\*\*\*\*\*\*有限公司信息资产和设备管理制度

* 1. 范围和职责

1. 本制度适用于信息资产的管理，包括：获取、分类、使用和处置以及安全设备的管理。
2. 本制度中的信息资产是指可以存储信息数据的信息载体，包括：硬件、软件、数据（电子数据）、文档（纸质文件）、人员、服务设施、其他。
3. （ ）部门主要负责信息资产的分类、汇总、使用与处置方法，以及安全设备的选型、检测、安装、登记、使用、维护和储存。
4. 计算机资产统计信息的范围包含但不限于：计算机主机名、IP地址、MAC地址、使用人/责任人、所属部门、物理位置、服务器的内外网IP对应等（参见表A.12，A.13）。
   1. 信息资产的获取
5. 软件、硬件设施、服务性设施等的获得主要以采购的方式获得，采购按照有关规定进行采购和验收。
6. 数据信息资产的获得来源主要为：外包供应商、市场信息、其他信息。
   1. 信息资产的分类
7. 各部门根据业务流程列出信息资产清单并将每项资产的资产类别、信息资产编号、资产现有编号、资产名称、所属部门（组别）、管理者、使用者、地点等相关信息记录在资产清单上。
8. 资产的分类原则和编号原则如下：
   1. 硬件
      1. 计算机设备：(台式终端、移动终端)、服务器；
      2. 存储设备：磁带机、磁盘整列、磁带、光盘、软盘、移动硬盘等；
      3. 网络设备：路由器、交换机、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）、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。
   2. 软件
      1. 如：操作系统、系统软件（office/AutoCAD）、应用软件（生产软件）、网管软件、杀毒软件、财务软件、开发工具和资源库等；
   3. 电子数据
      1. 存在电子媒介的各种数据资料。如：源代码、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、电子设计图纸等；
   4. 纸质文件
      1. 纸质的各种文件。如：传真、电报、合同、纸张图纸等；
   5. 服务性设施
      1. 如：供电、供水、保洁、门禁、消防设施等；
   6. 人员
      1. 如：各级领导、各级正式雇员、临时雇员等；
   7. 其他。
9. 按照信息资产的敏感程度，将信息资产化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。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持有人自行定义。
10. 识别各个流程的各类关键信息资产，最终（ ）部门汇总，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）。
11. 对信息资产进行编号，同时对重要信息资产进行标识：文档需有固定版本编号规则；硬件设备粘贴在设备明显位置处。
    1. 信息资产的使用和处置
       1. 硬件资产
12. 硬件的使用处置包括购买/接收、使用（交接、维修、重用）、处置等有关内容。
13. 购买新的硬件设备或者从其他部门接收转移的设备时，要核对设备清单，对相关设备进行测试验证，然后登记。由资产管理员对硬件设备进行管理，明确设备管理职责。
14. 硬件资产的保存
    1. 机房选址要避免在地下室、一楼（水淹和渗水）和顶层（渗水和失火时火向上燃烧），同时考虑相邻楼层的活动（避免热源和渗水）；
    2. 处理敏感数据的信息处理设施放在适当安全的位置，以减少在设备在使用期间信息被窥视的风险，保护储存设施以防止未授权访问；
    3. 设备的选址应采取控制措施以减小潜在的物理威胁的风险，例如偷窃、火灾、爆炸、烟雾、水（或供水故障）、温度、湿度、尘埃、振动、化学影响、电源干扰、通信干扰、电磁辐射和故意破坏；
    4. 禁止在信息处理设施附近进食、喝饮料和抽烟；
    5. 对专门保护的部件要予以隔离，以满足特殊安全要求；
15. 硬件资产的日常使用安全
    1. 所有的硬件资产必须明确设备的使用人员/管理人员，明确职责；
    2. 硬件资产的使用人（或管理人），在使用或管理硬件资产时，要注意硬件资产的安全性、机密性、完整性，防止信息载体的毁坏和信息的泄密，防止信息处理设施的滥用；
    3. 对设备定期进行维护保养，发生毁坏，丢失等问题时能够及时处置；
    4. 新硬件设备接入网络按照相关规定处理；
    5. 在人员上岗时，可根据需要为上岗人员配备必要的办公设备，包括电脑（移动终端或台式终端），电话机，其它办公用品；（ ）部门根据该工作人员所处部门、工作性质为其设置相应的办公网访问权限；
    6. 需要使用移动计算设备（包括移动终端、无线网卡、移动硬盘和U盘）的用户，应得到（ ）部门负责人的同意后方可使用；
    7. 对于无人职守的设备，要明确管理人员，加强物理安全控制。
16. 硬件资产的转移安全
    1. 当设备迁移时，必须先对设备中存储的重要信息进行备份；
    2. 设备迁移完成后，必须检查设备是否损坏；
    3. 设备迁移出本单位时，设备中禁止存放重要信息，以防止机密信息泄露或泄露的风险增加。
17. 办公地点外使用任何信息处理设备必须通过管理者授权。场外设备的保护要考虑下列内容：
    1. 离开本单位的设备和介质（如现场的设备和介质），必须有人值守或委派负责人(或者公共场所放置的需要有人值守或监视系统)；
    2. 制造商保护设备用的说明书要始终加以遵守，例如，防止暴露于强电磁场内；
    3. 根据风险的不同采取足够的安全保障措施，以保护离开办公室设备的安全。
18. 硬件资产的处置和重用
    1. 存储设备销毁前，必须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；
    2. 服务器、主要网络设备的处置由（ ）部门进行安全处置；
    3. 台式终端、打印机、传真机、扫描仪等IT设备的处置由（ ）部门进行并做登记；
    4. 如需报废时，应向主管部门提出报废申请，经批准后报废。
       1. 软件资产
19. 软件资产的使用
    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（ ）部门保管，在安装软件时要规定使用权限，防止非授权访问；
    3. 按照《系统运行维护管理制度》中“备份与恢复管理”章节要求，对重要系统进行备份；
    4. 当人员离职或岗位变动，需要回收有关的软件，必要时，由（ ）部门技术人员对离职人员使用的软件进行卸载，删除。
20. 软件资产的处置：对过时或确认无效的软件资产，定期进行清除。
    * 1. 电子数据
21. 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；
22. 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；
23. 重要的电子数据要使用可靠的加密手段进行保护；
24. 所有电子文件保存在电脑或服务器中，应根据业务实际需要选择不同的备份频率（周/月/季/年）定期进行备份并保证备份数据的完整性和可用性；
25. 备份数据与原始数据分开存放，严禁直接在同一主机或服务器上保存，应存放在外部带锁的文件柜或保密柜中；
26. 对于存于服务器上的电子数据的访问，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，避免非授权访问；
27. 对于内部公开级别的电子信息，其使用要控制在内部，禁止带出；
28. 对于密件的处理应经过严格授权；
29. 对于秘密级别以上的电子文件的使用，系统应进行审计；
30. 对于秘密级别以上的电子文件的传输，必须采取适当的安全措施加以保护，如加密传输、分散传输等；
31. 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。
    * 1. 纸质文档
32. 所有的秘密级以上的纸质文件资料要（通过标签或其它方式）标识出资产的保密级别，分类存放，不同安全级别的纸质文件应按类按级传达，便于纸质文件的安全管理；
33. 对于比较重要的纸质文件（机密级别以上）必须保存在带锁的文件柜或保险柜中，钥匙由专人保管；
34. 对于纸质文件的保存期限依据实际要求制定和实施；
35. 对于比较重要的纸质文件的使用过程，必须注意信息的保密，确保信息的完整性和可用性；
36. 对于比较重要的纸质文件的传输，必须采取适当的安全措施加以保护，如专人递送、分散传输等；
37. 实体数据资料达到保存期限后，必须将其撕毁或者粉碎到读不出来为止，避免实体数据资料的泄密；
38. 对于重要纸质文件的销毁，如财务纸质文件，要求两人以上在场，防止信息的泄密。
    * 1. 服务性资产
39. 所有服务性资产要设置专人管理，定期维护，避免损坏、非授权使用或丢失。涉及服务性的合同，相关管理部门在签署合同时，应审核涉及信息保密的相关条款。
40. 当服务性设施损坏，如果可以维修，由负责人联络相关人员进行维修，如果涉及到第三方，依据《用户管理制度》对第三方进行管理。
41. 当服务性设施损坏，不可维修，只能报废时，应联络相关管理部门提出报废申请。
    1. 设备管理
42. 严禁采购和使用未获得销售许可证的设备。
43. 应优先采用我国自主开发研制的信息安全技术和设备。
44. 避免采用境外的密码设备。
45. 如需采用境外信息安全产品时，必须确保产品获得我国权威机构的认证检测和销售许可证。
46. 应使用经国家密码管理部门批准和认可的国内密码技术及相关产品。
47. 终端物理隔离必须使用经国家保密部门认可的隔离卡或其他方式。
48. 购回的设备均须在测试环境下经过连续72小时以上的单机运行测试和联机48小时的应用系统兼容性运行测试。
49. 主机、服务器、网络设备、安全设备等上架运行前必须经过安全测试和加固。
50. 通过安全测试和加固的设备才能接入生产系统，正式运行。
51. 对所有设备均应建立严格完整的购置、移交、使用、维修和报废等记录，认真做好资产登记和管理工作，保证设备管理的正规化。
52. 每台设备的使用均应指定专人负责并建立详细的运行日志。
53. 由责任人负责进行设备的定期保养维护，做好维护记录，保证设备处于最佳状态。
54. 一旦设备出现故障，管理员如实填写故障报告，通知有关人员处理。
55. 设备由专人负责维修，并建立满足正常运行最低要求的易损件备件库。
56. 根据每台设备的使用情况及系统的可靠性等级，制定预防性维修计划。
57. 对系统进行维修时必须采取数据保护措施，安全设备维修时应有安全管理员在场。
58. 对设备进行维修时必须记录维修对象、故障原因、排除方法、主要维修过程及维修有关情况等。
59. 对设备应规定折旧期，设备到了规定使用年限或因严重故障不能恢复，由专业技术人员对设备进行鉴定和残值估价，并对设备情况进行详细登记，提出报告书和处理意见，由主管领导或上级主管部门批准后方能进行报废处理。
60. 设备储存环境应符合出厂标称要求。
61. 建立详细的设备进出库、领用和报废台帐。
62. 安全产品及保密设备应造册登记（参见表A.14）并单独存放，并采取相应的保护措施。
    1. 附则
63. 本制度由（ ）部门负责解释。
64. 本制度自发布之日起生效执行。