中共合肥市委平安合肥建设领导小组办公室文件

合平安办〔2021〕10号

关于印发《合肥市智慧平安小区网络安全指导意见》的通知

各县（市）区、开发区平安办，市住宅小区安全防范设施建设和管理工作领导小组成员单位:

为推进和规范我市智慧平安小区建设，有效保障智慧平安小区网络运行安全和信息安全，根据《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》《信息安全等级保护管理办法》等法律法规要求，市委平安办、市公安局制定了《合肥市智慧平安小区网络安全指导意见》，现印发给你们，请对照要求抓好贯彻落实。

附件：合肥市智慧平安小区网络安全指导意见

中共合肥市委平安合肥建设领导小组办公室

2021年3月15日

合肥市智慧平安小区网络安全指导意见

2021 年 3 月

目 录

一、指导思想

为贯彻落实《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》《信息安全等级保护管理办法》等法律法规要求，严格落实网络安全等级保护制度，规范和促进合肥市智慧平安小区网络安全建设，有效保障智慧平安小区网络运行安全和信息安全，现制定《智慧平安小区网络安全指导意见》（以下简称《指导意见》），为全市智慧平安小区网络安全建设和管理工作提供指导和依据。

二、总体目标

建立合肥市智慧平安小区网络安全监督管理机制，完善安全管理制度和技术防护措施，切实提高网络安全防护能力、隐患发现能力、应急处置能力，为智慧平安小区信息化健康发展提供安全保障。主要包括：完成已运营（运行）或新建的第二级以上（含第二级）信息系统的定级、备案、安全建设整改和等级测评等工作；建立完善的智慧平安小区网络安全等级保护政策标准体系，常态化开展网络安全技术检测、安全评估、监督检查等工作。

三、主要依据

《指导意见》的制定参考或引用了以下法律法规、政策文件和技术规范：

（一）法律法规和政策文件

1.《中华人民共和国网络安全法》

2.《中华人民共和国民法典》

3.《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）

4.《信息安全等级保护管理办法》(公通字〔2007〕43 号)

5.《智慧社区建设指南（试行）》（中华人民共和国住房和城乡建设部办公厅）

6.《关于加强政法机关信息技术产品使用安全管理的意见》（中政委〔2014〕34 号）

7.《全省智慧社区建设试点工作方案（2018—2020）》（安徽省人民政府办公厅）

8.《合肥市人民政府办公厅关于印发智慧合肥建设“十三五”规划纲要的通知》（合政办〔2016〕65 号）

9.《合肥市智慧平安小区建设标准规范指南（试行）》（合肥市住宅小区安全防范设施建设和管理工作领导小组办公室）

10.《合肥市立体化信息化社会治安防控体系建设（2018-2020 年）》（合办〔2018〕17 号）

（二）技术规范

1.GB 17859-1999《计算机信息系统安全保护等级划分准则》

2.GB 35114-2017《公共安全视频监控联网信息安全技术要求》

3.GB/T 35273-2020《信息安全技术 个人信息安全规范》

4.GB/T 25058-2019《信息安全技术 网络安全等级保护实施指南》

5.GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》

6.GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

7.GB/T 25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》

8.GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》

9.GB/T 28449-2018《信息安全技术 网络安全等级保护测评过程指南》

10.GB/T 37024-2018《信息安全技术 物联网感知层网关安全技术要求》

11.GB/T 37025-2018《信息安全技术 物联网数据传输安全技术要求》

12.GB/T 37093-2018《信息安全技术 物联网感知层接入通信网的安全要求》

13.GB/T 25000.10-2016《系统与软件工程 系统与软件质量要求和评价(SQuaRE) 第 10 部分:系统与软件质量模型》

14. GB/T 25000.51-2016《系统与软件工程系统与软件质量要求和评价(SQuaRE) 第 51 部分:就绪可用软件产品(RUSP)的质量要求和测试细则》

四、整体架构

合肥市智慧平安小区网络部署方式主要包括云平台、小区数据接入终端（以下简称“盒子”）、云平台+盒子、本地部署等。其中，云平台包括私有云（如政务云、企业云等）、公有云（如运营商云、阿里云、华为云等）、混合云等。针对不同的部署方式应提供相应等级的安全防护措施，按照“安全合规、重点防护”的原则，全面保障智慧平安小区网络安全。安全防护体系包括智慧平安小区管理系统及运行载体（如云平台、盒子、本地部署服务器等）安全防护、物业侧安全防护两部分，均应参照《指导意见》开展等级测评、技术检测、安全评估等工作。

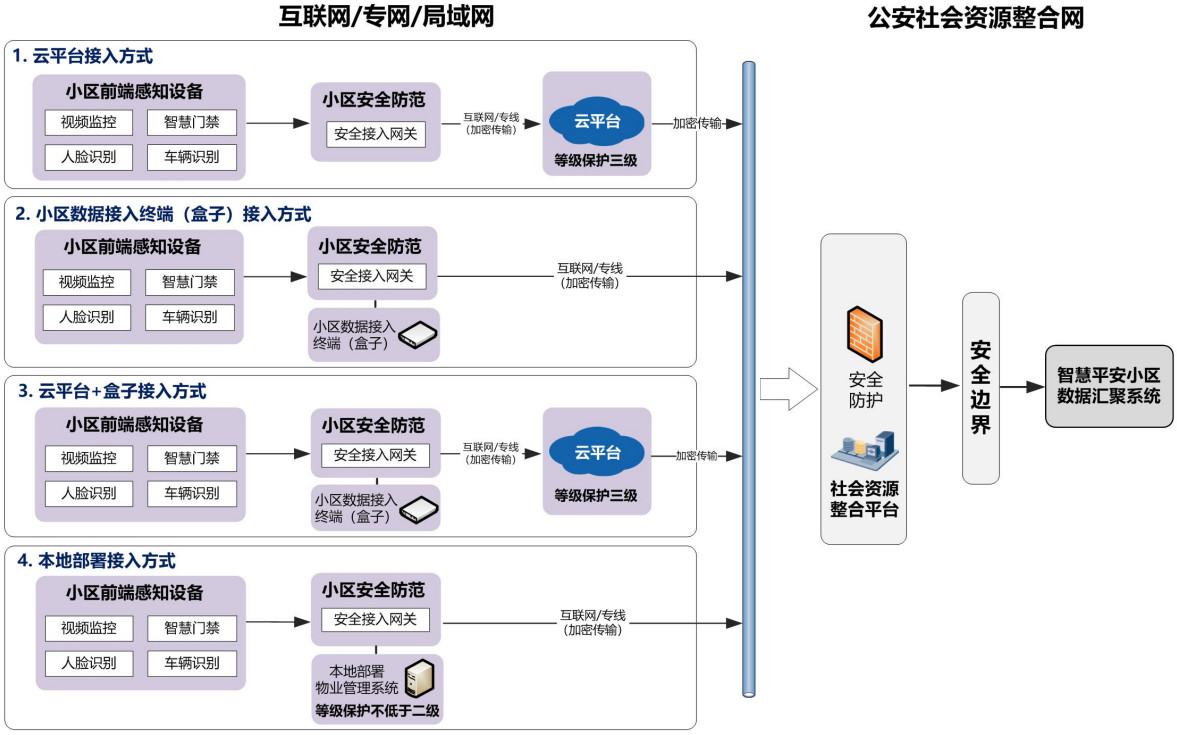

图. 合肥市智慧平安小区安全接入架构图

五、安全要求

（一）系统侧安全要求

系统侧安全包括边界防护、应用程序安全、个人信息保护等。

1.边界防护

（1）边界隔离：重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。可部署安全接入网关、防火墙、网闸等具备可靠技术隔离手段的设备，或采用其他可靠的技术措施实现专用网络的逻辑隔离。

（2）传输保护：小区采集数据上报至公安社会资源整合网应采用校验技术或密码技术保证通信过程中数据的完整性、保密性。可在通信过程中配备SSLVPN网关、IPSecVPN网关、安全接入网关或其他具有相同功能的设备。

2.应用程序安全

（1）身份鉴别：应禁用“超级管理员”权限，重命名或删除默认帐户，修改默认帐户的默认口令。

（2）恶意代码防范：应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库，实现对恶意代码的有效防范。

（3）数据存储加密：应具备对关键数据加密存储能力，防止来自外部攻击或内部高权限用户的数据窃取以及由于磁盘、磁带等存储介质失窃引起的数据泄露行为。

（4）安全审计：应具备对系统关键日志，如登录日志、操作日志、运行日志等的存储功能，审计记录应留存6个月以上，日志应采用加密方式存储，并遵循访问权限最小化原则。

3.个人信息保护

（1）收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

（2）不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理保存的个人信息。

（3）管理系统仅限存储姓名、采集图片（特征码）、手机号码、车牌号码、身份证号（脱敏处理）、家庭住址；出入记录、抓拍图片等个人信息不得保存，应在上传至公安社会资源整合网后及时删除。数据采集和上传终端不得保存个人信息。个人信息查看展示时应采取脱敏等去标识化措施。

（4）不得泄露、篡改、损毁收集的个人信息；未经被收集者同意，不得向他人提供个人信息。

（5）应当采取技术措施和其他必要措施，确保收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

（6）应提供用户删除或更正个人信息的相关措施或手段。

（二）物业侧安全要求

物业侧安全包括应用程序安全、个人信息保护、感知终端安全、管理终端安全、安全管理制度等。

1.应用程序安全

物业侧应用程序包括Web应用、APP应用、微信小程序等。

（1）物业管理终端管理员登录系统应进行身份标识和鉴别，确保在系统整个生存周期用户名的唯一性，避免共享帐户存在。

（2）身份鉴别应满足口令复杂度要求，且满足双因素认证。

（3）应启用登录失败处理功能，登录失败后采取结束会话、限制非法登录次数和自动退出等措施。

（4）当进行远程管理时，应采取SSH、HTTPS等加密通信协议防止鉴别信息在网络传输过程中被窃听。

（5）应启用安全审计功能，审计覆盖到每个远程连接管理用户，对重要的用户行为和重要安全事件进行审计。

2.个人信息保护

同系统侧“个人信息保护”安全要求。

3.感知终端安全

（1）应提供感知终端设备认证能力，保证只有授权设备可以接入，防止前端仿冒、替换等非法接入行为。可在小区侧部署安全接入网关，或采取其他具备准入控制能力的措施。

（2）应能够限制与设备通信的地址，并检测来自非法地址的攻击行为（非法攻击、恶意扫描、漏洞攻击等）。可在小区侧部署安全接入网关，或采取其他具备入侵防范能力的措施。

（3）若只采用“用户名+口令”的鉴别方式进行身份鉴别，则应使用具有一定复杂度的用户口令（用户口令须由大小写英文

字母、数字、特殊字符3种以上组成、长度不少于8位），每90天更新一次。

（4）应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施，连续5次登录失败至少锁定10分钟。

（5）应保证只有授权的用户可以对设备上的软件应用进行配置或变更。

4.管理终端安全

（1）应禁用访客帐户，修改默认帐户的口令，并设置满足复杂度要求的口令。

（2）应为每一位操作员分配专用的帐户，避免共享帐户存在。

（3）应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施，连续5次登录失败至少锁定10分钟。

（4）应采用免受恶意代码攻击的技术措施。

（5）应采用技术措施，保证管理终端操作系统高风险漏洞得到及时修复。

5.安全管理制度

小区物业公司或实际承担小区物业管理职能的单位应落实以下安全管理制度:

（1）应成立网络安全工作组织，负责人由单位主要负责人

担任。

（2）应制定符合实际工作需要的网络安全管理制度，并定期评审、更新，且做好必要的版本控制。

（3）应对系统操作员等关键岗位人员进行网络安全意识和操作技能培训，并进行必要的考核。

（4）应与系统操作员等关键岗位人员签订保密协议或保密承诺书，不得泄露用户个人信息。

（5）应做好人员招聘、录用、使用、离岗等人员全生命周期管理工作，尤其是离岗时应签署离岗保密协议和承诺书，收回钥匙、key 并注销其相关帐户等。

（三）盒子安全要求

盒子安全包括网络安全、应用程序安全等。

1.网络安全

（1）边界防护：盒子与其他网络区域之间应采取可靠的技术隔离手段。可部署安全接入网关、防火墙、网闸等具备可靠技术隔离手段的设备，或采用其他可靠的技术措施实现专用网络的逻辑隔离。

（2）感知设备安全接入：应提供前端感知设备认证能力，保证只有授权的设备可以接入，防止前端仿冒、替换等非法接入行为。可在小区侧部署安全接入网关，或采取其他具备准入控制能力的措施。

（3）攻击防范：应能够限制与设备通信的地址，并检测来

自非法地址的攻击行为（非法攻击、恶意扫描、漏洞攻击等）。可在小区侧部署安全接入网关，或采取其他具备入侵防范能力的措施。

（4）传输保护：应至少采用校验技术保证通信过程中数据的完整性；根据需要可采用密码技术保证通信过程中数据的完整性，密码算法应符合国家密码管理局相关规范要求。

2.应用程序安全

（1）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。

（2）应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施，连续5次登录失败至少锁定10分钟。

（3）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

（4）应重命名或删除默认帐户，修改默认帐户的默认口令。

（5）应及时删除或停用多余的、过期的帐户，避免共享帐户的存在。

（6）应授予管理用户所需的最小权限，实现管理用户的权限分离。

（7）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的

信息；应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；应对审计进程进行保护，防止未经授权的中断。

（8）应关闭不需要的系统服务、默认共享和高危端口。

（9）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。

（10）应启用操作系统防火墙，配置合理的访问控制策略，实现入侵防护功能。

（11）应采用免受恶意代码攻击的技术措施及时识别病毒攻击行为，并将其有效阻断。

（12）应采用校验技术或密码技术保证重要数据在传输和存储过程中的完整性、保密性。

六、建设规范

合肥市智慧平安小区网络安全建设应按照以下要求开展:

（一）云平台方式

建设方自行建设的私有云平台（如政务云、企业云等）或租用的公有云服务商（如运营商云、阿里云、华为云等）服务，智慧平安小区管理系统部署在云平台上，统一收集小区感知前端数据，并上报至公安社会资源整合网。

网络安全建设应按照：1.云平台按照安全保护等级第三级要求开展测评并达到“中”以上等次，同时满足“**附录A：系统增强项安全检查要求**”；2.物业侧安全满足“**附录B：物业侧安全**

检查要求”。（建设规范详见附件 1）

（二）盒子方式

建设方在小区部署盒子，智慧平安小区管理系统运行于盒子内，统一收集小区感知前端数据，并上报至公安社会资源整合网。

网络安全建设应按照：1.盒子安全满足“**附录 C ： 盒子安全检查要求**”，并通过公安部第一研究所、公安部第三研究所或安徽省电子产品监督检验所等具有资质的机构检测；2.物业侧安全满足“**附录 B ： 物业侧安全检查要求**”。（建设规范详见附件 2）

（三）云平台+盒子方式

建设方自行建设的私有云平台（如政务云、企业云等）或租用的公有云服务商（如运营商云、阿里云、华为云等）服务，智慧平安小区管理系统运行于云平台上，同时通过部署在小区的盒子统一收集小区感知前端数据，上传至云平台后再上报至公安社会资源整合网。

网络安全建设应按照：1.云平台按照安全保护等级第三级要求开展测评并达到“中”以上等次，同时满足“**附录 A ： 系统增强项安全检查要求**”；2.盒子安全满足“**附录 C ： 盒子安全检查要求**”，并通过公安部第一研究所、公安部第三研究所或安徽省电子产品监督检验所等具有资质的机构检测；3.物业侧安全满足“**附录 B ： 物业侧安全检查要求**”。（建设规范详见附件 3）

（四）本地部署方式

建设方在本地部署智慧平安小区管理系统，统一收集小区感

知前端数据，并上报至公安社会资源整合网。

网络安全建设应按照：1. 本地部署系统按照安全保护等级不低于第二级要求开展测评，并达到“中”以上等次,同时满足**“附录 A ： 系统增强项安全检查要求”**；2.物业侧安全满足“**附录 B: 物业侧安全检查要求**”。（建设规范详见附件 4）

（五）其他方式

建设方通过其他方式建设的，应根据实际情况按照安全要求开展网络安全建设。

附件：1.云平台方式安全建设规范

2.盒子方式安全建设规范

3.云平台+盒子方式安全建设规范

4.本地部署方式安全建设规范

附件 1：

云平台方式安全建设规范

云平台方式安全包括云平台和物业侧两部分。

一、云平台安全要求

云平台应按照安全保护等级第三级要求开展测评并达到“中”以上等次。建设方从网络安全等级保护网(www.djbh.net)的全国等级保护测评机构推荐目录中选择具有《网络安全等级保护测评机构推荐证书》的测评机构开展等级测评，测评结论不符合的应进行整改。同时，应委托测评机构按照**“附录 A：系统增强项安全检查要求”**，开展增强项安全检测，检测不合格的应进行整改。

二、物业侧安全要求

物业侧应按照**“附录 B：物业侧安全检查要求”**进行安全评估，可通过第三方评估和自评估两种方式。对于第三方评估方式，公安机关将进行抽查；对于自评估方式，公安机关将进行检查。抽查或检查不合格的应针对不符合项进行整改。

三、检查结果判定依据

附录的检查结果判定依据如下:

1.单项检查结果分为“符合”“部分符合”“不符合”“不适用”;

2.标“*”项，任一项检查结果为“不符合”或“部分符合”，

则不合格;

3. 整体检查结果不低于“中”以上等次。

四、流程图

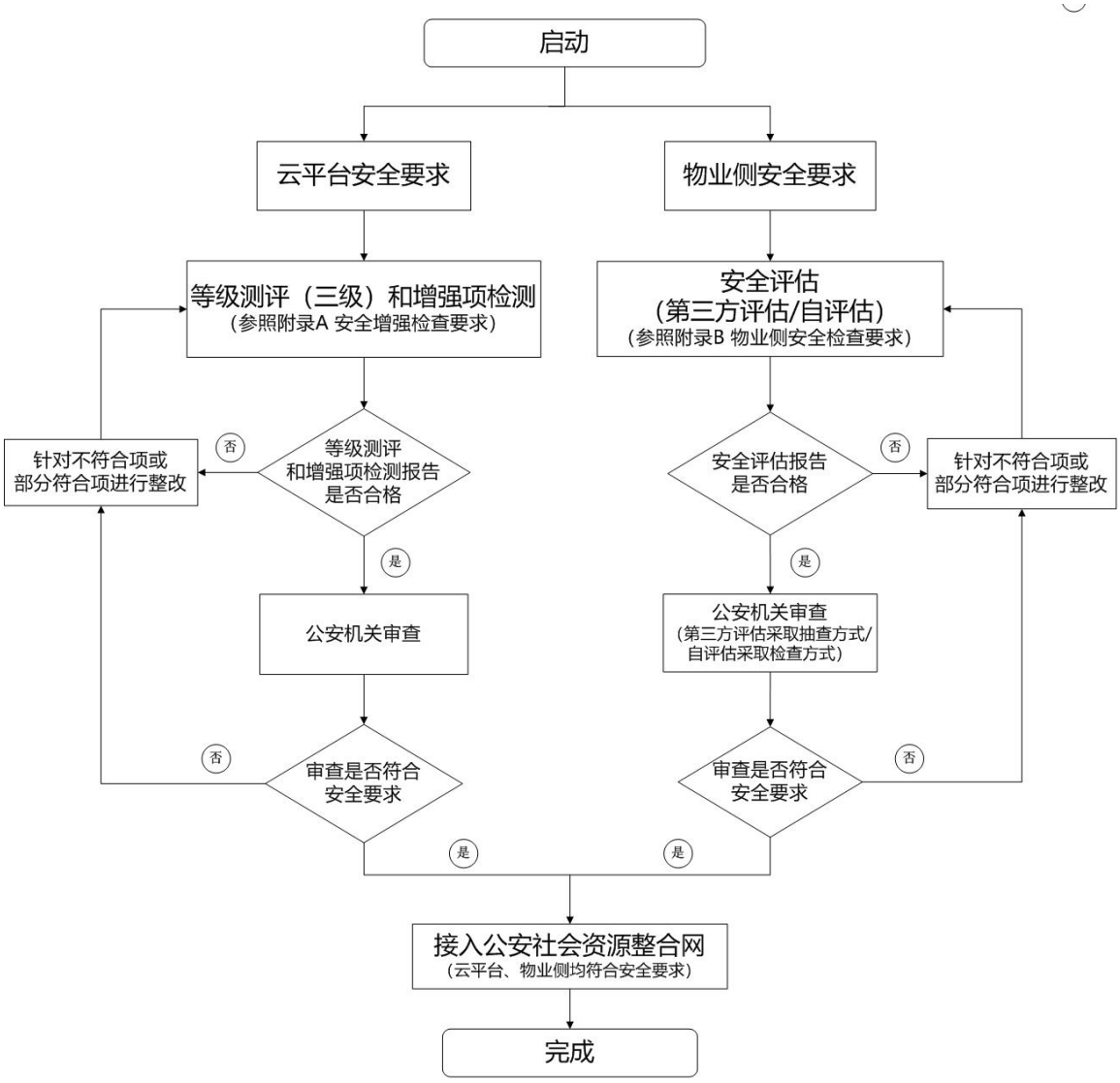

图1. 云平台方式接入流程图

附件 2：

盒子方式安全建设规范

盒子方式安全包括盒子和物业侧两部分。

一、盒子安全要求

盒子安全应满足**“附录 C：盒子安全检查要求”**。可通过第三方评估和自评估两种方式。对于第三方评估方式，公安机关将进行抽查；对于自评估方式，公安机关将进行检查。抽查或检查不合格的应针对不符合项进行整改。同时，盒子应通过公安部第一研究所、公安部第三研究所或安徽省电子产品监督检验所等具有资质的机构检测，并提供检测报告。

二、物业侧安全要求

物业侧应按照**“附录 B：物业侧安全检查要求”**进行安全评估，可通过第三方评估和自评估两种方式。对于第三方评估方式，公安机关将进行抽查；对于自评估方式，公安机关将进行检查。抽查或检查不合格的应针对不符合项进行整改。

三、检查结果判定依据

附录的检查结果判定依据如下：

1.单项检查结果分为“符合”“部分符合”“不符合”“不适用”；

2.标“*”项，任一项检查结果为“不符合”或“部分符合”，则不合格；

3. 整体检查结果不低于“中”以上等次。

四、流程图

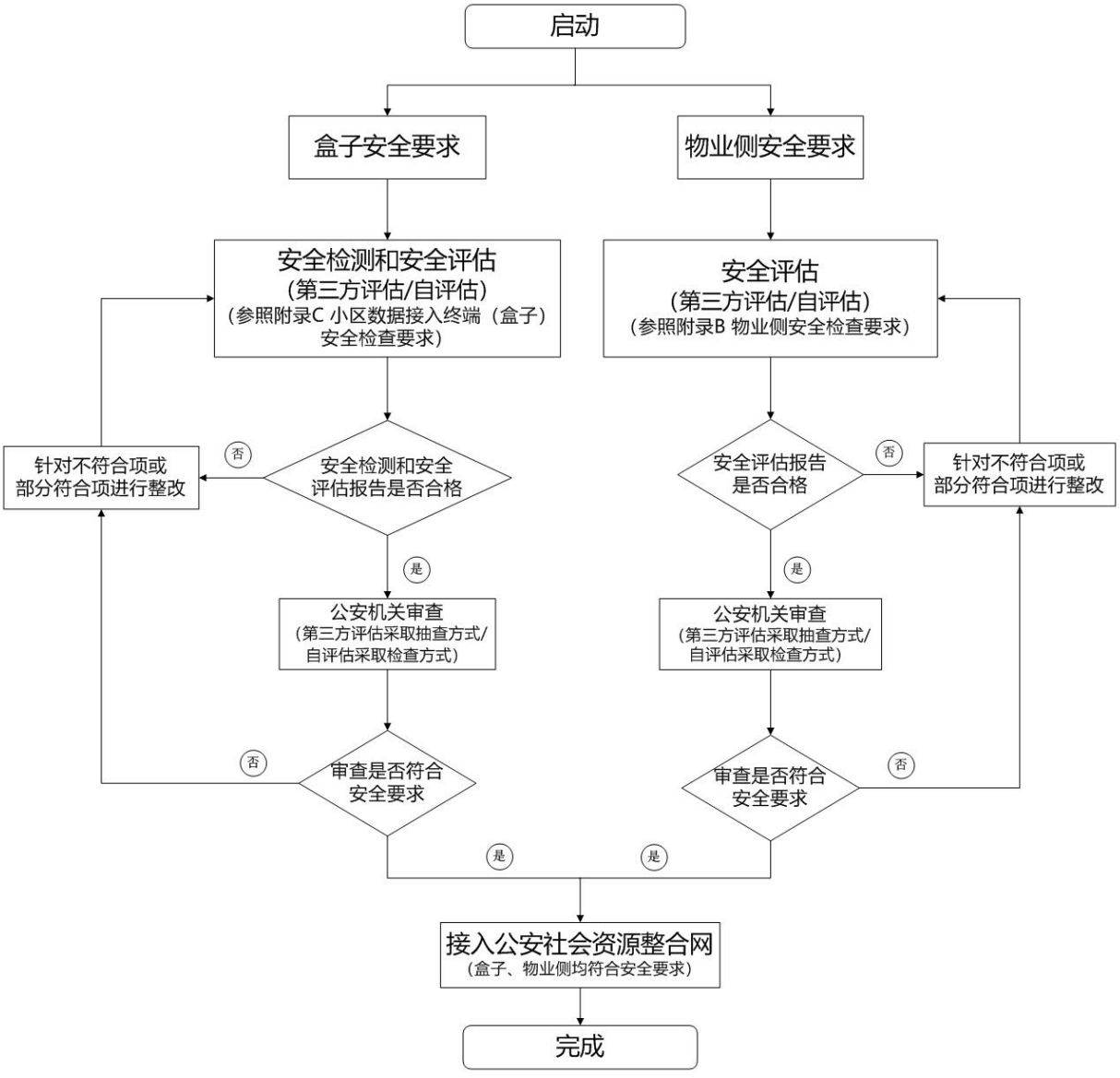

图2. 小区数据接入终端（盒子）方式接入流程图

附件 3：

云平台+盒子方式安全建设规范

云平台+盒子方式安全包括云平台、盒子和物业侧三部分。

一、云平台安全要求

云平台按照安全保护等级第三级要求开展测评，并达到“中”以上等次。建设方从网络安全等级保护网(www.djbh.net)的全国等级保护测评机构推荐目录中选择具有《网络安全等级保护测评机构推荐证书》的测评机构开展等级测评，测评结论不符合的应进行整改。同时，应委托测评机构按照**“附录 A：系统增强项安全检查要求”**，开展增强项安全检测，检测不合格的应进行整改。

二、盒子安全要求

盒子安全应满足**“附录 C ：盒子安全检查要求”**。可通过第三方评估和自评估两种方式。对于第三方评估方式，公安机关将进行抽查；对于自评估方式，公安机关将进行检查。抽查或检查不合格的应针对不符合项进行整改。同时，盒子应通过公安部第一研究所、公安部第三研究所或安徽省电子产品监督检验所等具有资质的机构检测，并提供检测报告。

三、物业侧安全要求

物业侧应按照**“附录 B：物业侧安全检查要求”**进行安全评估，可通过第三方评估和自评估两种方式。对于第三方评估方式，公安机关将进行抽查；对于自评估方式，公安机关将进行检查。

抽查或检查不合格的应针对不符合项进行整改。

四、检查结果判定依据

附录的检查结果判定依据如下:

1. 单项检查结果分为“符合”“部分符合”“不符合”“不适用”;

2. 标“*”项，任一项检查结果为“不符合”或“部分符合”，则不合格;

3. 整体检查结果不低于“中”以上等次。

五、流程图

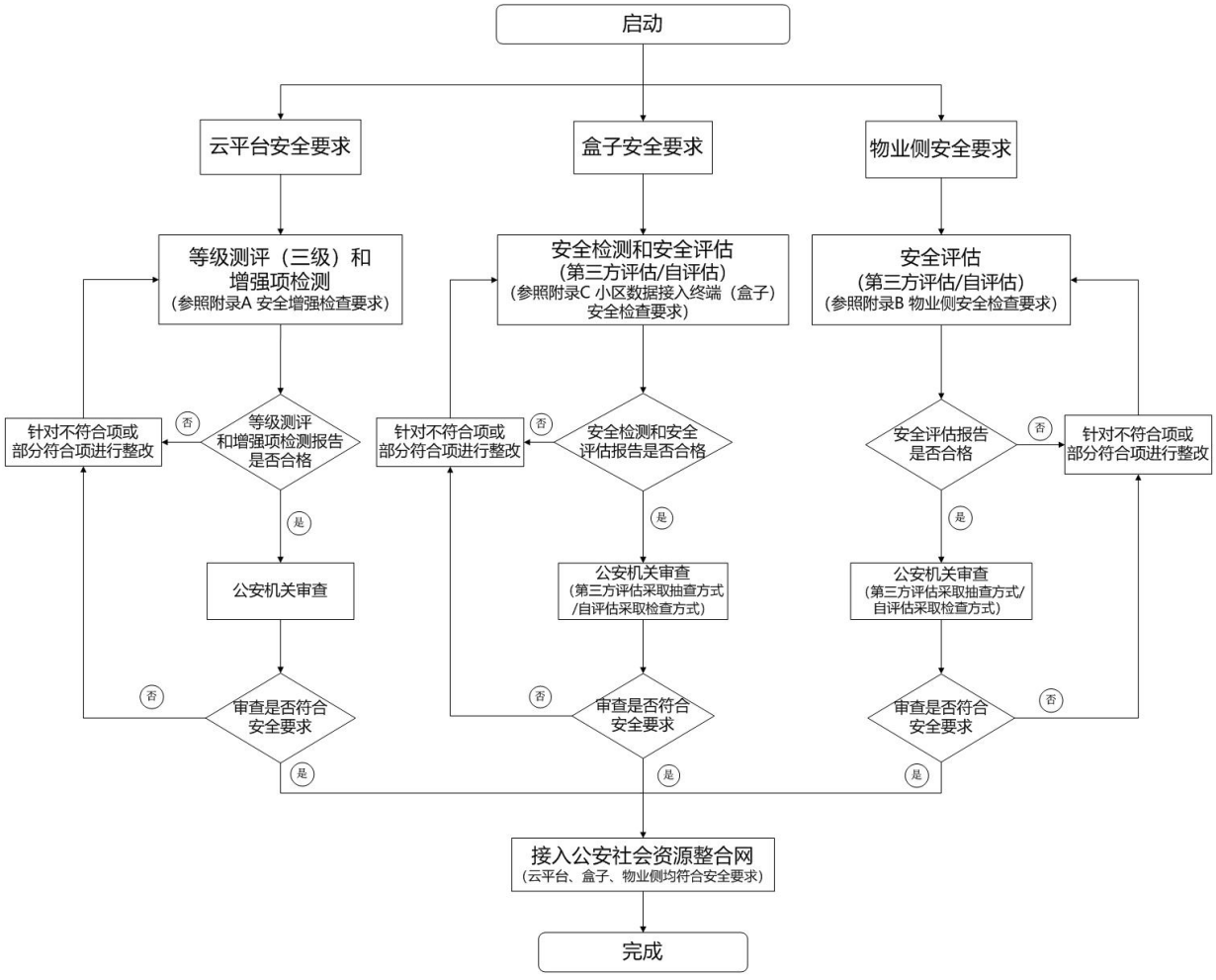

图3. 云平台（盒子）方式接入流程图

附件 4：

本地部署方式安全建设规范

本地部署方式安全包括本地部署系统和物业侧两部分。

一、本地部署系统安全要求

本地部署系统按照安全保护等级不低于第二级要求开展测评，并达到“中”以上等次。建设方从网络安全等级保护网(www.djbh.net)的全国等级保护测评机构推荐目录中选择具有《网络安全等级保护测评机构推荐证书》的测评机构开展等级测评，测评结论不符合的应进行整改。同时，应委托测评机构按照**“附录 A：系统增强项安全检查要求”**，开展增强项安全检测，检测不合格的要求进行整改。

二、物业侧安全要求

物业侧应按照**“附录 B：物业侧安全检查要求”**进行安全评估，可通过第三方评估和自评估两种方式。对于第三方评估方式，公安机关将进行抽查；对于自评估方式，公安机关将进行检查。抽查或检查不合格的应针对不符合项进行整改。

三、检查结果判定依据

附录的检查结果判定依据如下：

1.单项检查结果分为“符合”“部分符合”“不符合”“不适用”；

2.标“*”项，任一项检查结果为“不符合”或“部分符合”，

则不合格;

3. 整体检查结果不低于“中”以上等次。

四、流程图

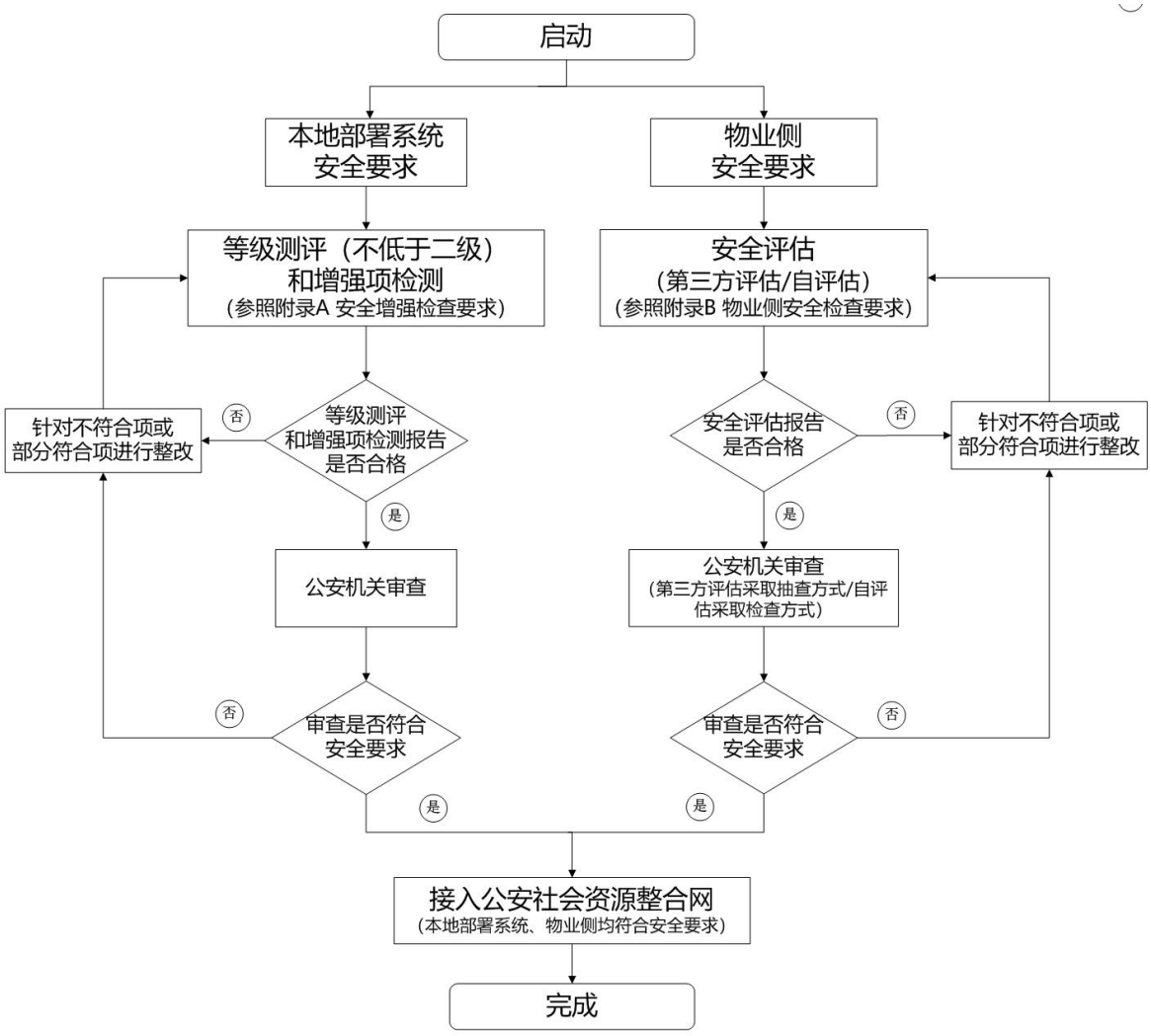

图4. 本地部署系统方式接入流程图

附录 A：增强项安全检查要求

序号	要求项目	要求子项	要求小项	不符合判例	补偿措施	检查结论
1	安全通信网络	通信传输	应至少采用校验技术保证通信过程中数据的完整性；根据需要可采用密码技术保证通信过程中数据的完整性，密码算法应符合国家密码管理局相关规范要求。	满足条件（任意条件）： 1.在通信过程中未配备 SSL 网关、IPSecVPN、SSLVPN 或其他具有相同功能的设备； 2.未使用加密通信协议，如 https 协议； 3.未采用 MD5、RSA、3DES 或国密算法等进行通信加密。	无。	
2	安全区域边界	边界防护	***智慧平安小区平台重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。**	满足条件（任意条件）： 1.平台内部网络与外部网络边界（如互联网）未设置防火墙、网闸、安全网关等进行隔离； 2.平台内部网络与外部网络边界（如互联网）隔离设备配置策略不当。	无。	
3		安全审计	***审计记录留存 6 个月以上。**	满足条件（任意条件）： 1.审计记录未留存 6 个月； 2.审计记录存储空间不足以存储 6 个月。	无。	
4	安全计算	身份鉴别	**1.*应禁用“超级管理员”权限，重命名或删除默认帐户，修改**	满足条件（同时）： 1.未修改默认帐户的默认口令；	无。	

序号	要求项目	要求子项	要求小项	不符合判例	补偿措施	检查结论
	环境		**默认帐户的默认口令。**	2.可使用该默认口令帐户登录。		
5			2.应采用口令、密码技术、生物技术等鉴别技术对用户进行身份鉴别，对管理员、运维人员、重要业务系统（业务数据处理类）用户应采取两种或两种以上组合的方式进行鉴别。	满足条件: 重要核心设备、操作系统等未采用两种或两种以上鉴别技术对用户身份进行鉴别。例如仅使用用户名/口令方式进行身份验证。	1.如设备通过本地登录方式（非网络方式）维护，本地物理环境可控，可酌情降低风险等级，可视同部分符合; 2.采用两重用户名/口令认证措施（两重口令不同），例如身份认证服务器、堡垒机等手段，可视同部分符合; 3.如设备所在物理环境、网络环境安全可控，网络窃听、违规接入等隐患较小，口令策略和复杂度、长度符合要求的情况下，可视同部分符合。	
6			3.应为通信的计算设备、安全防护设备实现双向身份标识认证，保障传输的安全。	满足条件: 通信的计算设备、安全防护设备未实现双向身份认证，如基于数字证书的双向认证。	通过IP+MAC绑定的白名单，可视同符合。	
7		安全审计	***审计记录留存6个月以上。**	满足条件（任意条件）: 1.审计记录未留存6个月; 2.审计记录存储空间不足以存	无。	

序号	要求项目	要求子项	要求小项	不符合判例	补偿措施	检查结论
				储 6 个月。		
8		入侵防范	应严格对 U 盘、移动光驱等外来介质设备的管控，并对各类硬件设备的外接存储接口进行限制或移除。	满足条件: 未对 U 盘、移动光驱等外来介质设备进行有效管控，且未对接口进行限制或移除。	无。	
9		恶意代码防范	***通过安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库，实现对恶意代码的有效防范。**	满足条件（任意条件）: 1.操作系统未安装杀毒软件; 2.操作系统安装的杀毒软件病毒库一个月以上未更新。	无。	
10		数据完整性	采用校验技术或密码技术保证重要数据在传输和存储过程中的完整性，包括但不限于鉴别数据和公民个人信息等;如使用密码技术，密码算法应符合国家密码管理局相关规范要求。	满足条件（任意条件）: 1.数据在传输和存储过程中无任何完整性保护措施; 2.未使用密码技术,如 MD5、DES、3DES、RSA 或国密算法等。	在数据完整性受到破坏时能够实施数据重传，并对存储的数据采取多重备份，可视同符合。	
11		数据保密性	1.采用校验技术或密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据和公民个人信息等;如使用密码技术，密码算法应符合国家密码管理局相关规范要求。	满足条件（任意条件）: 1.用户鉴别信息、公民敏感信息数据或重要业务数据等以明文方式在不可控网络中传输; 2.未采用加密通信协议，如 https 协议进行通信传输加密; 3.未使用密码技术,如 MD5、DES、3DES、RSA 或国密算法等。	如使用网络加密的技术确保数据在加密通道中传输，根据实际情况，可视同符合。	

序号	要求项目	要求子项	要求小项	不符合判例	补偿措施	检查结论
12			2.采用校验技术或密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据和公民个人信息等；如使用密码技术，密码算法应符合国家密码管理局相关规范要求。	满足条件（任意条件）： 1.应用软件未采取屏幕水印等技术； 2.应用软件未实现复制、粘贴功能最小化； 3.应用软件未限制敏感数据下载。	如采取区域隔离、部署数据库防火墙、数据防泄露产品等安全防护措施的，可通过分析造成信息泄露的难度和影响程度，可视同部分符合。	
13			3.应用软件（包括但不限于web端、客户端、APP、小程序等）应提供防截屏、防复制、防下载等功能。	满足条件（任意条件）： 1.可以截图或截屏。 2.可以复制、粘贴。 3.可以下载。	无。	
14		数据备份恢复	1.应提供关键业务数据、服务支持数据等的本地数据备份与恢复功能，每周至少进行一次全备份，每天进行增量或差分备份。	满足条件: 应用系统未提供任何数据备份措施，一旦遭受数据破坏，无法进行数据恢复。	小区采集数据上传至公安社会资源整合网，可视同符合。	
15			2.应提供异地备份功能，利用通信网络将关键业务数据备份至备份场地；有条件的可提供异地实时备份功能。	满足条件: 系统无异地数据备份措施，或异地备份机制无法满足业务需要。	同城异地机房直线距离不低于为30公里，跨省市异地机房直线距离不低于100公里，如距离上不达标，可酌情降低风险等级，可视同部分符合。 小区采集数据上报至公安社会资源整合网，可视同符合。	

序号	要求项目	要求子项	要求小项	不符合判例	补偿措施	检查结论
16	安全管理	个人信息保护	**1.*应当遵循合法、正当、必要的原则收集、使用个人信息，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。人像图片上传应限制 JPG、PNG 等格式。**	满足条件（任意条件）： 1.在未授权情况下，采集、存储用户个人隐私信息，无论该信息是否是业务需要； 2.采集、保存法律法规、主管部门严令禁止采集、保存的用户隐私信息； 3.采集信息超过业务所需范围。	无。	
17			**2.*管理系统仅限存储姓名、采集图片（特征码）、手机号码、车牌号码、身份证号（脱敏处理）、家庭住址；出入记录、抓拍图片等个人信息不得保存，应在上传至公安社会资源整合网后及时删除。**	满足条件（任意条件）： 1.存储超出“姓名、采集图片（特征码）、手机号码、车牌号码、身份证号（脱敏处理）、家庭住址”之外的数据类型； 2.出入记录、抓拍图片等个人信息保存在本地，上传至公安社会资源整合网后未及时删除。	无。	
18			**3.*应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发**	满足条件（任意条件）： 1.未采取有效的技术措施和管理措施保障个人信息的完整性、保密性和可用性；	无。	

序号	要求项目	要求子项	要求小项	不符合判例	补偿措施	检查结论
			生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。	2.未规定相关事件发生时的处理方式，相关人员不知道如何报告。		
19			**4.*应禁止未经被收集者同意，向他人提供个人信息等行为。**	满足条件: 在进行数据分析、共享等操作时未采取相关措施获取被收集者授权。	无。	
20			**5.*应禁止窃取或者以其他非法方式获取个人信息，禁止非法出售或者非法向他人提供个人信息。**	满足条件（任意条件）: 1.未采用硬件、软件等措施避免个人信息被窃取; 2.未建立相关管理制度、未开展相关培训降低个人信息被窃取的风险。	无。	
21			**6.*应当提供用户删除或者更正个人信息的相关措施或手段。**	满足条件: 未提供更正、注销、删除等功能或服务。	无。	
22			**7.*应禁止未授权访问或非法使用用户个人信息。数据采集和上传终端不应保存个人信息数据。**	满足条件（任意条件）: 1.在未授权情况下将用户个人信息共享给其他公司、机构、个人（法律法规另有规定的除外）; 2.未脱敏的情况下用于其他业务系统或测试环境等; 3.未严格控制个人信息查询以及导出权限;	无。	

序号	要求项目	要求子项	要求小项	不符合判例	补偿措施	检查结论
				4.非法买卖、泄露用户个人信息。		
23			**8.*应对用户个人信息存储和查看展示时采取脱敏等去标识化措施。**	满足条件: 未采取脱敏等去标识化措施。	无。	

附录 B：物业侧安全检查要求

序号	检查对象	检查项	检查方法	检查结论
1	区域边界	通过边界设备，保证跨越网络区域边界的访问和数据流通过边界设备提供的受控接口或端口进行通信。	1.检查是否有边界防护设备; 2.核查网络拓扑图与实际的网络链路是否一致，是否明确了网络边界，且明确边界设备端口; 3.应核查路由配置信息及边界设备配置信息，确认是否指定物理端口进行跨越边界的网络通信; 4.核查是否存在通过其他未受控端口进行跨越边界的网络通信，例如检测无线访问情况，可使用无线嗅探器、无线入侵检测/防御系统、手持式无线信号检测系统等相关工具进行检测; 5.核查内网服务器、终端或其他设备，是否存在绕过边界设备，直连外网的行为。 如采用 VPN 专线连接至上级节点，且物业侧为独立的逻辑隔离网络: 1.检查是否有边界设备是否配置了详细的 ACL 控制规则; 2.核查网络拓扑图与实际的网络链路是否一致，是否明确了网络边界，且明确边界设备端口; 3.应核查路由配置信息及边界设备配置信息，确认是否指定物理端口进行跨越边界的网络通信; 4.核查是否存在通过其他未受控端口进行跨越边界的网络通信，例如检测无线访问情况，可使用无线嗅探器、无线入侵检测/防御系统、手持式无线信号检测系统等相	

序号	检查对象	检查项	检查方法	检查结论
			关工具进行检测; 5.核查针对内网服务器、终端或其他设备，是否配置详细的 IP+MAC 绑定规则; 6.核查内网服务器、终端或其他设备，是否存在绕过边界设备，直连外网的行为。	
2	所有的应用程序包括 Web、APP、小程序、微信等	***数据采集终端和计算机终端等设施的管理员应进行身份标识和鉴别，且确保在系统整个生存周期用户名的唯一性。避免共享帐户存在。**	1.登录数据采集终端计算机终端等管理员用户存在空口令帐户，并可以登录; 2.访谈并检查是否多人共用一个帐户。	
3		***应满足口令复杂度要求，且满足双因素认证。**	检查身份鉴别是否采用密码技术实现，若只采用“用户名+口令”鉴别方式，用户口令须由大小写英文字母、数字、特殊字符 3 种以上组成、长度不少于 8 位，每 90 天更换一次；不应设置记住口令；是否启用双因素认证功能。	
4		***应启用登录失败处理功能，登录失败后采取结束会话、限制非法登录次数和自动退出等措施，例如连续 5 次登录失败至少锁定 10 分钟。**	查看是否具有登录失败处理功能，以及相关配置参数。	
5		***当进行远程管理时，应采取 SSH、HTTPS 等加密协议防止鉴别信息在网络传输过程中被窃听。**	1.检查是否通过不可控网络环境远程进行管理; 2.尝试使用截获的帐户是否可以远程登录; 3.查看管理帐户口令是否以明文方式传输。	
6		**设定特定终端或网络地址范围，对通过网络进行管理的终端进行限制。**	检查 PC、PAD、APP 等是否可以在未授权的终端登录使用。	
7		***应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安**	查看是否启用了审计功能，查看审计的内容是否全面。	

序号	检查对象	检查项	检查方法	检查结论
		全事件进行审计。		
8		审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	查看审计记录信息是否包含相关内容。	
9		***应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。日志保存时间应满足 6 个月。**	查看审计记录备份情况，查看审计记录保护措施，查看审计记录保存时间是否满足 6 个月以上。	
10		对于各小区物业管理终端登入后台管理系统，浏览器不应设置保存密码。	查看小区物业管理终端的浏览器，是否保存了后台管理系统的帐户密码。	
11		***应当遵循合法、正当、必要的原则收集、使用个人信息，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。人像图片上传应限制 JPG、PNG 格式。**	1.查看在未授权情况下，是否采集、存储用户个人隐私信息，无论该信息是否是业务需要。如初次登录、启用新服务、版本变更等是否就相关数据采集情况告知用户并获得授权; 2.采集、保存法律法规、主管部门严令禁止采集、保存的用户隐私信息。如征信等; 3.采集信息超过业务所需范围。	
12		***管理系统仅限存储姓名、采集图片（特征码）、手机号码、车牌号码、身份证号（脱敏处理）、家庭住址;出入记录、抓拍图片等个人信息不得**	1.检查是否存储超出“姓名、采集图片（特征码）、手机号码、车牌号码、身份证号（脱敏处理）、家庭住址”之外的数据类型; 2.检查出入记录、抓拍图片等个人信息是否保存在本地，	

序号	检查对象	检查项	检查方法	检查结论
		保存，应在上传至公安社会资源整合网后及时删除。	是否上传至公安社会资源整合网后未及时删除。	
13		*应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。	1.是否采取有效的技术措施和管理措施保障个人信息的完整性、保密性和可用性，如采用密码技术; 2.访谈及查看规定相关事件发生时处理方式的制度及过程文档。	
14		*应禁止未经被收集者同意，向他人提供个人信息等行为。	1.登录查看是否有共享数据的接口或功能; 2.在进行数据分析、共享等操作时未采取相关措施获得收集者授权。	
15		*应禁止窃取或者以其他非法方式获取个人信息，禁止非法出售或者非法向他人提供个人信息。	登录查看是否具有防范分享、截屏、下载等可能会导致用户信息泄露的措施。	
16		*应当提供用户删除或者更正个人信息的相关措施或手段。	登录查看是否为用户提供了相关信息的更正、注销、删除等功能或服务。	
17		*应禁止未授权访问和非法使用用户个人信息。	登录不同权限的帐户，检查是否能看到用户信息。	
18		*应对用户个人信息存储和查看展示时采取脱敏等去标识化措施。	登录检查是否能直接查看到用户的身份证号码等敏感信息。	
19	小区物业公司/实际承担小区物业管理职能的	*应成立网络安全工作组织，负责人由单位主要负责人担任。	1.是否成立网络安全工作组织; 2.网络安全工作组织的负责人是否为主要负责人。	
20		*应制定符合实际工作需要的网络安全管理制度，并定期评审、更新，且	检查是否制定相关制度或制度与本身实际情况是否相符。	

序号	检查对象	检查项	检查方法	检查结论
	单位（有的物业公司同时服务多个小区，则需要公司总部及小区分部都要有相关的要求）	**做好必要的版本控制。**		
21		***应对系统操作员等关键岗位人员进行网络安全意识和操作技能培训，并进行必要的考核。**	访谈并检查是否开展网络安全相关培训，需查看相关的照片、签到表等过程文档。	
22		***应与系统操作员等关键岗位人员签订保密协议或保密承诺书，不可泄露用户的敏感信息。**	查看相关人员是否签订相关保密协议或保密承诺书。	
23		***应做好人员招聘、录用、使用、离岗等人员全生命周期管理工作，尤其是离岗时应签署离岗保密协议和承诺书，收回钥匙、key 并注销其相关帐户等。**	访谈相关人员，抽查相关人员过程材料。	
24		采购的软硬件产品，应符合国家法律法规及标准要求。	检查采购的软硬件产品是否具有检测报告、设备手册、购买协议等相关材料并做好归档。软件产品的检测报告应包含安全要求。	
25		应做好智慧平安小区相关关键设备的运维工作，确保设备所在区域干净整洁，不堆放杂物，不在此接待外来无关人员。	1.设备运维是否定岗定人; 2.设备区域堆放杂物，人员混杂。	
26		***应做好移动介质、文档管理工作，由专人负责存档、借出、归还等管理工作，并做好相应的记录。**	介质是否有专人管理，并检查相关过程文档。	
27		应定期对终端等设备开展检查工作，包括但不限于身份鉴别、访问控制、	是否定期开展相关工作，并查看相关过程文档。	

序号	检查对象	检查项	检查方法	检查结论
		恶意代码防范等。做好检查过程和结果的记录和存档。		
28		应定期对关键岗位人员开展网络安全工作开展情况检查，按照相关的规定考核并作出奖惩。	是否定期开展检查工作，是否有考核要求，是否有奖惩记录等过程文档。	
29	人脸识别门禁闸机等感知终端	应具备防水、防潮、防尘设计，防护等级应不低于 IP44。设备工作温度范围应满足-15℃~+55℃，湿度范围应满足 25%~95%（无凝露）	1.检查设备说明书及检测报告，设备防尘、防水等级为 IP44，设备工作温度范围应满足-15℃~+55℃，湿度范围应满足 25%~95%（无凝露）； 2.访谈设备管理员及相关人员，设备近 3-6 个月是否出现过宕机情况，出现多少次，是否有相关维修记录。	
30		设备应固定不能轻易移动，且设置有明显的不易去除的唯一性标识。设备外壳应具备一定的防物理拆卸等措施。	1.检查设备是否采用合理方式进行固定，是否可以轻易挪动。是否有不易去除的唯一性标识; 2.检查设备是否可以用普通工具拆卸或者破坏，是否有专人值守或视频监控，是否在发生非授权打开时能告警或及时发现; 3.如专人值守应检查值班记录，如有视频监控应检查视频监控是否有盲区及存储时长。	
31		设备应集成防雷和接地保护装置，具备防雷击和防浪涌冲击的能力，或有效接地。	1.检查设备说明书及检测报告，设备是否具有防雷击、过电压保护措施; 2.检查是否有效接地。	
32		设备所在地应具备火灾探测和灭火能力。	检查设备自身或所处环境，是否具备及时发现火灾及灭火的能力。	
33		当进行远程管理时应启用 SSH、HTTPS 等加密通信协议，加密管理数据、鉴别信息，防止被网络窃听。	1.检查是否通过不可控网络环境进行远程管理; 2.使用截获的帐户是否可以远程登录; 3.管理帐户口令是否以明文方式传输。	

序号	检查对象	检查项	检查方法	检查结论
34		*应提供设备认证能力，保证只有授权的设备可以接入，防止前端仿冒、替换等非法接入行为。可在小区侧部署安全接入网关措施，采用内置准入控制技术措施。	1.检查设备有哪些接入方式，包括但不限于usb、蓝牙、无线等; 2.检查设备说明书及检测报告，是否有明确说明具备授权认证能力; 3.现场开展非授权设备接入测试，验证是否真实有效。	
35		*应能够限制与设备通信的目标地址，以避免对陌生地址的攻击行为（非法攻击、恶意扫描、漏洞攻击等）。可在小区侧部署安全接入网关措施，或采取其他具备入侵防范能力的措施。	1.检查是否有统计各设备的MAC地址及IP地址等信息的功能; 2.现场检查与该设备关联的相关设备是否进行了IP地址及MAC地址绑定; 3.现场测试非绑定设备能否接入; 4.检查现场是否采取攻击防范措施; 5.攻击防范措施配置是否得当，是否存在较大安全隐患。	
36		*设备的合法用户应具有统一的用户标识、不得使用默认口令，不得存在共享帐户。	1.查看是否修改默认帐户的默认口令; 2.测试使用该设备的默认帐户及口令能否登录; 3.访谈并查看是否存在多人共用一个帐户的情况;	
37		*若只用“用户名+口令”的鉴别方式进行身份鉴别，则应使用具有一定复杂度的用户口令（用户口令须由大小写英文字母、数字、特殊字符3种以上组成、长度不少于8位），90天进行更新。	1.检查只用“用户名+口令”的鉴别方式进行身份鉴别，则应使用具有一定复杂度的用户口令（用户口令须由大小写英文字母、数字、特殊字符3种以上组成、长度不少于8位），90天进行更新; 2.查看是否采用密码技术。需通过抓包工具来进行验证，密码技术使用是否合法、正确、有效。	
38		*具有登录失败和登录超时处理功能，连续5次登录失败至少锁定10分钟。	1.是否可以通过远程登录; 2.对连续登录失败有哪些处理措施; 3.攻击者是否可以利用登录界面进行口令猜测。	

序号	检查对象	检查项	检查方法	检查结论
39		***应保证只有授权的用户可以对设备上的软件应用进行配置或变更。**	1.检查登录该设备是否需要用户名和口令; 2.用户存在空口令或弱口令帐户，并可以登录; 3.检查设备上用户类型，查看权限是否有进行区分控制。	
40		设备应支持远程集中管控，并纳入远程集中管控。	检查所有感知终端是否支持且纳入远程集中管控。	
41	数据采集终端（电脑、手机、pad等）	系统数据上传终端（各小区物业windows台式机）应保持可控管理，设置满足复杂度要求的口令和屏保。	1.是否对终端设置了满足复杂度要求的口令（长度8位以上，由大小写字母、数字和特殊字符2种或3种组合方式组成），必要时重启电脑，现场进行登录演示; 2.查看windows“屏幕保护程序设置”，是否设置了屏保时间，是否勾选了“在恢复时显示登录屏幕”。	
42		对于业务操作的终端，不应安装不可信任的软件，操作员应定期检查操作系统版本，进行在线更新。	1.检查终端电脑，是否存在不必要的软件（qq、微信、游戏等）; 2.查看系统更新，是否及时更新了最新补丁。	
43		应采用免受恶意代码攻击的技术措施，能够识别、阻断病毒入侵行为。	检查终端是否安装杀毒软件，病毒库是否是最新版本，是否进行定期安全扫描。	
44		系统应仅采集与业务相关的数据，避免出现未授权采集、超范围采集的情况（对于所采集的数据详情，应及时告知用户）。	1.调查当前系统采集的个人信息涉及哪几类（姓名、手机号、身份证号码、住址等），是否为业务必须采集的; 2.系统是否对用户提供服务协议说明; 3.服务协议说明是否明确告知用户所采集的数据明细。	
45	物业管理PC	物业管理PC是否处于防风、防雨的房屋内。	检查是否放置在防风、防雨的屋内，是否会面临水患等风险。	
46		物业管理PC所在房间应通过门禁等方式进行有效控制。	检查管理PC的房间是否有门禁等，避免盗窃等情况的发生。	
47		***物业管理PC终端应禁用访客帐户，修改默认帐户的口令，并设置满足复**	1.是否对终端设置了满足复杂度要求的口令（长度8位以上，由大小写字母、数字和特殊字符2种或3种组合	

序号	检查对象	检查项	检查方法	检查结论
		杂度要求的口令。	方式组成），必要时重启电脑，现场进行登录演示; 2.是否禁用来宾帐户，是否修改默认帐户的登录口令。	
48		*对每一位操作员分配专用的帐户，避免共享帐户存在。	现场检查物业配备了几名数据上传操作员，并查看是否为每人配备了专用的操作员帐户，不可多人使用同一帐户。	
49		*应启用登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施（可设置登录失败 5 次锁定 10 分钟）。	1.连续输入多次错误密码物业后台管理系统是否会锁定; 2.锁定后等待多久可以再次登录，如何解锁; 3.系统长时间未操作，是否会自动退出需要再次登录。	
50		*应采用免受恶意代码攻击的技术措施。	1.核查操作系统中防病毒软件安装情况，访谈管理员病毒库是否定期更新，核查病毒库是否更新至最新版本; 2.是否启用了防火墙，查看防火墙的配置。	

附录 C：盒子安全检查要求

序号	检查对象	检查项	检查方法	检查结论
1	网络全局	***应至少采用校验技术保证通信过程中数据的完整性；根据需要可采用密码技术保证通信过程中数据的完整性，密码算法应符合国家密码管理局相关规范要求。**	1.在通信过程中是否配备 SSLVPN 网关、IPSecVPN、安全接入网关或其他具有相同功能的设备; 2.是否采用加密通信协议，如 https 协议进行通信加密 3.是否使用 MD5、RSA、3DES 或国密算法进行数据通信加密。	
2		***盒子应与其他网络区域之间应采取可靠的技术隔离手段。**	查看互联网边界、社会资源整合平台边界、前端感知边界等是否采取有效措施，如部署网闸、防火墙、安全接入网关、采用专线+VPN 等技术实现网络的逻辑隔离。	
3		***应提供前端感知设备认证能力，保证只有授权的设备可以接入，防止前端仿冒、替换等非法接入行为，可在小区侧部署安全接入网关措施，采用内置准入控制技术措施。**	现场开展非授权设备接入测试，验证是否具备准入控制功能。	
4		***应能够限制与设备通信的目标地址，以避免对陌生地址的攻击行为（非法攻击、恶意扫描、漏洞攻击等）。可在小区侧部署安全接入网关，或采取其他具备入侵防范能力的措施。**	1.是否采取攻击防范措施; 2.攻击防范措施配置是否得当，是否存在较大安全隐患。	
5	主机（检查方法以 CentOS、	***应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。**	CentOS: 1.访谈主机服务器运维负责人，是否通过帐户和口令维护 Linux 服务器，并登录操作系统验证是否符合。除 root	

序号	检查对象	检查项	检查方法	检查结论
	Windows 为例，其他操作系统应根据实际情况进行检查。)		帐户外，使用最高的权限身份登录后，在命令行状态下可直接输入命令，或在图形界面状态下右键点击桌面空白处，选择“打开终端”，执行下列命令#cat /etc/passwd查看文件中每行的第二个值是为空还是“X”，“X”则有密码，空则为无密码，为“X”符合，为空不符合。如example::3:3:example:/bin/example ；用户登录后，命令行状态下输入#cat /etc/passwd，检查各帐户第一列值是否名称相同，如相同，则不符合; 2.用户登录后，命令行状态下输入#cat /etc/passwd，检用户名相同、UID（第三字段）相同的帐户，如相同，则不符合; 3.检查设备是否存在同名用户，是否能新建同名用户; 4.使用用户身份登录后，命令行状态下输入#cat /etc/login.defs 查看关于密码验证的各种设置，是否满足密码的复杂度、定期更换等要求，CentOS 推荐配置PASS_MAX_DAYS:90; PASS_MIN_DAYS:2; PASS_MIN_LENS:8; PASS_WARN_AGE:7; 口令推荐设置：密码长度不小于 8 位，由（字母、数字、特殊字符）中任意三种或三种以上组成; 5.检查是否有定期更换口令。 Windows: 1.用户需要输入用户名和密码才能登录; 2.Windows 默认用户名具有唯一性; 3.打开“控制面板”->“管理工具”->“计算机管理”->“本地用户机组”检查有哪些用户，并尝试空口令登	

序号	检查对象	检查项	检查方法	检查结论
			录; 4.打开“控制面板”->“管理工具”-> “本地安全策略”-> “账户策略” “密码策略”。	
6		***应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。**	CentOS: 1.用户身份登录后，命令行状态下输入#cat /etc/pam.d/system-auth,查看是否存在 account required /lib/security/pam_tally.so deny=5 no_magic_rootreset 项，deny=5 表示 5 次失败则锁定，有此项则满足; 2.退出帐户，验证是否按照配置启用了登录失败这个功能; 3.当服务器通过 SSH 方式进行远程连接时，需在命令行状态下输入#cat /etc/pam.d/ssh/sshd 查询是否设置了登录失败的策略; 4.检查并记录系统是否启用了用户超时自动注销功能，命令行状态下输入 cat /etc/profile 中的 TIMEOUT 环境变量，在“HISTFILESIZE=”行的下一行是否有如下一行: TMOUT=XXX 秒，上述配置表示所有用户将在 XXX 秒无操作后自动注销，查看是否设置，设置为符合。 Windows: 1.打开“控制面板”-> “管理工具”->“本地安全策略”-> “账户策略”->“密码锁定策略”; 2.右键点击桌面->“个性化”->“屏幕保护程序”，查看“等待时间”的长短以及“在恢复时显示登录屏幕”选项是否打钩。	

序号	检查对象	检查项	检查方法	检查结论
7		***当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。**	CentOS: 1.最高权限用户身份登录，命令行状态下输入#service --status-all | grep running,查看是否开启了 telnet 服务，telnet 使用明文传输信息，应当禁用此服务; 2.最高权限用户身份登录，命令行状态下输入#service --status-all | grep sshd,查看是否开启了 SSH 服务，SSH 采用加密连接，密码信息得到加密，使用 SSH 才能满足要求; 3.若不确定是否安装了 SSH 服务，首先查看是否安装 SSH 相应包#rpm -aq|grep ssh 或者查看是否运行了 sshd 服务#service --status-all|grep sshd。如果已经安装则查看相关的端口是否打开#netstat -an|grep 22。 Windows: 1.如果是本地管理成 KVM 等硬件管理方式，此要求为不适用; 2.如果采用远程管理，则需采用带加密管理的远程管理方式。在命令行输入”pgedit.msc“弹出“本地组策略编辑器”窗口，查着“本地计算机策略->计算机配置->管理模板->Windows 组件->选程桌面服务->远程桌面会话主机-安全”中的相关项目。	
8		应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	CentOS: 1.访谈系统管理员，对系统的登录是否采用双因子身份认证方式进行验证，查看有无 CA 认证服务器或其他身份认证手段，如存在其他认证方式，尝试进行其他认证方式的身份登录验证，生物技术，当存在两种或两种以上	

序号	检查对象	检查项	检查方法	检查结论
			身份登录方式为符合; 2.核查其中一种鉴别技术是否使用密码技术来实现。 Windows: 查看和访谈系统管理员在登录操作系统的过程中使用了哪些身份鉴别方法，是否采用了两种或两种以上组合的鉴别技术，如口令、教字证书 Ukey、令牌、指纹等，是否有一种鉴别方法在鉴别过程中使用了密码技术 记录系统管理员在登录操作系统使用的身份鉴别方法，同时记录使用密码的鉴别方法。	
9		应对登录的用户分配帐户和权限。	CentOS: 1.访谈系统管理员，日常登录和使用的用户有哪些，是否为用户分配了帐户和权限及相关设置情况; 2.root 身份登录系统，检查不同用户的/etc 下的重要的配置文件的 mask 值，用“ls-l”查看文件访问权限，其 mask 值不能大于 644（即-wr--r--r--），查看可执行文件，权限不大于 755(即-xwr-xr-xr)，如 passwd，shadow，login.defs，crontab，group，hosts 等。 Windows: 访谈系统管理员，操作系统能够登录的账户，以及它们拥有的权限， 选择%systemdrive%\windows \system、%systemroot %\system32\config 等相应的文件夹，右键选择“属性”->“安全”，查看 everyone 组、users 组和 administrators 组的权限设置。	

序号	检查对象	检查项	检查方法	检查结论
10		***应重命名或删除默认帐户，修改默认帐户的默认口令。**	CentOS: 1.查看#cat/etc/shadow 文件，访谈相应帐户情况和作用，检查存在的系统默认帐户是否已经重命名或禁用（已锁定帐户其所在行第一个和第二个冒号之间的口令字段为“!!或*”）； 2.应核查是否已修改默认帐户的默认口令。 Windows: 在命令行输入"lusrmgr.msc"弹出“本地用户和组”窗口，查看“本地用户和组->用户”中的相关项目。	
11		***应及时删除或停用多余的、过期的帐户，避免共享帐户的存在。**	CentOS: 1.查看#cat /etc/shadow 文件，访谈相应帐户是否为过期、多余帐户（已锁定帐户其所在行第一个和第二个冒号之间的口令字段为“!!或*”），管理员用户与帐户之间是否一一对应; 2.检查 shadow 文件下 Linux 系统的常见的默认帐户,如:uucp、nuucp、lp、adm、sync、shutdown、halt、news、operator、gopher 用户是否已禁用; 3.检查和验证常见的默认帐户如 root 帐户的口令是否是默认口令，是否定期更换口令; 4.应测试验证多余的、过期的帐户是否被删除或停用。 Windows: 在命令行输入“lusmrgr.msc",弹出“本地用户和组”窗口，查看“本地用户和组->用户”中的相关项目，查看右侧用户列表中的用户,访谈各账户的用途，确认账户是否属于多余的、过期的账户或共享账户。	

序号	检查对象	检查项	检查方法	检查结论
12		应授予管理用户所需的最小权限，实现管理用户的权限分离。	CentOS: 1.访谈系统管理员，日常登录和管理使用的用户有哪些，核查是否进行角色划分; 2.最高权限用户身份登录，在命令行下输入#cat /etc/passwd，查看各用户具备的权限和拥有的目录，不同的帐户是否分配了不同的权限，查看用户权限是否过高，如使用 groups 命令查看组属性，用 cat /etc/group 查看是否有过高权限的组; 3.root 身份登录系统，检查不同管理员帐户的/etc 下的重要的配置文件的 mask 值，用“ls -l”查看文件访问权限，其 mask 值不能大于 644（即-wr--r--r--），查看可执行文件,权限不大于 755(即-xwr-xr-xr),如 passwd，shadow，login.defs，crontab，group，hosts 等。 Windows: 1.在命令行输入"secpol.msc"，弹出“本地安全策略”窗口，查看“安全设置->本地策略->用户权限分配”中的相关项目。右侧的详细信息窗口即显示可配署的用户权限策略设置。	
13		应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。	CentOS: 1.访谈系统管理员，是由哪个帐户来进行访问控制策略的配置。检查其它帐户是否能越权配置访问控制策略; 2.检查访问控制策略，是否定义了每个帐户能进行的具体操作，如使用某个应用，访问某个文件等。应测试验证用户是否有可越权访问情形。 Windows:	

序号	检查对象	检查项	检查方法	检查结论
			1.访谈系统管理员,能够配置访问控制策略的用户; 2.查看重点目录的权限配置，是否依据安全策略配置访问规则。	
14		访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。	CentOS: 应检查重要文件目录等权限设置，包括但不限于etc/passwd、etc/profile、var/log/audit/audit.log等。 Windows: 选择%systemdrive%\program files 、%systemdrive%\system32 等重要的文件夹， 以及%systemdrive%\Windows \system32 config 、%systemdrive%\Windows\system32\secpol 等重要的文件，右键选择“属性”->“安全”，查看访问权限设置。	
15		***应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。**	CentOS: 1.查看是否启用安全审计功能。使用最高权限用户身份登录进入 Linux 命令行状态下输入命令 service syslog status 和 service audit status，或者输入 service --status-all|grep running。分别查看审计进程是否开启，如显示“running”，则符合; 2.通过访问控制策略规定主体对客体的访问规则。若运行了安全审计服务，则查看安全审计的守护进程是否正常: ps -ef |grep auditd。 Windows: 1.查看系统是否开启了安全审计功能。在命令行输入	

序号	检查对象	检查项	检查方法	检查结论
			“"secpol.msc”,弹出“本地安全策略”窗口，查看“安全设置->本地策略->审核策略”中的相关项目。右侧的详细信息窗格即显示审核策略的设置情况; 2.访谈并查看是否有第三方审计工具或系统。	
16		***审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。**	CentOS: 1.使用最高管理员帐户登录，在命令行下输入: more /var/log/messages 查询日志记录; 2.Linux 系统在开启审计进程后，能记录日期、时间、主客体、结果等属性值，因此当开启审计进程时，此项自动满足; 3.此项可访谈客户是否通过第三方安全审计软件对服务器进行审计，若实际查看了第三方安全审计软件已对服务器进行审计，则此项符合。 Windows: 1.在命令行输入"eventvwr.msc"，弹出“事件查看器”窗口，“事件查看器(本地)->Windows 日志"下包括“应用程序”、“安全”、“设置”、“系统”几类记录事件类型，点击任意类型事件，查看日志文件是否满足此项要求; 2.如果安装了第三方审计工具，则:查看审计记录是否包括日期、时间，类型、主体标识、客体标识和结果。	
17		***应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。**	CentOS: 1.访谈系统管理员，日常登录和管理使用的用户有哪些，不同的帐户是否分配了不同的权限; 最高权限用户身份登录，查看 syslog.conf、audit.conf 文件中日志信息	

序号	检查对象	检查项	检查方法	检查结论
			所在文件的访问权限，如: ls -l /var/log/messages; ls -l /var/log/secure; ls -l /var/log/audit/audit.log; 权限值不能超过 644，超过则为不符合; 2.访谈是否对审计日志进行保护; 3.访谈审计的记录是否进行日常备份，查看日志备份文件和存储日期是否满足 6 个月及以上。 Windows: 1.如果日志数据本地保存，则访谈审计记录备份周期，有无异地备份。在命令行输入“eventvwr. msc”,弹出“事件查看器”窗口，“事件查看器(本地)->Windows 日志”下包括“应用程序” 、“安全”、“设置”、“系统”几类记录事件类型，右键点击类型事件，选择下拉菜单中的“属性”，查看日志存储策略; 2.如果日志数据存放在日志服务器上并且审计策略合理,则该要求为符合。	
18		***应对审计进程进行保护，防止未经授权的中断。**	CentOS: 1.访谈是否安装额外的审计进程保护软件，确保审计进程不会受到未预期的中断; 2.若系统未安装额外的审计进程保护软件，查看并访谈对审计进程的监控和保护措施，有能力的情况下对审计进程进行中断测试，查看能否单独中断审计进程。 Windows: 1.访谈是否有第三方审计进程监控和保护的措施;	

序号	检查对象	检查项	检查方法	检查结论
			2.在命令行输入"secpol.msc"，弹出“本地安全策略”窗口，点击“安全设置->本地策略->用户权限分配”，右键点击策略中的“管理审核和安全日志”，查看是否只有系统审计员或系统审计员所在的用户组。	
19		应遵循最小安装的原则，仅安装需要的组件和应用程序。	CentOS: 1.应核查是否遵循最小安装原则; 2.root 权限执行命令 service --status-all,查看是否存在多余的应用程序和组件。 Windows: 1.访谈安装系统时是否遵循最小化安装原则，查看安装操作手册; 2.查看操作系统中已安装的程序，否有目前非业务必须的组件和应用程序。	
20		***应关闭不需要的系统服务、默认共享和高危端口。**	CentOS: 1.网络端口：检查并记录系统开启的网络端口 netstat -nltp 记录系统开启的 TCP 和 UDP 端口; 2.开启服务：检查并记录系统开启的服务，root 权限执行命令 service --status-all|grep running,查看并确定是否关闭危险的网络服务如 echo、shell、login、finger 等，关闭不必要的服务如 talk、ntalk、pop-2、sengmail、imapd、pop3d 等。 Windows: 1.查看系统服务。在命令行输入"services. msc “，打开系统服务管理界面，查看右侧的服务详细列表中多余的服务， 如 Alerter、Remote Registry Servicce	

序号	检查对象	检查项	检查方法	检查结论
			Messsenger,Task Scheduler 是否已启动; 2.查看监听端口在命令行输入"netstat -an”，查看列表中的监听端口，是否包括高危端口，如 TCP 135、139、45、593、1025 端口，UDP 135、137、138、445 端口，一些流行病毒的后门端口，如 TCP 2745、3127、6129 端口; 3.查看默认共享。在命令行输入"net share"，查看本地计算机上所有共享资源的信息，是否打开了默认共享，例如 C$、D$; 4.查看主机防火墙策略。在命令行输入"firewall. cpl”打开 Windows 防火墙界面，查看 Windows 防火墙是否启用。点击左侧列表中的“高级设置”，打开“高级安全 Windows 防火墙”窗口。点击左侧列表中的“入站规则”，右侧显示 Windows 防火墙的入站规则，查看入站规则中是否阻止访问多余的服务，或高危端口。	
21		应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。	CentOS: root 身份登录系统，命令行模式下查看对主机的访问设置。cat /etc/hosts.deny，查看是否有“ALL:ALL”禁止所有的请求，并查看允许规则 cat /etc/hosts.allow，是否设置了最小的服务访问允许规则，如 sshd:IP/掩码。 Windows: 1.询问系统管理员管理终端的接入方式。查看主机防火墙对登录终端的接入地址限制，在命令行输入"firewall.cpl",打开Windows防火墙界面,查看Windows防火墙是否启用。点击左侧列表中的“高级设置”，打开“高级安全 Windows 防火墙”窗口，点击左侧列表中	

序号	检查对象	检查项	检查方法	检查结论
			的“入站规则”，双击右侧入站规则中的“远程桌面->用户模式(TCP-In)"，打开“远程桌面用户模式(TCP-In)属性"窗口，选择“作用城”查看相关项目; 2.查看 IP 筛选器对登录终端的接入地址限制。在命令行输入“gpedit.msc"打开本地组策路编辑器界面，点击左侧列表中的“本地计算机策略->计算机配置 Windows 设置->安全设置->IP 安全策略”，在本地计算机双击右侧限制登录终端地址的相关策略”，查看 “IP 筛选器列表”和“IP 筛选器属性”; 3.网络方面对登录终端的接入方式和地址范围的限制 访谈并查看是否通过网络设备或硬件防火墙对终端接入方式、网络地址范围等条件进行限制。	
22		***应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。**	CentOS: 1.根据主机漏洞扫描结果,输入命令 rpm -qa |grep patch 查看补丁版本,是否安装了相关补丁; 2.应通过漏洞扫描、渗透测试等方式核查是否不存在高风险漏洞; 3.核查是否在经过充分测试评估后及时修补漏洞。 Windows: 1.访谈系统管理员是否定期对操作系统进行漏洞扫描，是否对扫描发现的漏洞进行评估和补丁更新测试，是否及时进行补丁更新，及补丁更新的方法; 2.在命令行输入"appwiz.cpl" ,打开程序和功能界面，点击左侧列表中的“查看已安装的更新”，打开“已安装更新”界面，查看右侧列表中的补丁更新情况。	

序号	检查对象	检查项	检查方法	检查结论
23		***应启用操作系统防火墙，配置合理的访问控制策略，实现入侵防护功能。**	CentOS: 1.查看系统日志是否有入侵留痕，“more /var/log/secure|grep refused”查看是短时间内否有大量的尝试失败信息; 2.查看是否开启防火墙 service iptables status，查看状态是否启用。 Windows: 1.检查 windows 操作系统是否开启了防火墙功能，限制对高危端口的访问; 2.访谈系统管理员是否安装了主机入侵检测软件，查看已安装的主机入侵检查系统的配置情况，是否具备报警功能。	
24		***应采用免受恶意代码攻击的技术措施及时识别病毒攻击行为，并将其有效阻断。**	CentOS: 核查操作系统中安装了什么防病毒软件，访谈管理员病毒库是否定期更新，核查病毒库是否为最新版本。 Windows: 1.查看系统中安装的防病毒软件。访谈管理员病毒库是否定期更新。查看病毒库是否更新至最新版本; 2.询问系统管理员网络防病毒软件和主机防病毒软件分别采用什么病毒库; 3.访谈系统管理员是否果有统一的病毒更新策略和查杀策略; 4.当发现病毒入侵行为时，如何发现，如何有效阻断等，报警机制等。	

序号	检查对象	检查项	检查方法	检查结论
25		***应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。**	1.应核查系统设计文档，鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在传输过程中是否采用了校验技术或密码技术保证完整性; 2.应测试验证在传输过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。	
26		***应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。**	1.应核查设计文档，是否采用了校验技术或密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性; 2.应核查是否采用技术措施（如数据安全保护系统等）保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性; 3.应测试验证在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。	
27		***应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。**	1.应核查是否采用技术措施（如数据安全保护系统等）保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性; 2.应测试验证是否对指定的数据进行加密处理。	

序号	检查对象	检查项	检查方法	检查结论
28		应提供重要数据的本地数据备份与恢复功能。	1.访谈系统管理员哪些是重要数据处理系统，重要数据处理系统是否有备份机制，是否采用本地热备份站点备份或异地活动互援备份; 2.核查备份路径下是否有备份文件存在，备份日期是否为最近的日期; 3.访谈小区采集数据是否上报至公安社会资源整合网，如上报，可视同符合。	
29		应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。	1.访谈是否有异地灾备机房实现实时数据备份。 2.访谈小区采集数据是否上报至公安社会资源整合网，如上报，可视同符合。	
30		应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。	检查操作系统维护/操作手册，查看其是否明确用户的鉴别信息存储空间以及被释放或再分配给其他用户前的处理方法和过程。	
31		应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。	检查操作系统维护/操作手册，系统内的文件、目录等资源所在的存储空间，被释放或重新分配给其他用户前的处理方法和过程。	
32	数据库（检查方法以MySQL为例，其他数据库应根据实际情况进行检查。）	***应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。**	1.尝试登录数据库，执行mysql -uroot -p查看是否提示输入口令鉴别用户身份; 2.使用如下命令查询帐户: select user, host from mysql.user 结果输出用户列表，检查是否存在相同用户名; 3.执行如下语句查询是否在空口令用户: select* from mysql.user where length(passwor= 0 or password is null输出结果是否为空; 4.执行如下语句查看用户口今复杂度相关配置:	

序号	检查对象	检查项	检查方法	检查结论
			show variables like ′validate%′; 或 show variables like "%password”	
33		***应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。**	1.访谈管理员是否采取其他手段配置数据库登录失败处理功能; 2.执行 show variables like %max_connect_errors%”; 或核查 my.cnf 文件，应设置如下参数: max_connect_errors=100; 3. show variables like “%timeout%”，查看返回值。	
34		***当进行远程管理时，应采取必要措施、防止鉴别信息在网络传输过程中被窃听。**	1.是否采用加密等安全方式对系统进行远程管理; 2.执行 mysql>show variables like %have_ssl%" 查看是否支持 ssl 的连接特性，若为 disabled 说明此功能没有激活，或执行\s 查看是否启用 SSL; 3.如果采用本地管理方式，该项为不适用。	
35		应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	1.MySQL 不能集成其他身份鉴别措施，应通过对操作系统层面实现双因素; 2.访谈系统管理员，是否采用其他技术手段实现双因素身份认证，是否采用了两种或两种以上组合的鉴别技术，如口令、数字证书 Ukey.令牌、指纹等，是否有一种鉴别方法使用密码技术。	
36		应对登录的用户分配帐户和权限。	1.执行语句 select user,host from mysql.user 输出结果是否为网络管理员，安全管理员，系统管理员，是否创建了不同帐户; 2.执行 show grants for′ XXXX′@′ localhost′: 查看网络管理员，安全管理员、系统管理员用户帐户的权限，权限间是否分离并相互制约。	

序号	检查对象	检查项	检查方法	检查结论
37		***应重命名或删除默认帐户，修改默认帐户的默认口令。**	1.执行 select user,host from mysql.user 输出结果查看 root 用户是否被重命名或被删除; 2.若 root 帐户未被删除，是否更改其默认口令，避免空口令或弱口令。	
38		***应及时删除或停用多余的、过期的帐户，避免共享帐户的存在。**	1.在 sqlplus 中执行命令: select username,account_status from dba_users; 2.执行下列语句: select* from mysql.user where user="" select user, host FROM mysql.user 依次核查列出的帐户，是否存在无关的帐户; 3.访谈网络管理员，安全管理员、系统管理员不同用户是否采用不同帐户登录系统。	
39		***应授予管理用户所需的最小权限，实现管理用户的权限分离。**	1.是否对用户进行角色划分且只授予帐户必须的权限。如除 root 外，任何用户不应该有 mysql 库 user 表的存取权限，禁止将 fil、process、super 权限授予管理员以外的帐户; 2.查看权限表，并验证用户是否具有自身角色外的其他用户的权限。	
40		应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。	1.访谈管理员是否制定了访问控制策略; 2.执行语句: mysql>selcec* from mysql.user\G -检查用户权限列 mysql>selcec* from mysql.db\G --检查数据库权限列 mysql>selcec* from mysql.tables_priv\G 一检查用户表权限列 mysql>selcec* from mysql.columns_privi\G -检查列	

序号	检查对象	检查项	检查方法	检查结论
			权限列管理员 输出的权限列是是否与管理员制定的访问控制策略及规则一致; 3.登录不同的用户，验证是否存在越权访问的情形。	
41		访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。	1.执行下列语句: mysql>selcec* from mysql.user\G -检查用户权限列 mysql>selcec * from mysql.db\G --检查数据库权限列; 2.访谈管理员并核查访问控制粒度主体是否为用户级，客体是否为数据库表级。	
42		***应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。**	1.执行下列语句: mysql>show variables like ′log_%′ 查看输出的日志内容是否覆盖到所有用户，记录审计记录覆盖内容; 2.核查是否采取第三方工具增强 MySQL 日志功能。若有，记录第三方审计工具的审计内容，查看是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	
43		***审计记录应包括事件的日期和时间，用户、事件类型，事件是否成功及其他与审计相关的信息。**	1.执行下列语句: mysql>show variables like ′log_%′ 查看输出的日志内容是否覆盖到所有用户，记录审计记录覆盖内容; 2.核查是否采取第三方工具增强 MySQL 日志功能。若有，查看记录第三方审计工具的审计内容，是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。	

序号	检查对象	检查项	检查方法	检查结论
44		***应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。**	1.访谈管理员对审计记录如何保护，对审计记录是否定期备份，备份策略; 2.是否严格限制用户访问审计记录的权限。	
45		***应对审计进程进行保护，防止未经授权的中断。**	1.访谈是否严格限制管理员、审计员权限; 2.用户重启实例关闭审计功能，查看是否成功。	
46		***应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。**	查看用户登录的 IP 地址，是否给所有用户加上 IP 限制，拒绝所有未知主机进行连接。 注:当 user 表中的 Host 值不为本地主机时，应指定特定 IP 地址，不应为%; 或将 user 表中的 Host 值为空，而在 host 表中指定用户帐户允许登陆访问的若干主机; 在非信任的客户端以数据库帐户登录应被提示拒绝，用户从其他子网登录，应被拒绝。	
47		***应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。**	访谈 MySQL 补丁升级机制，查看补丁安装情况: 1.执行如下命令查看当前补丁版本: show variables where variable name like "version" 2.是否定期进行漏洞扫描，针对高风险漏洞是否评估补丁并经测试后再进行安装。	
48		应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。	1.访谈系统管理员是否提供异地数据备份功能，是否定时批量传送至备用场地; 2.如果条件允许，则查看其实现技术措施的配置情况。 3.访谈小区采集数据是否上报至公安社会资源整合网，如上报，可视同符合。	