|  |  |
| --- | --- |
|  |  |

|  |
| --- |
| XX单位  资产安全管理制度 |

20xx年xx月目录

[1 总则 3](#_Toc373060025)

[1.1 目的 3](#_Toc373060026)

[1.2 范围 3](#_Toc373060027)

[2 规范性引用文件 3](#_Toc373060028)

[3 职责 3](#_Toc373060029)

[3.1 信息中心 3](#_Toc373060030)

[3.3 其他各科室 3](#_Toc373060031)

[4 术语与定义 3](#_Toc373060032)

[4.1信息 3](#_Toc373060033)

[4.2 资产 3](#_Toc373060034)

[5 管理内容和方法 4](#_Toc373060035)

[5.1 资产清单 4](#_Toc373060036)

[5.2 资产管理 4](#_Toc373060037)

[5.3 信息资产的存放和使用 5](#_Toc373060038)

[5.4信息资产分类 6](#_Toc373060039)

[5.5信息的标识及处置 7](#_Toc373060040)

[5.6资产转移 8](#_Toc373060041)

[5.7资产数据安全管理 8](#_Toc373060042)

[6 附则 8](#_Toc373060043)

[7 附表 8](#_Toc373060044)

# 1 总则

## 1.1 目的

为了规范XX单位网络与信息系统的信息资产管理，明确各种岗位的信息资产管理职责，方便在XX单位内部推广和执行信息资产的管理和使用要求，特制订本制度。

本细则描述了XX单位信息中心在信息资产管理方面的职责、管理内容和管理方法。

## 1.2 范围

本细则适用于XX单位信息中心所有信息资产的管理。

# 2 规范性引用文件

GB/T 22081-2008/ISO/IEC 27002:2005《信息技术 安全技术 信息安全管理实用规则》

# 3 职责

## 3.1 信息中心

（1）负责所有信息资产的管理工作。

（2）负责制作和维护所管辖系统的信息资产管理清单。

（3）负责审核各个科室的信息资产变更。

（4）定期对信息资产进行清查盘点。

## 3.3 其他各科室

（1）负责维护本科室的信息资产清单。

（2）负责审核本科室信息资产的变更管理。

（3）协助信息中心进行信息资产清点工作。

# 4 术语与定义

## 4.1信息

对组织具有重要价值，可以通过媒体传递和存储的一种资产。

## 4.2 资产

本程序所称的资产指是指XX单位在生产、经营和管理过程中，所需要的以及所产生的，用以支持（或指导、或影响）XX单位生产、经营和管理的一切有用的数据和资料等非财务的无形资产，其范围包括现在的和历史的。

# 5 管理内容和方法

## 5.1 资产清单

5.1.1 资产清单可帮助确保有效的资产保护，编制一份完整的资产清单是风险管理的一个重要的先决条件。XX单位信息中心应制定和维护所管辖的资产清单，清单中应包括如下与信息系统相关的资产：

（1）信息资产：数据库和数据文件、合同和协议、系统文件、研究信息、用户手册、培训材料、操作或支持程序、业务连续性计划、应变安排 （fallbackarrangement） 、审核跟踪记录（audit trails） 、归档信息；

（2）软件资产：应用软件、系统软件、开发工具和实用程序；

（3）物理资产：计算机设备、通信设备、可移动介质和其他设备；

（4）服务：计算和通信服务、公用设施，例如，供暖，照明，能源，空调；

（5）人员：与信息安全相关的重要人员，如信息系统管理岗位人员、应用集成岗位人员、局域网及终端管理岗位人员、数据管理岗位人员、资产管理岗位人员等。

（6）无形资产：如组织的声誉和形象、商标、知识产权等。

5.1.2资产清单中应包括资产责任科室、责任人、重要程度、所处位置、安全分类、保存方式、使用方法等内容。

## 5.2 资产管理

5.2.1资产责任人

XX单位在资产管理过程中，应将一组资产指派给一个责任人，与信息处理设施有关的所有信息和资产应由组织的指定科室或人员承担责任，资产责任人应负责：

（1）确保与信息处理设施相关的信息和资产进行了适当的分类；

（2）确定并周期性评审访问限制和分类，要考虑到可应用的访问控制策略。

5.2.2新资产必须进行入库登记接收，明确资产接收人、责任人、时间等信息；

5.2.3资产应明确其所有者、管理者及使用者三类角色，对于每一个资产必须有且仅有一个所有者角色，同时必须有且仅有一个管理者角色。

5.2.5 任何对网络与资产的变更、访问应在获得资产责任人的批准后进行。

5.2.6 所有需要接入XX单位信息网络的设备，应经信息中心审核、备案。

5.2.7 随机资料、软件等应由使用者或资产责任人妥善保管，重要的专用驱动程序应有备份。

5.2.8 XX单位信息中心应定期对资产进行清查盘点，确保资产帐物相符和完好无损。

5.2.9 资产的报废应由使用科室提出书面申请，信息中心根据资产的使用情况进行审核，提出资产报废清单，按固定资产报废程序办理。

## 5.3 信息资产的存放和使用

5.3.1信息资产的存放应立足于管理和安全的考虑，为了便于保管、提取、查询，信息资产应尽量以电子介质的形式存储，因此，对于存储在纸介质等其他非结构化的信息资产，如果技术上允许并且有必要的话，应及时进行适当的处理，转换为结构化的电子信息，并以电子介质的形式存储。资产具体存放形式参见（附件1）《信息资产的存放形式表》。

5.3.2 信息资产的存储介质存放的地点要求如下：

（1）对于对外公开信息，存放地点没有要求。

（2）对于对内公开信息，如果是结构化的电子信息，应存放在内部服务网络中的文件服务器等；如果是非结构化的其他信息，应存放在室内文件柜中，并有明显的分类标识。

（3）对于秘密信息，如果是结构化的电子信息，应存放在有严格管理制度、具有足够的安全防护措施的机房环境中的相关服务器和存储设备上；如果是非结构化的其他信息，应存放在室内具有较强防盗窃能力的文件柜中，并造册登记，分项存放。

（4）对于机密信息，如果是联机存储的结构化电子信息，应存放在有严格管理制度、具有高强度的安全防护措施的机房环境中的相关服务器和存储设备上；如果是脱机存储的结构化电子信息，以及非结构化的其他信息，应存放在具有严格保安措施的、专门的保管环境中（如机要室等），并造册登记，分项存放。

5.3.3 信息资产的存储介质使用控制要求如下：

（1）对于对外公开信息，介质使用没有限制要求，任何人在任何场合均可以使用。

（2）对于对内公开信息，对于存储在电子介质上的信息，必须通过内部网络，以注册的合法身份，登录访问和下载使用；对于非结构化的其他信息，经介质保存科室同意，可以提取存储信息的介质使用，使用完毕放回原处。

（3）对于秘密信息，对于存储在电子介质上的信息，原则上要求联机使用，信息只能通过应用系统专用界面使用，使用者必须具有足够的使用权限；秘密信息的脱机提取或抄录，必须有相关领导的书面批准意见，其提取或抄录的相关细节必须记录在案，使用者必须对其提取或抄录秘密信息的安全保密负责；对于非结构化信息的使用，必须符合秘密级文件的相关使用规定，信息的提取或抄录必须有相关领导的书面批准意见，其相关细节必须记录在案，使用者必须对其提取或抄录秘密信息的安全保密负责。

（4）对于机密信息，对于存储在电子介质上的信息，必须联机使用，信息只能通过应用系统专用界面使用，使用者必须具有足够的使用权限；机密信息绝对禁止的脱机提取，特殊信息的抄录，必须有相关领导及保密人员的书面批准意见，抄录的过程及内容必须有保密人员现场监督检查，抄录的相关细节必须记录在案，使用者必须对其抄录的机密信息的安全保密负责；对于非结构化信息的使用，必须符合机密级文件的相关使用规定，特殊信息的抄录必须有相关领导及保密人员的书面批准意见，其相关细节必须记录在案，使用者必须对其提取或抄录秘密信息的安全保密负责。

## 5.4信息资产分类

5.4.1 按照信息资产管理的相关标准和信息资产的表现形式，信息资产包括：

（1）单位的域名、网络拓扑结构、网络IP地址及分配规则、企业标准编码。

（2）单位投资开发的（或具有独立知识产权的）程序软件的源代码、支持程序软件、外购软件的使用许可证记录、系统平台基础数据等。

（3）系统配置数据、系统授权信息、口令文件、密钥及算法文件、系统说明文档、用户手册等系统基础数据。

（4）各类系统的应用数据库及数据文件、业务报表等系统业务数据。

（5）各类系统的运行方案、运行记录、变更记录等系统运行数据以及应急计划。

（6）各类的规划、方案与策略、业务流程、业务规范、操作规程等管理数据。

（7）技术图纸、技术文档、工程资料等项目数据。

（8）其他纸介质的重要办公文件（信件）、图像、影像、录音和照片等非结构化办公资料。

（9）单个员工拥有的专家技能和经验等隐性数据。

5.4.2 信息资产具有不同的敏感度和重要性，应从其机密性、完整性和可用性等属性对其进行分级，反映不同的保护要求、优先级和程度。XX单位信息资产按信息的敏感度分类为机密信息、秘密信息、对内公开信息、对外公开信息。信息资产安全分类见附件2《信息资产安全分类表》

## 5.5信息的标识及处置

XX单位的信息系统应在物理或逻辑标签中标明其资产分级。

5.5.1 应根据品牌型号、设备流水号、设备名称、设备序列号、设备责任人、使用单位、资产编码等制定资产标签，并把标签贴在相应的信息资产上；

5.5.2 应明确信息处于不同载体的标注方法。信息的密级必须被明确标注。根据存储和输出方式的不同，可以采用物理标签、电子标记等方法。

5.5.3 XX单位的客户或第三方在制作XX单位的信息资产标识时，应遵循XX单位统一的计算机和服务器标识定义及《保密法》有关规定要求。

5.5.4 XX单位的客户或第三方在对XX单位的信息资产标识时，应遵循XX单位统一的标识定义。

5.5.5 XX单位不同分级的信息在处置过程中应采取不同的控制和保护措施，对实物形式和电子形式信息资产的信息处置活动包括如下类型：

（1）复制；

（2）存储；

（3）通过邮寄、传真或电子邮件等方式进行传输；

（4）通过口头对话方式进行传播，包括电话、语音邮件、应答设备等；

（5）销毁。

5.5.6 XX单位机密信息的处置要得到XX单位主管领导的批准，并报信息中心备案审核。

5.5.7 处置信息类资产信息时，须在XX单位内部的专门处置场所，设置特殊的处置柜存放；含XX单位机密信息的纸件不得重复使用，纸质文件要通过专门设备彻底粉碎；电子文件要使用专门的清除软件安全清除；存储介质需要可靠地擦除或物理上彻底销毁。

## 5.6资产转移

在未经设备管理责任科室领导审批的情况下，不得让信息设备离开办公场所。对于有权允许移动信息设备，应设置信息设备移动的时间限制，明确对资产的转移、外出等进行跟踪管理，并在返还时进行一致性检查，并对设备做移出记录和送回记录的管理。

为了防止未授权的信息设备移动，进出时由信息中心进行抽查，以检测未授权的信息设备进出。这样的抽查应按照相关规章制度执行，并告知局所有员工此种抽查制度。

## 5.7资产数据安全管理

5.7.1应采取措施确保系统管理数据、鉴别信息和重要业务数据在传输过程中得到完整性检验与保护。

5.7.2应采取措施确保系统管理数据、鉴别信息和重要业务数据在传输过程中得到保密保护。

5.7.3应采取措施对关键数据得到及时备份，确保数据的可恢复性。

5.7.4应建立规范的资产销毁流程，确保资产销毁过程中信息的备份回收，并做好销毁记录（填写《资产销毁记录表》，见附件3），确保信息的保密、防止信息泄露。

# 6 附则

6.1本细则自批准发文之日起生效。

6.2本细则由XX单位信息中心负责解释。

# 7 附表

**附件1信息资产的存放形式表**

| **定义类别** | **信息资产名称** | **存储方式** | **存储介质** |
| --- | --- | --- | --- |
| 1 | 单位的域名 | 无 | 无 |
| 1 | 网络拓扑结构 | 脱机 | 电子介质 |
| 1 | 网络IP地址及分配规则 | 脱机 | 电子介质 |
| 1 | 企业标准编码 | 脱机 | 电子介质或纸介质 |
| 2 | 程序软件的源代码 | 脱机 | 电子介质 |
| 2 | 支持程序软件 | 脱机 | 电子介质 |
| 2 | 外购软件的使用许可证记录 | 脱机 | 纸介质 |
| 2 | 系统平台基础数据 | 联机 | 电子介质 |
| 3 | 系统配置数据 | 脱机 | 电子介质或纸介质 |
| 3 | 系统授权信息 | 脱机 | 电子介质或纸介质 |
| 3 | 口令文件 | 脱机 | 电子介质或纸介质 |
| 3 | 密钥及算法文件 | 脱机 | 电子介质 |
| 3 | 系统说明文档、用户手册 | 脱机 | 纸介质 |
| 4 | 各类系统的应用数据库及数据文件、业务报表等 | 联机 | 电子介质 |
| 5 | 各类系统的运行日志 | 联机 | 电子介质或纸介质 |
| 5 | 客户服务记录 | 联机 | 电子介质 |
| 6 | 企业各类规划、方案与策略 | 脱机 | 电子介质或纸介质 |
| 6 | 的业务流程、业务规范、操作规程 | 脱机 | 电子介质或纸介质 |
| 7 | 技术图纸、技术文档、工程资料 | 联机 | 电子介质或纸介质 |
| 8 | 其他纸介质办公文件（信件）、图象、影象、录音和照片等非结构化办公资料 | 脱机 | 按实际需要选择的各种介质 |
| 9 | 单个员工拥有的专家技能和经验等 | 无 | 无 |

**附件2信息资产安全分类表**

| **定义类别** | **信息资产名称** | **信息资产分类** |
| --- | --- | --- |
| 1 | 单位的域名 | 对外公开信息 |
| 1 | 网络拓扑结构 | 秘密信息 |
| 1 | 网络IP地址及分配规则 | 秘密信息 |
| 1 | 企业标准编码 | 对内公开信息 |
| 2 | 程序软件的源代码 | 秘密信息 |
| 2 | 支持程序软件 | 对内公开信息 |
| 2 | 外购软件的使用许可证 | 对内公开信息 |
| 2 | 系统平台基础数据 | 秘密信息 |
| 3 | 系统配置数据 | 秘密信息 |
| 3 | 系统授权信息 | 秘密信息 |
| 3 | 口令文件 | 机密信息 |
| 3 | 密钥及算法文件 | 机密信息 |
| 3 | 系统说明文档、用户手册 | 对内公开信息 |
| 4 | 系统应用数据库及数据文件、业务报表等 | 秘密信息 |
| 5 | 数据中心、机房运行日志及应急计划 | 秘密信息 |
| 5 | 客户服务记录 | 对内公开信息 |
| 6 | 单位经营方案与策略 | 机密信息 |
| 6 | 单位信息与网络安全方案与策略 | 机密信息 |
| 6 | 单位及各专业的规划与投资方案 | 秘密信息 |
| 6 | 单位的业务规范、操作规程 | 对内公开信息 |
| 6 | 各专业的业务流程 | 对内公开信息 |
| 7 | 技术图纸、技术文档、工程资料 | 秘密信息 |
| 8 | 其他纸介质的重要办公文件（信件）、图象、影象、录音和照片等非结构化办公资料 | 不定 |
| 9 | 单个员工拥有的专家技能和经验等 | 具体确认 |

**附件3资产销毁记录表**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **资产名称** | **资产编号** | **销毁事因** | **销毁方式** | **销毁时间** | **保管人** | **审批人** | **备注** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |