**XXX单位**

**保密管理制度**

V1.0

20XX年XX月XX日

目录

[1 目的 1](#_Toc479443468)

[2 适用范围 1](#_Toc479443469)

[3 敏感信息管理 1](#_Toc479443470)

[4 涉密信息管理 2](#_Toc479443471)

[5 附则 4](#_Toc479443472)

# 目的

为确保XXX单位网络和信息安全，保护系统内信息不被非授权的浏览、复制、传播、篡改或破坏，保证各应用系统的正常运行和各项业务的正常开展，特制定本管理制度。

# 适用范围

本制度适用于XXX单位内部所有人员和外部所有参与信息化项目的单位和个人。

# 敏感信息管理

（1）信息化项目的“敏感信息”可分为以下三级：核心级、重要级、一般级三类。

核心级，涉及信息化建设的核心技术信息和业务信息，泄漏会使国家和利益造成严重损失。如：内部文件、业务数据、财务信息、人事信息、项目谈判、合同、设计文档、网络架构、安全策略、配置信息以及其他内部保密信息等。

重要级，涉及信息化建设和业务的重要信息，向外扩散有可能对利益造成损害，如规章制度、标准化程序文件、计算机软件或程序、需求文档、测试文档、实施文档、软硬件配置、项目过程文档、培训信息以及其它不为公众所知悉的信息等。

一般级，不涉及信息化建设核心和业务的信息，公开不会对利益造成损害的一般性信息。

（2）内部人员和所有参与信息化建设的单位和个人均有责任和义务对信息化“敏感信息”进行保密。

（3）内部和参与信息化建设的单位和个人应建立信息保密管理员制度，保密管理员由与合作单位项目负责人担任，负责项目全过程的信息保密管理工作，对项目涉及所有信息的产生、传播、存储和使用进行监督检查，并负责项目相关信息的移交归档，以及项目完成后的监督销毁等。

（4）内部人员在授权范围内，具有浏览、复制、传播和存储信息化“敏感信息”的权利，但不得对外泄漏核心和重要信息。

（5）参与信息化建设的单位和个人应将所有参与项目人员及其背景资料向备案，并确保人员诚实可靠。如有人员调离，应主动向\*项目负责人汇报，并做好工作的交接及离岗时文档的清理和脱密工作。

（6）参与信息化建设并经过备案的单位和个人应对 “敏感信息”严格保密，未经\*正式许可或授权，不得浏览、复制、传播、篡改或破坏 “敏感信息”，不得以任何形式向第三方泄漏 “敏感信息”，同时接受\*保密管理员的监督和各项技术手段的监控。

（7）信息化项目验收应包含信息保密验收，对合作单位在信息化项目的所有过程文档的产生、传播、存储和使用是否保密进行评判，对存在“专有信息”遗失或失、泄密事件的项目合作单位验收不予通过。

（8）核心和重要信息原则上不得通过互联网传输，确需通过互联网传输时应采取加密措施，并在传输完成后及时清除。

（9）参与信息化项目的单位应签订《保密协议》，并严格遵守该协议。如违反《保密协议》，造成信息化项目“专有信息”遗失和失、泄密事件将依法追究有关单位和个人的责任。

# 涉密信息管理

（1）涉及国家秘密的计算机，不得直接或间接地与互联网或其它公共信息网络相联接，必须实行物理隔离。

（2）涉及国家秘密的信息，不得在上互联网的计算机中存储、处理、传递。

（3）使用电子邮件进行网上信息交流应遵守国家有关保密规定，不得利用电子邮件传递、转发或抄送国家秘密信息。对于对外提供邮件服务的服务器，应当明确保守国家秘密的要求。

（4）任何单位或个人不得在信息网络中发布或谈论涉及国家秘密的信息；当发现信息网络中有涉及国家秘密的信息时，应当立即向省局保密委员会报告；任何人不得再通过计算机信息网络国际互联网继续转贴、扩散、传播国家秘密信息。

（5）实行保密领导责任制，发布信息应按照信息内容归口管理，分级负责，规范信息保密审查制度，防止国家秘密信息泄露。

（6）在网络上编发信息的部门，要根据省局有关的保密文件，确定需要保密的信息内容、划分编发等级、明确信息提供范围。凡向国际互联网的站点提供和发布信息，应严格杜绝涉密信息发布。对于信源单位已提出保密要求的信息，信息编发部门要严格按照信源单位提出的保密要求和提供范围提交本单位保密部门确定网上编发级别及编发与否；对于未明确密级但内容涉密的信息，要根据有关的保密规定，由本单位保密部门确定编发级别及编发与否；对有涉密嫌疑又来源不明的信息不予编发。

（7）凡以提供网上信息服务为目的而采集的信息，除在其他新闻媒体上已公开发表的，组织者在上网发布前，应当征得提供信息单位的同意；凡对网上信息进行扩充或更新，应当认真执行信息保密审核制度。

（8）凡在网上开设电子公告系统、聊天室、论坛、网络新闻组的单位和用户，应报省局保密委员会审批，明确保密要求和责任。任何单位和个人不得在电子公告系统、聊天室、论坛、网络新闻组上发布、谈论和传播国家秘密信息。

（9）面向社会开放的电子公告系统、聊天室、论坛、网络新闻组，开办单位或其上级主管部门应认真履行保密义务，建立完善的管理制度，加强监督检查。发现涉密信息，应及时采取措施，并报告省局保密委员会及当地保密工作部门。

（10）在信息网络上存储和传输的信息，分清涉密和非密的性质。需要在网络上存储、传输的涉密信息，应遵守有关的保密要求，报请本单位保密部门审批。

（11）绝密及机密级信息不得网络上（包括外部互联网以及内部办公网）传输，秘密级信息不得在外部互联网传输，如需要在内部网络上传递，应报请本单位保密部门审批，并在传递的双方同时使用涉密计算机。

（12）网络上的数据库内容涉及保密的数据资料时，要在数据库设计时就提出保密要求和调用权限，并进行安全保密设计。如果委托其它单位设计，须由设计单位提供源码程序，经安全保密认证并进行保密设置后方可入网运行。

（13）信息使用、加工处理部门及网络管理部门，不得通过不正当的手段，超越权限查看、使用、复制保密信息，也不能擅自降低保密级别，把涉密信息作为非密信息传播。

（14）涉及国家秘密的计算机信息网络的建设，必须严格按照中共中央保密委员会办公室和国家保密局的要求，报经有关保密部门审批后，方可投入使用。涉密网络建设和运行，必须有技术上的安全和保密控制措施，拒绝未经授权的访问。

（15）计算机网络用户的口令和采取的安全措施，属于秘密级事项；有调阅机密内容权限的用户口令和网络系统级口令及安全措施属于机密事项。

# 附则

本文件由XXX单位信息中心负责解释与修订。

本文件自颁布之日起发布执行。