

# 《上海市机构编制实名制信息系统》应用及终端管理

## 保密承诺书

我单位了解《上海市机构编制实名制信息系统》应用及所使用的公务网涉密域接入终端管理有关保密法规制度，知悉应当承担的保密义务和法律责任。现庄重承诺：

- 一、 认真遵守国家相关保密法律、法规和规章制度，履行保密义务；
- 二、 不提供虚假个人信息，自愿接受保密审查；
- 三、 不违规记录、存储、复制国家秘密信息，不违规留存国家秘密载体；
- 四、 认真遵守上海市公务网涉密终端相关保密管理规定；
- 五、 认真遵守《上海市机构编制实名制信息系统》应用及终端管理规定；
- 六、 离岗时，自愿接受脱密期管理，签订保密承诺书。

违反上述承诺，自愿承担党纪、政纪责任和法律后果。

承诺单位（盖单）：

承诺人（签名）：

年 月 日

# 《上海市机构编制实名制信息系统》

## 涉密终端登记表

使用单位 (盖单)		
使用部门		
主要用途		
设备标识		
设备型号		
放置位置		
IP 地址		
MAC 地址		
硬盘序列号		
配置	(操作系统, 电脑名称)	
责任人	联系方式	电话

登记人:

年 月 日

# 《上海市机构编制实名制信息系统》

## 应用及终端管理规定

按照公务网涉密域应用及终端接入管理要求，对于接入《上海市机构编制实名制信息系统》的应用及电脑终端应满足以下规定：

1、接入《上海市机构编制实名制信息系统》的电脑终端，必须部署红黑电源隔离插座、视频干扰器、保密技术防护专用系统（三合一）等防护措施。

2、接入终端的设备型号，设备标识、序列号、配置（操作系统、电脑名称、IP地址、MAC地址、硬盘序列号）、放置位置、单位、部门、使用人、联系方式等必须填写统一的登记备案表，汇总到市编办备案管理，如有变更，需及时上报更新。

3、接入《上海市机构编制实名制信息系统》的电脑终端，必须做到专机、专人、专网、专用，不得混作其他用途，电脑更换或报废前，必须由保密局指定的具有专业资质的单位进行硬盘消磁处理。

4、接入终端必须安装正版的操作系统和杀毒软件，限制安装非工作所必须的软件，操作系统补丁和杀毒软件病毒库至少每周更新一次，有条件的，尽量做到每天更新；禁止安装不明来源，不明用途或者带有木马、黑客性质的软件。

5、为防止终端电脑被非授权访问，必须设置符合安全密码要求的BIOS开机密码和操作系统登录密码，必须定期修改，如发现异常，及时上报核查。

6、终端电脑上，建议停用系统的 Guest 账号，修改默认的 Administrator 账号名称，并且登录时不显示上次登录的用户名；通过修



改组策略或者注册表方式配置终端电脑的“密码策略”、“账户锁定策略”、“审核策略”、“安全选项”等，以尽可能确保系统安全。

7、终端电脑必须安装并开启防火墙，通过修改设置，只开放应用端口，屏蔽所有不用的端口；

8、修改设置，严禁电脑开机后自动登录，必须输入密码才能登录；开启自动屏幕保护功能，进入屏保时间设置为10分钟，并在操作人员临时离开电脑时进行屏幕锁定。人员外出和下班时，电脑要关机。

9、修改浏览器设置，禁用自动保存用户名和密码，设置退出时自动清空浏览器记录。

10、终端操作人员应每天查看系统审计日志，如发现本人不知情的尝试登陆失败或者成功登陆记录，应立即上报、核查，采取必要的预防和处置措施。

11、终端电脑上的重要数据务必及时妥善备份，如发现机器遭破坏，数据失窃等情况，应当及时报告备案，核查处理。

12、严禁使用私人电脑或者单位中未登记备案的电脑终端接入《上海市机构编制实名制信息系统》。