程序）设置在线热备份：操作系统盘采取镜像文件备份，每月初做备份，晚间进行：保留3个月的备份版本数目（即备份保留版本数为3 个）。

B.5 灾难恢复

系统出现故障，导致不能运行的时候，应有排除故障的预案，以便于及时解决故障并迅速使系统正常运行，表B.6对可能出现的故障进行列举，并列出故障排除方案。

表B.6 常见故障排除方案

故障类型	故障点	故障排除方案
硬件故障	电源、内存等非存储相关设备故障	确定故障点，更换故障配件，如故障配件没有备份配件，联系相关配件生产厂家进行采购；如配件发货周期较长，可考虑把同类型服务器的配件暂用替换下，先拷贝数据出来，然后在其他备用服务器上安装程序，以及恢复数据，使系统尽快地先恢复起来。
	硬盘或者磁盘阵列 故障	如出现一块坏硬盘,可通过替换相同类型的硬件,服务器自带Raid5功能，将自动修复。如多块硬盘出现故障，数据无法读取的时候，首先查找备份文件，如备份文件较新，如是一天内的备份数据，此时应评估丢失的数据是否重要或者可以通过其他方式恢复。如不重要或者可以通过重新录入恢复，则用备份服务器上的数据进行数据恢复；否则应请专业磁盘数据恢复公司进行数据恢复。
软件故障	操作系统故障	首先确保数据没有丢失的情况，备份数据，然后重新安装系统以及数据库，并重新安装相关应用程序，最后进行数据恢复。
	应用程序故障	联系应用程序开发厂家，要求进行售后支持，或者根据厂家提供的安装程序，进行重新安装部署。

附 录 C
（资料性）
操作流程

C.1 计算机重新安装系统操作流程

计算机重新安装系统操作步骤及注意事项与说明应符合表C.1的要求。

表C.1 计算机重新安装系统操作流程

操作步骤	注意事项与说明
确认重装系统	a）根据计算机重新安装系统条件判定为重新安装系统； b）系统盘由客户提供。如客户不能提供，则运维服务人员安装官方版系统，版权由客户负责，并向客户确认。
数据备份	a）虚拟桌面系统资料，进行整机备份。 b）备份系统盘资料。 如需运维服务人员操作， 应该提前声明运维服务人员不对资料的损坏、丢失负责； c）备份储存介质由客户提供。 如客户不能提供， 则使用运维服务人员备份储存介质前须经过客户同意，并在资料还原后经客户检查恢复完成后， 将客户备份在运维服务人员储存介质上的全部资料完全删除； d）记录 IP、 DNS、打印机等网络配置； e）和客户确认其他需要保存的资料，并妥善保存，并由客户签字确认资料已经保存。
检测安装	a）检测硬盘是否有坏道、 内存条是否报错和其他硬件是否有报错或异常， 如有坏道或报错 等异常应主动及时向客户提出，并提出合理的建议； b）检测硬件配置， 根据计算机系统安装标准确定电脑可以安装的系统版本。 如客户需要安装更高版本的系统， 则须给客户说明情况， 表明此硬件安装高版本系统可能会导致运行异常或不畅； c)所安装系统如果是运维服务人员自备的，系统文件应是官方的、安全的且经过验证的，系统版权由客户负责。
软件安装	a）安装软件时， 如果软件是运维服务人员自备的， 则软件应是官方的、 安全的且经过验证的， 也可参照平台计算机软件安装标准进行； b）安装软件时，安装顺序为： 杀毒软件→驱动→压缩软件→OFFICE→专业软件→邮箱及配 置导入邮件→导入其他备份资料→测试； c）让客户确认是否还需安装其他软件。
验收确认	a）首先自己检查设备是否恢复正常； b）经检查无误后交给客户检验， 由客户检验完成后签字确认。
注：符合以下情形之一，计算机应重新安装系统： a）客户请求服务； b）系统宕机，且无法恢复状态时； c）为确保系统满足用户使用需求。必要时，经客户确认批准。	

C.2 软件安装操作流程

软件安装操作步骤及注意事项与说明应符合表C.2的要求。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/556103021113011105