**北京汇聚融达网络科技有限公司**

**——信息资产管理制度**

**文件编码：HJRD-5-02**

**版 本：****V1.0**

**发布日期：2017-11-23**

**文档信息**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **基本信息** | | | | | |
| **文档名称** | 信息资产管理制度 | | **保密级别** | 内部 | |
| **文档编号** | HJRD-5-02 | | **牵头部门** | 技术部 | |
| **分发范围** | 制度管控员工 | | | | |
| **版本修订** | | | | | |
| **生效日期** | **版本号** | **版本说明** | **制作** | **复审** | **批准** |
| 上半年 | V1.0 | 第一版 | 刘少会/刘陵镇 | CTO | CEO |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注：文档基本信息记录本文档提交时的当前有效的基本控制信息，当前版本文档注有效期将在新版本文档生效时自动结束。文档版本小于1.0 时，表示该版本文档为草案，仅可作为参照资料之目的。

**第一条 【信息资产定义】**信息资产是指可以存储信息数据的载体，包括：硬件、软件、数据（电子数据）、文档（实体信息）、人员、服务设施、其他。

**第二条 【信息资产分类】**根据信息资产的类型和用途将信息资产进行分类。具体分类如下：

（一）硬件

1、终端设备：台式机、笔记本、服务器。

2、存储设备：磁带机、磁盘阵列、磁带、光盘、软盘、移动硬盘等。

3、网络设备：路由器、交换机、HUB、网关、程控交换机等。

4、传输线路：光纤、双绞线、电话线(布线)、电源线。

5、安全设备：硬件防火墙、入侵检测、网络隔离设备（如网闸）、负载均衡设备、身份验证等。

6、办公设备：打印机、复印机、扫描仪、传真机、碎纸机、写字白板、应急照明设备等。

7、保障设备：动力保障设备（UPS、变电设备）、空调、保险柜、文件柜、门禁、消防设施等。

8、其他设备。

（二）软件，如：操作系统、系统软件、应用软件、网管软件、杀毒软件、财务软件和资源库等。

（三）电子数据，存在电子媒介的各种数据资料。如：数据库数据、各种数据资料、系统文档、运行管理规程、计划、日周月报告、财务报告（电子版本）、用户手册、方案等。

（四）实体信息，纸质的各种文件。如：传真、电报、财务报告、发展计划、合同、纸张图纸等。

（五）服务，如：信息服务、网络服务、办公服务等。

（六）人员，如：学校各级领导、各级正式雇员、临时雇员等。

（七）其他；如：学校形象、客户关系等。

**第三条 【信息资产标识】**按照北京农学院对信息资产的要求，对信息资产进行编号，同时还需要对重要信息资产进行标识，标识要张贴在明显的位置。对于北京农学院的信息资产，为了可唯一进行识别，建议制定以下编号规则：

说明：资产编号 = 资产分类标识+"-"+六位顺序号；其中硬件（H）、软件（S）、电子数据（D）、实体信息（E）、服务（R）、人员（P）、其他（O）。

**第四条 【信息资产的分级】**

（一）按照《涉及国家秘密的信息系统分级保护技术标准》和信息安全管理体系建设要求，按照信息资产的公开和敏感程度，将北京农学院的信息资产划分为不同的保护等级，并对不同等级的信息资产进行保护，确保信息安全。

（二）各部门要将所有的移动介质和电子文件按照敏感性和重要程度分为不同的保护等级，保密级别与保密期限由信息持有人自行定义。

（三）信息资产密级划分原则

绝密：只对内部个别关键重要人员公开，对其它人员保密的信息，包含业务等最重要的机密信息，关系北京农学院未来发展的前途命运和根本利益，如果信息泄漏会造成灾难性的影响。

机密：对某一部门中的部分人员内部公开，对其它人员保密的信息，包含业务等重要秘密，其泄露会使北京农学院的安全和利益遭受严重损害。

秘密：在某一部门内部公开，对其它部门保密的信息，包含学校业务等一般性秘密，其泄露会造成北京农学院安全和利益受到损害；质量/信息安全管理体系文件都定义为秘密。

内部公开：在北京农学院内部公开，对外保密的信息，向外扩散有可能对北京农学院的利益造成损害。

公开：对社会公开的信息，公用的信息处理设备和系统资源等信息资产。

**第五条 【信息资产的识别与汇总】**通过台帐和人工识别，由各部门汇总《信息资产清单》，统一由国有资产管理处管理，并每半年进行一次更新，确保重要信息资产的完备性（重要信息资产没有遗漏和缺失）和准确性（信息资产的保密级别和重要程度能够真实反映信息资产的状态）。

**第六条 【信息资产的使用和处置】**规范信息资产的使用和处置，主要包括硬件资产的管理、维护和处置，软件资产的使用处置，电子数据的使用处理，实体信息的使用处置等。

（一）硬件资产的管理、维护和处置

1、设备管理根据“谁使用谁负责”的原则，由计算机等设备的操作人员（或使用人员）负责日常维护。对于无人职守的设备，要明确管理人员，加强物理安全控制。

2、启动设备前，必须认真检查各种设备的状态，确认正常方可开启；关闭系统时，按规定程序操作；严禁在通电情况下拆卸、移动、擦拭设备；严禁带电插、拔电缆线；定期对设备内部进行清扫；长期不使用设备应定期开机检测。

3、各部门要加强对设备管理情况的检查，应落实专人负责设备定期检查工作，记录计算机及网络设备的运行情况。

4、计算机设备及网络设备发生故障时，操作人员应立即报告，由相关人员及时诊断处理。

5、凡因管理不当造成计算机等设备丢失、严重破损的，应及时上报国有资产管理处，在责任分清的基础上依照安全保卫管理条例、固定资产管理规定等由安保、财务部门进行相应处理。

6、设备迁移时，如果设备中存储有重要信息，需事先进行备份；设备迁移出本部门时，检查人员在检查时要格外注意，禁止设备中存放重要信息，以防止机密信息泄露或泄露的风险增加。

7、计算机等硬件设备因故障损坏且无修复价值的，由主管部门填写《信息设备报废审批表》报资产管理部门，由该部门与网络与信息中心及计划财务处共同进行审核，经呈报北京农学院领导审批同意后再进行处理。

8、带有存储的设备销毁前，应确保所有存储的敏感数据或授权软件已经被移除或安全重写，再在负责人的监控下进行彻底的物理销毁，对保密性较高的存储设备未经批准不得自行销毁。

9、任何单位及个人不得擅自处理任何硬件设备。

（二）软件资产的使用处置

1、所有的软件资产必须设置专人管理，明确职责，避免软件资产的丢失，泄密。

2、所有正版软件实体由专人保管，在安装软件时要规定使用权限，防止非授权访问。

3、当人员离职或岗位变动，需要回收有关的软件，必要时，由网络与信息中心人员对离职人员使用的软件进行卸载、删除。

4、对过时或确认无效的软件资产，定期进行处置（清除）。

（三）电子数据的使用处理

1、对所有电子数据进行分类/分级，标识未授权人员的访问限制，不同安全级别的数据应存储在不同的区域，按类按级传达，便于信息的安全管理。

2、不同类型的电子文件按照统一规律存放在个人电脑或服务器中，便于整理和查阅以及工作交接时转移。

3、所有电子文件保存在电脑或服务器中，并按照备份策略规定的备份频率定期进行备份。

4、网络与信息中心每半年定期对备份数据进行恢复性测试工作，并记录保存测试结果，根据测试结果及时修改或更新灾难恢复计划。

5、对于存于服务器上的电子数据的访问，应根据服务器提供服务的不同与部门、职务的不同，设置不同的访问权限，减少非授权的访问。

6、对于绝密级别的电子信息要加密保存，由专人负责安全保管，进行严格的授权访问。

7、对于机密／秘密级别的电子信息，也要由专人管理，存放在授权控制的路径下，但相对的绝密级别的电子信息，其授权的人员数量多于后者。

8、对于内部公开级别的电子信息，其使用要控制在学校内部，禁止带出。

9、对于秘密级别以上的电子文件的处理过程，应保障数据的完整性、机密性和可用性。

10、对于秘密级别以上的电子文件的使用，系统应进行审计。

11、对于秘密级别以上的电子文件的传输，应采取适当的安全措施加以保护，如加密传输、分散传输等。

12、在整理电脑中的电子数据时，要小心操作，确认后再进行处理，避免由于误操作将有用的电子数据删除。

（四）实体信息的使用处置

1、所有的秘密级以上的实体信息资料要（通过标签或其它方式）标识出资产的保密级别，分类存放，不同安全级别的实体信息应按类、按级传达，便于实体信息的安全管理。

2、对于比较重要的实体信息（机密级别以上）必须保存在带锁的柜子或保险柜子中，柜子钥匙由专人保管。

3、对于实体信息的保存期限依据信息内容实施。

4、对于比较重要的实体信息的使用过程，应注意信息的保密，确保信息的完整性和可用性。

5、对于比较重要的实体信息的传输，应采取适当的安全措施加以保护，如专人递送、分散传输等。

6、实体数据资料达到保存期限后，应将其撕毁或者粉碎，避免实体数据资料的泄密。

7、对于重要实体信息的销毁，如财务实体信息，要求两人以上在场，防止信息的泄密。

**第七条 【各类设备的操作规程】**

（一）交换机、路由器操作规程

1、开关电源

1. 非经管理人员批准，任何人不许随便开关电源。
2. 当关闭电源时，必须提前通知网络与信息中心及业务相关部门，并在OA系统上发布消息。
3. 当开启电源时，首先通过主控台进行监控，查看设备是否正常启动，等设备正常启动并正常运行20分钟后方可认为启动成功。
4. 将过程登记到记录本上。

2、安全管理

1. 操作人员应有互不相同的用户名，定期更换操作口令，严禁操作人员泄露自己的操作口令。
2. 必须启动系统软件提供的安全审计功能。
3. 当发现系统有异常时，必须立刻通网络与信息中心领导，并采取相关的应急措施，事后应将处理过程登记到记录本上。

3、修改配置

1. 修改配置的工作必须由管理人员完成，其他人员禁止随意修改配置。
2. 禁止直接在交换机/路由器上修改配置。
3. 修改配置前必须首先将当前配置文件通过TFTP协议传送到一台TFTP服务器上，然后通过文本编辑软件修改配置文件并将修改后的配置文件上传到交换机/路由器上。
4. 将配置修改情况登记到记录本上。

4、增加新的接入单位

1. 为保证网络设备的正常使用，禁止任何人随意在交换机/路由器上私接窗口。
2. 在正常增加的接入单位而需要在交换机/路由器上接入时，必须首先做好标签，由管理员执行，如管理员不在又需要立刻接入时应执行补报手续。
3. 将连接修改情况登记到记录本上。

（二）服务器操作规程

1.服务器只能由系统管理员一人操作，其他人不得操作产服务器。

2.服务器应使用独立的UPS后备电源并不得随意断电、重启，一旦发生故障，应当及时通知系统管理员处理。

3.系统管理员应当妥善设置系统密码，不得泄漏、不得过于简单，并定期更改密码。

4. 系统管理员应当定期升级防毒程序和定期对系统查杀病毒，应当注意服务器的清洁卫生，定期对服务器进行除尘。