电子政务外网信息系统管理制度

信息系统使用授权、审批制度

第一条　本规定所称信息系统是指终端设备利用计算机通信网络技术进行信息采集、处理、存贮和传输的设备、技术、管理的组合。嘉定区电子政务外网信息系统包括内部计算机信息系统——处理嘉定区内部日常办公的专用信息网络或单机，简称政务网；外部信息系统——连接因特网的单机，简称外网。

第二条　建立、使用政务网计算机信息系统必须实现与外网的逻辑隔离，政务网下连单位不得通过其他任何途径接入国际互联网和其他计算机网。

第三条　未经批准的计算机一律禁止私自联通社会公共网。要求开通国际互联网应向有关部门申请，审批。联入互联网的计算机，严禁处理涉密信息。

电子信息共享管理制度

第一条　政务网信息系统禁止直接通过客户端进行文件共享，所有的文件共享均应通过文件服务器进行。

第二条　政务网信息系统中的每个用户都设有独立的帐号。政务网信息系统将对帐号进行统一管理，根据一定的要求设置分组。如人员发生变更，（岗位调动，调离）应及时通知系统管理员更改分组。分组信息应进行登记备案。

第三条　为方便操作，在文件服务器中将设置各类预设访问控制目录，如处室文件共享目录、各室之间文件交换等各类共享目录。非涉密信息可以直接复制到相应的目录中进行共享使用。

第四条　政务网信息系统访问授权需要经过处室领导审批，应填写涉密信息系统联网及访问授权审批单，（审批程序和审批表见附表 2.1、2.2），交由信息中心执行相应的授权管理工作。

计算机机房管理制度

第一条　本管理规定所称的机房坐落于上海市博乐南路 111 号 410 室。

第二条　信息化委员会负责计算机系统的运行、维护和管理工作。

第三条　计算机系统的运行、维护和管理人员（以下简称机房工作人员），应经计算机知识及安全保密方面的相关培训，考核合格后方可上岗工作。

第四条　各处室计算机管理员负责和机房工作人员的联络，并具体负责本处室计算机设备的报修及相关事宜的登记工作。

第五条　非机房工作人员，未经批准，不得随意进入机房或操控机房设备，进入机房应进行相关的登记。

第六条　机房工作人员应严格遵守操作规程，安全操作，注意爱护设备，定期检查、保养和保持清洁，使设备处于良好状态。

第七条　机房工作人员应做好日常维护、管理的相应记录，并定期归档。

第八条　做好机房设备，包括硬件、软件、网络、媒体和介质使用登记工作。

第九条　外来的设备维修人员进入机房工作，必须在机房工作人员的陪同下进行维修维护工作，机房工作人员应做好登记记录工作。

第十条　为防止磁记录的破坏，机房内不准使用磁化杯、收音机等产生磁场的物体。

第十一条　机房温度应保持在 22~24 摄氏度，相对湿度保持在 50~60%，电压 220 ±5%，电流≤40A。

第十二条　机房工作人员应做好机房清洁工作，保证机房清洁明亮。

第十三条　机房工作人员应遵守工作纪律，严格按照已制订的信息管理制度执行。

第十四条　发现异常应及时上报，处理完毕需要填写汇报处理单。

计算机病毒防治管理制度

第一条　为了加强对嘉定区计算机信息网络系统的管理，更有效地防止计算机病毒侵害，确保嘉定区计算机及网络系统正常运行，特制定本制度。

第二条　本制度所称的计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

第三条　嘉定区范围内计算机信息系统、联网的计算机（包括公务网计算机）、以及未联网的计算机的计算机病毒防治管理工作，均适用本制度。

第四条　嘉定区信息化委员会负责主管嘉定区的计算机病毒防治工作，机房负责计算机病毒防治中的技术支持工作。

第五条　任何处室和个人不得有下列传播计算机病毒的行为：
（1）故意输入计算机病毒，危害计算机信息系统安全；
（2）向他人提供含有计算机病毒的文件、软件、媒体；
（3）其他传播计算机病毒的行为。

第六条　机房工作人员会各处室有关人员采取计算机病毒安全技术防治措施，统一部署防病毒软件，定期升级这些软件的病毒定义码，建立病毒防范软件资料库。

第七条　各使用人员不得随意在计算机上使用外来软盘、光盘和u盘等移动介质，尤其严禁使用游戏盘，凡确因业务需要使用外来移动介质的，必须先进行病毒检测，杀灭工作，方可进入计算机和网络系统运行；在接收电子邮件时不要随意打开邮件附表，以防外来病毒侵害。

第八条　各处室和个人不得私自从计算机信息网络上下载程序，确与业务有关需要下载时，应当报经处长审核同意，并进行计算机病毒检测后方可下载。

第九条　各处室对本处室重要业务资料、信息应及时做好两种以上介质的备份工作，防止因病毒发作导致信息丢失。

第十条　各处室制作多媒体时、或者向其他处室和部门提供文档和使用的各种移动介质，都应该进行病毒的查杀，绝对不允许数据带毒复制。

第十一条　信息化委员会会机房工作人员对计算机系统使用人员进行病毒防治教育和培训。

第十二条　违反以上制度造成外来病毒引起计算机或网络系统故障的，信息化委员会将根据《中华人民共和国计算机信息系统安全保护条例》、《计算机病毒防治管理办法》，除按规定处罚外，另责成当事人或当事人所在处室负担机器和网络修复所需费用并承担相应行政责任。

数据备份与恢复制度

第一条　为了保证嘉定区计算机信息网络系统中的数据安全，使得在计算机系统失效或数据丢失时，能依靠备份尽快地恢复系统和数据，保护关键应用数据的安全，保证数据不丢失，特制定本制度。

第二条　本制度所指的数据包括系统数据和业务数据，所涵盖的备份与恢复技术包括服务器热备和移动介质备份。

第三条　拥有重要系统或重要数据的处室应该建立数据备份系统和数据备份制度，防止系统、数据的丢失；涉及数据备份和恢复的处室要由专人负责数据备份工作，并认真填写备份日志。

第四条　要做好机房主机系统的数据备份工作，增量备份每天做，系统备份三个月做一次。

第五条　备份数据应该严格管理，妥善保存；备份数据资料保管地点应有防火、防热、防潮、防尘、防磁、防盗设施。

第六条　一旦发生数据丢失或数据破坏等情况，要由负责人员进行备份数据的恢复，以免造成不必要的麻烦或更大的损失。

（1）全盘恢复一般应用在服务器发生意外灾难导致数据全部丢失、系统崩溃或是有计划的系统升级、系统重组等；

（2）个别文件恢复一般用于恢复受损的个别文件，或者在全盘恢复之后追加增量备份的恢复，以得到最新的备份。

技术文档管理

第七条　技术文档是指对系统设计研制、开发、运行、维护中所有技术问题的文字描述，它反映了系统的构造原理，表示了系统的实现方法，为系统维护、修改和进一步开发提供了依据。

第八条　技术文档依照涉密载体的有关规定设定密级。

第九条　借阅、复制技术文档要履行相应的手续，包括申请、审批、登记、归档等必要环节，并明确各环节当事人的责任和义务。

第十条　对重要技术文档应当进行双份以上的备份，并存放于异地。

安全设备管理制度

第一条　为了正确恰当地对安全设备进行配置和管理，使安全设备真正发挥功能和作用，特制定本制度。

入侵检测及防火墙等安全设备

第二条　安全管理员负责对入侵检测及防火墙等安全设备进行配置和部署，除安全管理员之外的其他人员不应具有对安全设备的访问权。安全管理员的职责必须与系统管理员和保密员分离，并由不同人担任。

第三条　安全管理员必须具备熟练的网络知识和相应的安全设备知识，并且要定期接收业务知识的培训，能对入侵检测及防火墙等安全设备进行正确的配置和适当的管理。

第四条　安全设备必须做好防火、防热、防潮、防尘、防磁、防盗各方面的物理安全防护。

第五条　安全管理员应该尽量通过与入侵检测及防火墙主机物理连接（使用串口直接连接）的终端对其进行管理。

第六条　当需要通过对安全设备的远程访问来进行管理时，必须使用严格的用户认证手段和访问控制，任何情况下都不允许通过不可信任的网络来对入侵检测及防火墙实施远程访问。远程连接应该使用专用客户端程序或者经过加密技术的连接，以防窃听。

第七条　安全管理员应该根据安全策略配置安全设备，并且应该每月定期检查其配置。

第八条　安全设备的配置如果需要更改，应由安全管理员提交申请，经主管安全保密工作的领导批准后方可实施，配置的更改必须留有系统日志备查。附表 9.1

第九条　安全设备的访问清单和配置规则每月应该以报告的形式提交主管安全保密工作的领导审查。

第十条　入侵检测及防火墙（系统软件、配置文件、数据库文件等）必须进行周期性的备份，以防备系统失败时进行恢复，后备文件应该安全的存储在只读介质中，以防不慎覆盖，并且锁定只允许适当的人员访问该介质。

第十一条　安全设备如遇故障，应立即通知厂商报修。

审计系统

第十二条　按照系统的使用手册正确地使用审计系统，对被审计主机的信息要进行及时的整理。

第十三条　审计中心管理员应每天确定客户端的登陆数量，对未登陆用户情况进行确认，发现不安全因素因及时排除。

第十四条　屏幕信息审计做到工作时间内完全审计，非工作日对重点保密机器也要进行屏幕审计，具体情况视存储工具确定。

第十五条　键盘审计、网络连接审计、拨号审计必须全天使用，并周期性对数据进行备份。

第十六条　对需要进行拨号上网的计算机需进行登记，由网络管理员根据实际情况分配拨号时间和拨号号码，并对该用户拨号上网的日志进行记录。

第十七条　对需要进行文件保护的用户，需进行登记，由保密员对需要保密的文件进行保护，并对文件的流向进行管理。需要解除文件保护限制的用户，需进行登记，保密员每周对已经保护的文件进行汇总，并向上级汇报。

第十八条　对屏幕信息的审计要做到每周分析，对保存数据周期性进行备份，具体周期视存储工具确定。并保障备份资料保密性，对网络中存在的不安全因素及时排除。

第十九条　对键盘、网络连接、拨号连接审计做好备份，对备份的文件信息要做好安全保密工作，确保专人管理。

第二十条　审计软件周期性在有关产品提供商指导下进行升级。

第二十一条　审计系统的审计日志及其他系统自身的审计日志要定期检测，一般为每天，系统管理员检查后要有记录文件（附件 9.2）,每天分析日志是否有异常情况。

第二十二条　文件保护功能要专人负责，系统管理员和日志管理员应设置不同人员。

第二十三条　泄密事件发生时，通过审计方式再现的泄密当时的情况，分析泄密情况，确定损失，并及时向上级汇报。

CA 认证系统

第二十四条　CA 系统由安全管理员与保密管理员分别进行管理。

第二十五条　安全管理员负责系统的设置与维护工作。

第二十六条　保密管理员负责 USBKey 的发放管理工作。

第二十七条　USBKey 的发放、补发应经过部门领导批准，由信息中心保密管理员负责发放。

第二十八条　安全管理员，保密管理员应妥善保管好个人的 USBKey，不得私自外界，如遗失应立即汇报，经领导批准，进行 USBKey 的重新发放工作，发放工作应在安全管理员、保密管理员、信息中心领导同时在场时进行。

第二十九条　USBKey 应统一进行购置，并进行编号，登记。

第三十条　空白的 USBKey 与暂时存放于带密码的文件柜中。

第三十一条　个人应妥善保管好 USBKey。

第三十二条　如发生USBKey遗失或损坏，应立即上报部门领导，并填写补发申请单，经部门领导、保密委员会批准后方可进行补发工作。

第三十三条　补发完成后应由安全管理员与系统管理员进行黑名单发布以及应用系统配置修订工作。