主动公开

上海市浦东新区城市管理行政执法局文件

浦城执法〔2022〕51号

关于印发《浦东城管执法局加强内部工作保密管理的制度》的通知

局机关各处室、生态环境（水务）执法支队，交通执法支队，规划土地执法大队、城管执法支队各大队，各街镇（管委会）中队：

《浦东城管执法局加强内部工作保密管理的制度》已经局长办公会审议通过，下发给你们，请认真贯彻执行。

浦东新区城市管理行政执法局

2022年8月11日

浦东城管执法局
加强内部工作保密管理的制度

第一部分　总则

为进一步提高本单位全体工作人员的保密意识，确保各项内部管理工作更加规范安全，切实将保密工作落到实处，根据《中华人民共和国保密法》、《上海市保密工作暂行规定》等法律法规，按照市、区两级保密相关工作要求，结合本单位工作实际，特制定本制度。

本制度适用于本单位涉密工作及非涉密工作中的保密管理事项两大部分，主要就接收或产生的涉密和非涉密工作文件、材料、储存介质、移动设备，以及本单位建设的信息化网络平台等内容，进一步明确了保密管理的要求。

第二部分　涉密工作的保密管理

一、机构设置及职责

（一）组织架构。

局主要负责人为本单位保密工作第一责任人；办公室主任为直接责任人。执法局设立保密工作领导小组负责保密工作，领导小组办公室设在局办公室，由办公室指定各业务条线保密工作专管员负责日常管理指导。各处室、各直属单位负责人为本部门、

本单位保密工作第一责任人，下面设立保密管理员，负责日常保密管理工作。

（二）保密人员职责。

1. 保密工作专管员。负责各自业务条线日常工作中所涉及到的内部保密管理工作。建立健全各业务条线加强内部保密管理的规章制度，协调、督促各自业务条线内部保密管理，并定期开展自查，对存在问题及时落实整改。

2. 保密管理员。配合保密工作专管员宣传、贯彻执行各类内部保密管理的规章制度。按照具体办理审批流程进行规范办理，对本部门、本单位接收或产生的工作文件、材料、储存介质、移动设备等加强保密管理。

二、硬件设置的要求

根据国家保密部门对于涉密场所及保密要害部门的设备设施管理要求，在涉密场所安装电子监控、防盗、报警等保密安全装置，并在门口设置“禁止带入电子设备”字样。涉密场所调整、搬迁等须向上级保密部门申报，经上级部门现场踏勘审核通过后，由指定集成单位承建专门的计算机涉密网络，并开展日常维护检查。

三、涉密人员的管理

（一）涉密岗位确定。

涉密岗位分为核心涉密岗位、重要涉密岗位和一般涉密岗位。局主要负责人、办公室主要责任人及保密专管员为重要涉密岗位，

其他各处室、各直属单位负责人及保密管理员为一般涉密岗位。

（二）人员审查上岗。

根据涉密岗位，由所在处室、直属单位拟定涉密人员，填写《涉密人员保密审查表》，报政治处进行涉密审核，审核通过后向局办公室报备。局办公室统一组织安排涉密人员开展岗前教育培训，签订承诺书。涉密人员因公、因私出国（境）的，一律按照干部人事管理权限进行审批。涉密人员离岗离职需进行脱密期管理。

四、涉密文件的管理

（一）外单位涉密文件流转。

纸质涉密文件由局办公室机要保密人员统一进行盖章签收，登记造册。涉密公务网流转涉密文件由局办公室机要保密人员按要求登录涉密网络收取。制作文件流转单提出拟办意见后报局办公室负责人审核，审核通过后进行纸质流转，流程过程中落实保密提醒，明确阅件人、归还期限。文件归还后，进行登记归档，放入专门的保密文件铁皮柜，由专人进行保管。

涉密文件不允许外借、复印、传真、扫描、拍照等。如确需复印传阅的，因经过主管领导和保密专管员审核同意，由保密专管员确定复制份数做好登记后方可印制流转。

（二）本单位涉密文件制发。

经办部门需提前向保密领导小组报批，由局主要负责人或指定人员进行定密，指定专人在涉密计算机上进行起草，经主要领

导审核签发后由局办公室机要保密人员负责印发，通过机要交通方式寄送至相关部门。本单位存档登记，放入专门的保密文件铁皮柜，由专人进行保管。

（三）涉密文件清退销毁。

根据上级保密管理部门要求，每年度盘查保密件收发情况，区级保密件全数清退。本单位按要求线上签收并印制的涉密文件材料，原件及签发单留存归档，复议件梳理后装入保密袋中封口保存，由区保密办组织统一销毁。所有涉密文件材料不得擅自销毁。

五、涉密设备的管理

（一）涉密设备的登记备案。

涉密计算机、多功能一体机等办公自动化设备，以及涉密移动存储介质，须由专人负责，实行统一编号管理，在设备指定位置贴上相应的密级标识，并做好登记备案。

（二）涉密设备的使用管理。

涉密计算机、多功能一体机等办公自动化设备仅供专职保密人员使用，使用时制作专门的使用登记手册，做到详细记录，包括使用时间、使用人、使用内容、印制份数等。

涉密移动存储介质应由涉密人员集中管理。使用时，须核查使用人员的身份与权限，办理申请登记手续，由保密专管员落实保密教育提示，明确保管要求、归还期限等。临时借用的，使用完毕必须及时归还。

（三）涉密设备的维修销毁。

涉密设备、移动存储介质的维修，应由本单位计算机专业技术人员进行操作，如需外送维修的，因报保密工作领导小组办公室审批同意后，到上级保密部门指定维修点进行维修。涉密设备、移动存储介质的维修应保证所有存储信息不被泄露。

涉密设备、移动存储介质需要报废销毁的，需报保密工作领导小组审批同意，由保密专管员负责信息清除，并由两名保密工作人员同时押送至保密工作部门指定的销毁点进行现场销毁。任何人不得擅自销毁。

（四）涉密设备禁止事项。

涉密计算机等办公自动化设备不得与互联网或其他非涉密网络相连，使用过程中禁止连接各类非涉密存储介质。

第三部分　非涉密工作的保密管理

一、内部文件资料的管理

（一）内部文件资料的保管销毁。

本单位各部门、各直属单位自行起草产生的非涉密内部文件、音视频资料等，由各部门、各单位按照对应的上级条线规定自行管理保存，对涉及敏感信息的材料由专人专管。局办公室将根据区委保密办安排，每年对各部门纸质内部文件资料进行统一收集销毁。

（二）内部文件资料的借阅。

内部文件借阅，主要指档案资料，包括文书档案、财务档案、人事档案、案卷档案等，根据不同条线档案室的保密管理要求落实查阅管理，制定相应查阅规范。查阅文件资料需经管理部门负责人审核通过，登记好借阅人、借阅期限、借阅用途等。如借阅涉及个人隐私等敏感信息的文件材料的，同时还需要求借阅人员签订保密承诺书，做好保密提示。

二、非涉密设备的管理

（一）非涉密设备的备案管理。

非涉密计算机等办公自动化设备应按照固定资产管理规定进行统一的登记备案管理，在设备指定位置贴上二维码标识，标明资产名称、标号、部门及管理人，设备实际使用人为设备保管的第一责任人。

用于存储内部工作信息的移动存储介质由实际使用人进行保管。单位所属设备应做好登记备案，私人存储设备在存储内部工作信息完毕后应及时清除信息，防止信息外泄。

（二）非涉密设备的维修销毁。

非涉密设备、移动存储介质的维修，为有效防止信息外泄，参照非涉密设备的维修办理流程。存储过内部工作信息数据的设备、移动存储介质在报废销毁前，应及时转存有用的数据，后通过消磁、物理粉碎等方式进行销毁。

（三）非涉密设备的禁止事项。

非涉密计算机等办公自动化设备、移动存储介质只能用于非涉密信息的处理、存储，不得处理、传递、存储涉密信息。

三、网络与平台数据的保密管理

（一）网络安全的维护管理。

本单位使用的内部网络为新区政务外网，由指定的专业技术人员专门负责日常技术维护，配备系统管理员，负责制定网络设备策略，对网络设备、服务器进行维护、管理，并负责紧急情况下政务外网运行。

（二）平台数据的安全管理。

本单位系统内建设的各类数字化信息平台，包括城管执法业务综合管理平台、城管执法综合指挥平台、浦东城管智能综合信息平台等，须指定专人负责数据信息的安全管理，并制定相应的管理规范（详见附件）。

一是针对平台数据信息，通过角色设定分级开展权限管理，强化保密安全审查流程环节，对各角色人员进行保密教育，确保信息数据安全。

二是针对端口应用安全，增设个人账户浏览记录查询、设置水印，对当事人身份信息等敏感信息的查阅设置审核授权流程。

三是针对设备终端安全，落实专人进行维护、维修，在机房设置出入管理、视频监控等，严格控制人员和设备进出机房。

四、公开信息保密审查的管理

（一）建立保密审查制度。

各处室、各直属单位指定专人，负责本部门、本单位对外公开信息的保密审查工作，并做好记录。若涉及若干单位的，由主办单位牵头进行审查；多部门联合共同负责的分别进行审查。

一经发现公开信息存在涉密情况的，因立即上报局保密领导小组，并采取及时补救措施。

（二）禁止公开信息的范畴。

一是涉密信息，凡是标有绝密级、机密级、秘密级的文件信息不得公开；二是涉及国家安全、稳定的敏感信息不得公开；三是标有“内部文件”等字样的信息不得公开；四是涉及商业秘密、企业及个人隐私信息的内容不得公开；五是其他可能产生舆情等的敏感信息不得公开。

五、社交软件规范使用的管理

（一）禁止发布的内容。

一是不得发布涉密信息及禁止公开的信息内容；二是不得发布传输、泄露尚未公开的文件资料、重要决策事项等内容；三是不得制造、传播、扩散不利用国家安全稳定的消息和谣言等；四是不得转发、谈论低级庸俗、封建迷信、违背良知的内容及其他严重违反社会公德、职业道德的内容等；五是其他容易引发社会公众争议，造成社会不稳定的内容等。

（二）社交软件群的管理。

1. 建立群组的规定。因工作需要建群的，系统内原则上通过企业微信建群；其他社交软件建群的需经过部门负责人同意，并

向局办公室统一报备登记。系统外工作群组，原则上只允许针对专项工作建立临时微信群，群内仅发布与该项工作相关的内容，工作结束后非必要不保留群组。建群时如涉及人员和工作内容高度重合的，建议合并群组使用。

2. 群组管理的要求。各群组严格遵守《保密法》规定，不该发布的不发布，坚决做到“涉密不上网、上网不涉密”。群管理员为该群组的主体责任人，须及时保密提醒，对本群组人员及群内发布的信息内容开展监督管理，一旦发生泄密负主要责任。

第四部分 保密工作的考核和奖惩

本制度中所涉及的保密工作将纳入各单位的绩效考核扣分项。对个人违反保密制度规定的，根据情节轻重，给予纪律处分；构成犯罪的追究刑事责任。因单位管理责任未落实到位的，追究单位的责任。

本制度自印发之日起执行。

附件：浦东城管执法局平台数据信息安全规范

浦东新区城市管理行政执法局办公室　　2022年8月11印发

(共印51份)

附件

浦东新区城市管理行政执法局
平台数据信息安全规范

为保障浦东城管执法局信息化工作的有序开展，有效保护全系统数据信息资产，根据《中华人民共和国网络安全法》等国家法律法规，结合本单位实际情况，制定本规范。通过实施策略、规范、流程和技术等控制措施，保护全系统数据信息的机密性、完整性和可用性。

一、适用范围

本规范适用于浦东城管执法系统各类数字化信息平台，包括但不限于城管执法业务综合管理平台、城管执法综合指挥平台、浦东城管智能综合信息平台等的功能开发设计、数据使用分析及平台运行维护等环节。

二、角色设定

（一）城管系统

1. 系统综合管理员

局系统管理员权限配置对象为局指挥中心平台管理人员，拥有全局在数据处理、分析、下载及权限调整等层面最高权限。

2. 业务系统管理员

业务管理员权限配置对象为局各处室主要业务模块负责人，拥有对相应业务模块的全部管理权限，其权限配置需要由系统综合管理员进行授权获得。

3. 中台管理员

中台管理员权限配置对象为支（大）队及其中（分）队、街镇（管委会）中队平台管理人员，可对系统内数据进行线上编辑及申请导出权限，其权限配置需要由局系统管理员进行授权获得。

4. 执法队员

执法队员权限配置对象为全体城管执法系统正式队员，拥有管理范围内所有对象的编辑、检查、查处等权限，其权限配置需要由局系统管理员进行授权获得。

（二）外聘人员

1. 信息员

信息员权限配置对象为指挥中心指挥组审核人员，拥有对智能工单初审权限，其权限配置需要由局系统管理员进行授权获得。

2. 辅助队员

辅助队员权限配置对象为各街镇（管委会）中队执法辅助人员，其权限仅限于对沿街商户的街面秩序检查及疫情防控检查事宜，其权限配置需要由中队中台管理员进行授权获得。

（三）技术团队

技术人员根据保密协议规定对浦东城管执法系统数据进行归集处理，对外数据互联互通由单一技术负责，其他技术公司不得私自存储、导出数据。

三、应用安全

1. 手机端查看相关数据信息时，手机号隐藏中间 4 位、身份证号只显示前 3 位和末 4 位，页面内标注使用人员信息水印。

2. 电脑端查看相关数据时均标注水印: 内部信息-队员姓名，且电脑端无法选中相关信息并进行复制。

3. 申请下载的所有数据信息应当通过线上申请，并填写申请原因、数据用途等信息，局指挥中心应当把严数据申请审核工作。

4. 因统计分析、执法监管等工作需要申请使用含有敏感信息的数据，申请单位应明确使用期限和范围，以及是否对敏感信息进行脱敏处理。同时，要求数据使用单位按规定的范围使用，并在到达使用期限前删除；遵循“谁使用谁负责、谁使用谁销毁”的基本原则，数据持有者和使用者必须在权限范围内合法使用数据，不得泄漏或非授权使用。

四、终端安全

1. 设备现场维护、维修，应有执法局相关负责人员现场陪同，以防止其不正常的信息记录、提取，以及私自加装软件等行为。

2. 设备外送维护、维修，应通过拆除存储介质、消磁处理

或执法局相关负责人员在场监督等形式确保信息安全。

3. 应采取必要的控制措施，对人员和设备等进出机房进行管理和控制，包括但不限于人员和设备的出入管理、门禁管理、视频监控管理等。

五、系统安全

1. 各信息化平台应设置防火墙安全策略，策略需要考虑隔离病毒传播、非授权访问的通道等方面的内容，相关策略应注明用途，避免冗余策略的产生;

2. 按照不同的访问权限，在核心服务器、交换机设置不同的访问控制策略;

3. 主责部门协同技术保障团队不定期对服务器进行安全扫描，针对发现的漏洞及时补漏加固。

4. 移动存储设备(优盘、移动硬盘等)必须进行病毒扫描，确认无毒后，方能接入服务器;

5. 各应用系统管理员登录密码应遵循密码复杂度原则，按照数字、字母、符号组成的原则进行设置且位数不应少于 8 位;

6. 管理人员应定期查看各应用系统、终端操作系统相关安全公告，根据需要下载操作系统相关补丁安装包，进行测试后对服务器进行升级;

7. 禁止在机房服务器上安装与系统应用无关的软件并且安装软件要确认安装包的安全性，安装和卸载软件应做好相应记录;

8. 系统使用人员应定期对所配备的计算机终端的操作系统、杀毒软件等进行升级和更新，并定期进行病毒查杀;

9. 系统使用人员应妥善保管根据职责权限所掌握的各类办公账号和密码，严禁随意向他人泄露和借用;

10. 经远程通信传送的程序或数据，必须经过安全检测确认无病毒后方可安装和使用;

11. 定期组织系统故障应急演习，提高相关管理人员的应急反应能力，确保恢复过程安全、迅速和有效;

12. 重大节假日之前，相关人员应对网络、各应用系统进行巡检，确保节假日期间网络和各应用系统运行安全、稳定和有效。

六、存储安全

1. 存储数据的设备（包括存储介质）及系统平台在使用期间，应安装防病毒服务器等设备确保数据库及系统安全。

2. 存储数据的设备（包括存储介质）在闲置报废前，应对数据进行转存后，通过消磁、物理粉碎等方式销毁介质。

3. 应通过备份、镜像存储等办法确保数据库及系统的完整性，防范危及数据完整性的事件发生。

七、事故分类

1. 高危事故

因命令注入、远程命令执行、上传获取 WebShell、SQL 注入、缓冲区溢出、绕过认证直接访问管理后台、核心业务非授权

访问、核心业务后台弱密码等原因导致无关人员直接获取系统权限（服务器端权限、客户端权限）或者导致严重级别的信息泄漏。

2. 中危事故

因存储型 XSS 漏洞、客户端明文密码存储等导致用户身份信息被盗或者导致普通级别的信息泄漏。

3. 低危事故

因反射型 XSS（包括反射型 DOM-XSS）、JSON Hijacking、CSRF、路径信息泄露、SVN 信息泄露、phpinfo 等导致轻微信息泄露。

八、责任追究

1. 数据信息安全管理工作纳入各单位的绩效考核扣分项，对城管执法系统内个人违反数据安全管理制度规定的，根据情节轻重，给予纪律处分；构成犯罪的追究刑事责任。因单位管理责任未落实到位的，追究单位的责任。

2. 外聘平台信息员根据系统权限进行智能工单审核工作，对因审核工作不严不实造成不良影响将根据情况通报服务提供方予以责任人员予以扣发绩效、年度考核扣分直至解聘，构成犯罪的追究刑事责任。

3. 执法辅助人员根据赋予权限辅助开展执法检查工作，不得超越权限进行涉密数据处理，对因越权行为造成不良后果者，将建议所属单位予以扣发绩效、年度考核扣分直至解聘，构成犯罪的追究刑事责任。

4. 技术公司应严格遵守保密协议，做好城管执法系统内数据归集、处理工作，对因技术漏洞、人为泄密导致高危事故造成严重后果者将采用“一票否决”，取消合作关系，构成犯罪的追究责任人刑事责任。