ICS 35.240.01
L00

T/ZJSZJJ

团　　体　　标　　准

T/ZJSZJJ 0004—2025

国产桌面终端安全基线配置与防护通用技术规范

General technical specifications for security baseline configuration and protection of domestic desktop terminals

2025－12－05发布　　2025－12－06实施

浙江省数字经济联合会　　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。

本文件浙江省数字经济联合会提出并归口管理。

本文件起草单位：国网江苏省电力有限公司信息通信分公司、国网江苏省电力有限公司淮安供电分公司、福建亿榕信息技术有限公司、浙江省质量科学研究院、杭州吉网通信技术有限公司。

本文件起草人：王磊、庄岭、刘建戈、丁一新、宋浒、张鹏宇、邵剑飞、张富林、郭伟强、陈志彬、汤知源、白润泽。

国产桌面终端安全基线配置与防护通用技术规范

1 范围

本文件规定了国产桌面终端的安全基线配置与防护通用技术要求，涵盖基线配置技术要求、防护技术要求及相应的测试方法。

本标准适用于搭载国产操作系统的桌面终端，可用于指导该类终端在安全基线配置、防护措施实施及合规性测试等场景中的实践，同时适配等级保护、安全评估等相关要求。

2 规范性引用文件

下列文件的内容通过文中的规范性引用文件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—2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

GB/T 29240-2024 网络安全技术 终端计算机通用安全技术规范

GB/T 37092—2018 信息安全技术 密码模块安全要求

3 术语和定义

GB/T 29240-2024、GB/T 22239—2019 界定的以及下列术语和定义适用于本文件。

3.1

安全基线

能够满足国产桌面终端（含虚拟化环境）安全基本要求的一组配置项基值构成的集合，涵盖系统参数、权限设置、防护规则等核心安全配置。

3.2

国产桌面终端

配置了麒麟、统信等国产操作系统及其他国产硬件的计算机终端。

3.3

身份鉴别

用特定信息对用户身份的真实性进行确认。用于鉴别的信息一般是非公开的、难以仿造的。

3.4

访问控制

对主体访问客体的权限进行限制，以确保只有经过授权的主体才能访问特定客体的安全机制。

4 基线配置流程及要求

4.1 基线数据采集

4.1.1 应采集国产桌面终端当前系统的关键配置信息，包括但不限于账户权限、口令策略、访问控制规则、开放端口状态、系统服务运行情况、内核参数配置、启动项管理、安全审计策略等安全相关配置项。

4.1.2 采集结果应包含配置项的原始值、所属安全域、配置路径、采集时间、采集工具版本等元数据，确保可追溯性。

4.1.3 采集过程应采用自动化工具或标准化脚本执行，减少人工操作误差，且采集行为不得影响终端正常运行，资源占用率应低于 5%。

4.1.4 采集频率应至少每月一次，高风险环境应提高至每周一次，并支持按需触发采集。

4.1.5 采集数据在传输和存储过程中应进行加密处理，防止敏感信息泄露。

4.2 基线制定

4.2.1 应基于终端安全需求、业务场景及相关国家标准，结合基线数据采集结果，确定基线配置项的核心要素，包括基线名称、风险等级、配置要求、检测方法、加固方案及合规依据。

4.2.2 基线配置项应覆盖身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范、资源控制等安全控制点，并明确各配置项的取值范围、推荐值及安全影响说明。

4.2.3 基线清单应按终端安全域进行分类汇总，明确各基线条目的适用范围、优先级、依赖关系及例外处理流程，便于执行和管理。

4.2.4 基线制定应遵循最小权限原则和默认拒绝原则，确保安全性与可用性的平衡。

4.2.5 基线制定完成后应经过专家评审和安全测试，确保其科学性、合理性和可操作性，并根据技术发展和业务变化定期（至少每季度）更新，版本号明确且变更记录可查。

4.3 基线检查

4.3.1 终端开机运行状态下，应能按照定制的配置基线要求，对系统配置数据进行自动化或半自动化检查，检查覆盖率应达到 100%。

4.3.2 检查功能应支持策略导入、合规性判定及结果输出，其中合规性判定需明确符合项、不符合项、未检查项及风险等级，并支持偏差统计和趋势分析。

4.3.3 检查过程应记录检查时间、检查工具、检查人员、检查结果等日志信息，并支持结果导出和报表生成。

4.3.4 检查结果应形成详细报告，包含具体配置项的实际值与基线要求的对比、偏差分析、风险提示及整改建议，报告格式应支持 PDF、WORD 等常见格式。

4.3.5 检查频率应至少每月一次，对于高风险配置项应提高检查频率至每周一次，检查结果应存档备查至少一年。

4.4 基线加固

4.4.1 针对基线检查发现的不符合项，应依据预设的加固方案进行修正，加固操作应记录操作人、操作时间、操作内容、操作结果等详细信息。

4.4.2 加固方式应根据终端管理模式选择自动化脚本执行或人工手动操作，确保加固过程可审计、可回滚，且对业务影响最小化。

4.4.3 加固操作前应进行影响评估和备份，确保系统异常时可快速恢复。

4.4.4 加固完成后应重新进行基线检查，验证加固效果，直至不符合项全部整改到位，并生成加固验证报告。

4.4.5 应建立加固跟踪机制，对未及时整改的不符合项进行告警和升级处理，确保整改时效性。

5 主动防御防护技术要求

5.1 身份鉴别

5.1.1 应对操作系统用户进行身份鉴别，可采用账户口令、密码技术、生物技术等一种或多种组合方式。

5.1.2 若采用账户口令方式，应禁用空口令账户登录系统，明确口令长度不低于 8 位，且至少包含数字、小写字母、大写字母、特殊字符 4 类中的 3 类；用户设置或修改口令时，系统应强制校验并提示合规性要求。

5.1.3 应能配置身份鉴别失败的最大次数（建议不超过 5 次），达到限制次数后，应采取账户锁定（锁定时间可配置）或其他限制登录的安全措施。

5.1.4 口令有效期不超过 90 天，且禁止重复使用近期已使用的口令（建议至少限制前 5 次）。

5.1.5 终端存储的口令信息应采用符合 GB/T 37092—2018 中“安全一级”及以上要求的加密算法进行保护，禁止明文存储。

5.2 账号权限

5.2.1 应依据用户角色实施最小权限原则，确保用户仅能访问完成工作所需的资源和功能，禁止超权限分配。

5.2.2 应限制超级用户（如 root）的远程登录权限，确需远程操作时，应采用加密通道并严格限制访问来源；普通用户如需执行高权限操作，应通过临时提权机制实现。

5.2.3 临时账号的创建应明确有效期，任务完成后应立即禁用或删除，且权限应随账号失效自动清除。

5.2.4 应实行权限分离策略，将系统管理、业务操作等权限分配给不同用户，避免单一用户拥有过多敏感权限。

5.2.5 应每季度至少进行一次账号权限审计，清理无效账号、闲置账号及高风险权限配置，并记录审计结果。

5.2.6 应记录所有账号权限变更操作（包括创建、删除、权限调整等），审计日志应包含操作人、操作时间、操作内容及结果。

5.3 访问控制

5.3.1 本地访问控制

5.3.1.1 应配置系统关键文件（如配置文件、日志文件）和目录的访问权限，仅允许授权用户进行读取、修改或执行操作，新建文件或目录时应自动应用预设的默认权限（建议限制非授权用户的写入权限）。

5.3.1.2 应通过本地防火墙等机制实施网络访问控制，限制对终端关键服务的访问，仅允许特定 IP 地址或端口的连接请求。

5.3.2 远程访问控制

5.3.2.1 远程访问需采用 TLS 1.2 及以上版本加密，禁止使用明文传输协议（如 Telnet）。

5.3.2.2 应限制远程登录的用户范围和来源主机，仅允许授权用户从可信 IP 地址发起连接，未授权连接应实时拒绝并记录。

5.3.2.3 应设置远程会话超时机制（建议不超过 30 分钟），超时后自动断开连接；重新操作时需重新进行身份鉴别。

5.3.2.4 应限制远程登录的最大认证尝试次数（建议不超过 3 次），超过次数后自动断开连接。

5.3.2.5 应限制每个账户的最大并发远程会话数（建议不超过 2 个），超过限制时应阻止新会话建立或断开最早的会话。

5.3.2.6 应启用远程访问审计功能，记录登录、注销、命令执行等操作，日志应包含用户标识、IP 地址、操作时间及内容。

5.4 端口防护

5.4.1 应定期（建议每周至少一次）扫描系统开放端口，识别非必要端口和高危端口（如 3389、23 等），并及时禁用或限制访问。

5.4.2 应对敏感服务端口（如数据库端口、管理端口）配置访问控制策略，仅允许授权 IP 地址和用户访问，未授权访问应被阻断并告警。

5.4.3 默认状态下应关闭所有非必要端口，仅保留业务必需的端口，且端口用途应在系统文档中明示。

5.5 系统服务

5.5.1 应合理配置系统内核参数，增强网络协议栈安全性（如启用 SYN Flood 防护、限制 ICMP 报文等）。

5.5.2 应禁用所有非必要的系统服务（如 Telnet 服务、FTP 服务等），仅保留维持终端基本功能和业务运行的服务。

5.5.3 应建立系统服务漏洞扫描机制，每月至少进行一次扫描，及时发现并修复服务漏洞；扫描结果及修复记录应存档。

5.5.4 系统服务的启动项应严格管控，禁止未授权服务随系统启动；服务运行权限应遵循最小权限原则，避免使用高权限账户运行服务。

6 主动防御防护技术测试方法

6.1 身份鉴别测试

6.1.1 测试内容

测试内容如下：

1）尝试使用空口令登录，验证是否被拒绝；

2）检查口令长度和复杂度是否符合要求；

3）测试鉴别失败次数限制及锁定功能；

4）验证口令有效期和历史重用限制；

5）检查口令存储是否加密；

6）测试多种鉴别方式的组合应用。

6.1.2 预期结果

预期结果如下：

1）空口令登录被拒绝；

2）口令长度≥8 位且包含 3 类及以上字符；

3）失败次数达限时账户被锁定（锁定时间可配置）；

4）口令超期提醒且禁止重用近期口令（至少前 5 次）；

5）口令存储无明文，加密算法符合 GB/T 37092—2018 要求；

6）多种鉴别方式组合应用时，安全性得到增强。

6.1.3 结果判定

全部满足预期结果为符合，否则为不符合。

6.2 账号权限测试

6.2.1 测试内容

测试内容如下：

1）检查普通用户是否能访问超权限资源；

2）验证 root 用户远程登录是否被限制；

3）检查临时账号是否按时失效；

4）测试权限分离和定期审计机制；

5）检查权限变更日志是否完整；

6）验证最小权限原则的实施情况。

6.2.2 预期结果

预期结果如下：

1）普通用户无超权限访问；

2）root 用户远程登录被限制，确需远程操作时采用加密通道和访问限制；

3）临时账号按时失效，权限随账号失效自动清除；

4）权限分离明确，每季度至少进行一次权限审计；

5）权限变更日志包含操作人、时间、内容及结果等信息；

6）所有用户权限遵循最小权限原则。

6.2.3 结果判定

全部满足预期结果为符合，否则为不符合。

6.3 访问控制测试

6.3.1 本地访问控制测试

6.3.1.1 测试内容

测试内容如下：

1）检查关键文件权限配置是否合理；

2）验证本地防火墙是否限制非授权访问；

3）测试新建文件和目录的默认权限；

4）检查访问控制策略的有效性。

6.3.1.2 预期结果

预期结果如下：

1）关键文件仅授权用户可修改；

2）非授权 IP 地址无法访问关键服务；

3）新建文件和目录自动应用预设默认权限（非授权用户无写权限）；

4）访问控制策略有效，未出现越权访问。

6.3.1.3 结果判定

全部满足预期结果为符合，否则为不符合。

6.3.2 远程访问控制测试

6.3.2.1 测试内容

测试内容如下：

1）检查远程访问是否使用加密协议；

2）验证是否限制用户和来源主机；

3）测试会话超时、并发数限制功能；

4）检查远程操作审计日志；

5）测试认证尝试次数限制功能。

6.3.2.2 预期结果

预期结果如下：

1）禁用明文协议，使用 SSH/TLS 等加密方式；

2）非授权用户或主机被拒绝访问；

3）超时后自动断开，并发数不超过限制；

4）审计日志记录完整，包含用户标识、IP 地址、操作时间及内容；

5）认证尝试次数超过限制后自动断开连接。

6.3.2.3 结果判定

全部满足预期结果为符合，否则为不符合。

6.4 端口防护测试

6.4.1 测试内容

测试内容如下：

1）检查是否定期扫描端口及结果记录；

2）验证敏感端口是否限制访问；

3）检查非必要端口是否关闭；

4）测试端口访问控制策略的有效性；

5）验证高危端口的识别和处理。

6.4.2 预期结果

预期结果如下：

1）每周至少一次端口扫描，记录完整；

2）敏感端口仅授权 IP 和用户可访问；

3）非必要端口默认关闭；

4）端口访问控制策略有效，未授权访问被阻断；

5）高危端口被及时识别并处理（禁用或限制访问）。

6.4.3 结果判定

全部满足预期结果为符合，否则为不符合。

6.5 系统服务测试

6.5.1 测试内容

测试内容如下：

1）检查内核参数配置是否增强安全性；

2）验证非必要服务是否禁用；

3）测试漏洞扫描机制及修复记录；

4）检查服务启动项和运行权限；

5）测试服务漏洞的修复时效性。

6.5.2 预期结果

预期结果如下：

1）内核参数配置符合安全要求（如启用 SYN Flood 防护）；

2）非必要服务已禁用；

3）每月至少一次漏洞扫描，修复记录完整；

4）启动项无未授权服务，运行权限最小化；

5）发现的服务漏洞在规定时限内修复。

6.5.3 结果判定

全部满足预期结果为符合，否则为不符合。