**上海市视频安防监控数据导出防泄密系统基本技术要求（试行）**

1. 范围

本要求规定了对本市视频安防监控系统中采用的视频安防监控数据导出防泄密系统（以下简称“防泄密系统”）的总体要求、组成和基本功能，是相关产品设计、编制、安装和检测的主要技术依据之一。

本要求适用于视频安防监控系统中本地及远程视频安防监控数据导出的防泄密系统。

2. 术语及定义

2.1. 视频安防监控数据（文件）

采用用户终端由视频安防监控系统数字录像设备导出的录像文件和截图文件。

2.2. 安全策略

对视频监控文件使用范围的设定及操作行为的响应策略。

2.3. 用户终端

经联网系统注册并授权、对视频安防监控系统内的数据和/或设备有操作需求的客户端设备。

2.4. 防泄密网关

对视频安防监控系统获取视频安防监控数据（文件）进行防泄密保护的网间连接及协议控制设备。

2.5. 防泄密系统软件

依附于用户终端运行，结合防泄密网关，对获取视频安防监控数据（文件）进行防泄密保护的软件。

3. 总体要求

3.1. 防泄密系统安全性评估应符合《信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求》（GB/T 18336.3－2001）的规定。

3.2. 防泄密系统身份鉴别和安全审计的防控强度应满足《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）第三级安全防护的规定。

3.3. 防泄密系统应符合《信息安全技术 主机文件监测产品检验规范》（[MSTL\_JGF\_04-025](http://www.mctc.gov.cn/bz/MSTL_JGF_04-025.pdf)）的规定。

3.4. 防泄密系统应适用于符合《视频安防监控数字录像设备》（GB 20815-2006）、《上海综合型数字录像设备补充技术要求》及《本市专业型数字录像设备补充技术要求》规定的数字录像设备。

3.5. 用户终端任何对数字录像设备的操作应采用两组用户口令的认证方式。其中一组为视频安防监控系统自身的用户口令，一组为防泄密系统的口令。

4. 系统组成

4.1. 防泄密系统可由单台或多台防泄密网关及防泄密系统软件组成。

4.2. 防泄密网关的配置应与视频安防监控系统和联网模式相适应。

4.3. 防泄密系统软件的自身运行环境要求如下：

a) CPU：1.8GHz及以上

b) 内存：1G及以上

c) 操作系统：通用性操作系统

5. 技术要求

5.1. 安全策略

防泄密系统应具有对用户终端管理员提供策略增加、修改、删除与应用等功能。

5.2. 身份鉴别

a) 防泄密系统应提供专用的登录控制模块对登录用户进行身份标识和鉴别；

b) 防泄密系统应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

c) 防泄密系统应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

d) 防泄密系统应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

e) 防泄密系统应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

5.3. 访问控制

a) 防泄密系统应提供访问控制功能，依据安全策略，控制视频监控文件访问的授权环境及视频监控文件的访问。保护视频监控文件的能力应不小于5G字节；

b) 防泄密系统应具有防控用户终端截取内存和显存数据截屏的能力；

c) 防泄密系统应支持对视频监控文件的操作提交申请、批复和授权。申请、批复和授权均应被记录。

5.4. 安全审计

a) 防泄密系统应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件（对安全策略中指定文件的所有操作事件）进行审计；

b) 防泄密系统应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；

c) 防泄密系统审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；

d) 防泄密系统应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

5.5. 视频监控文件通信及存储的保密性和完整性保护

a) 防泄密系统应采用保密技术保证数字录像设备与用户终端间通信过程中数据的保密性和完整性。

b) 防泄密系统应采用保密技术保证用户终端存储的视频监控文件的保密性和完整性。

5.6. 视频监控文件的外发应用

a) 防泄密系统应能通过授权，在用户终端将视频监控文件制作成外发数据，并应具有设置密码、时效、编辑、自删除等修改、调整功能；

b) 防泄密系统所制作的外发数据，在时效和权限许可范围内，应无需安装专用软件即可使用；

c) 5G大小的外发文件在标准配置的计算机上打开时间比原始视频文件增加不应超过10秒钟。

5.7. 防泄密系统应能直接与“上海安全技术防范监督管理平台”联网并发送报警信息。