# 防灾科技学院信息化管理中心

信息中心〔2021〕24 号

## 关于印发《防灾科技学院商用密码应用安全管理制度》的通知

学校各部门、各单位：

为规范学校商用密码应用的管理工作，保护网络安全，特制定《防灾科技学院商用密码应用安全管理制度》，现予印发，请遵照执行。

防灾科技学院信息化管理中心

2021 年 12 月 9 日

# 防灾科技学院商用密码应用安全管理制度

## 第一章　总则

**第一条**　为规范学校商用密码应用的管理工作，保护网络安全，特制定本制度。

**第二条**　在实施网络安全等级保护的信息系统中，商用密码应用是指采用商用密码产品或者含有密码技术的产品集成建设的，实现相关信息的机密性、完整性、真实性、抗抵赖性等功能的应用系统。

**第三条**　本制度适用于学校所有密码产品。

**第四条**　学校网络安全和信息化领导小组办公室（以下简称“网信办”）负责此规定的落实，相关部门应予以配合、支持。

## 第二章 人员管理

**第五条**　密码管理人员及使用人员需了解并遵守密码相关的法律法规，经过培训后应能正确使用密码产品。

**第六条**　学校应设置密码系统负责人、密码安全主管、密钥管理员、密码安全审计员及密码操作员等关键岗位，并对关键岗位建立多人共同管理。其中，密钥管理员、密码安全审计员及密码操作员的职责应互相制约、互相监督。

**第七条**　密码系统负责人主要负责收集系统运行情况和对接网络安全领导小组。担任此岗位的人员在密码系统中可担任系统管理员职责，日常工作中可处理密码系统或密码设备的所有文件和数据。

**第八条**　密码安全主管向上负责向密码系统负责人汇报工作，向

下负责密码系统、设备的日常安全运维工作。担任此岗位的人员在密码系统和密码设备中可担任安全管理员职责，日常工作中可处理密码系统和密码设备的安全报警信息、安全检查报告等内容。

**第九条** 密钥管理员主要负责商用密码应用密钥以及加密机的操作。担任此岗位的人员不可在系统中担任管理员角色，不可处理密码系统和密码设备中的任何业务数据及业务文件，仅可以用普通用户管理、检查、升级密钥信息。

**第十条** 密码操作员要熟悉设备的使用，了解设备在网络中的作用，并定期更换密码设备的密码，做好登记备案。担任此岗位的人员不可在系统中担任管理员角色，不可处理密码系统和密码设备中的任何业务数据及业务文件，仅能以普通用户的角色处理日常工作，如遇到权限范围内无法处理的工作应向密码系统负责人申请使用更高级权限。

**第十一条** 密码安全审计员对密钥管理员及密钥操作人员的操作行为进行监督，对可疑的信息进行安全审计和跟踪控制，发现违规行为及时向领导小组办公室汇报。担任此岗位的人员在密码系统和密码设备中可担任审计管理员角色，可处理密码系统和密码设备日常工作中产生的审计数据和日志记录等信息，在日常工作中可汇聚审计信息编写审计报告向密码系统负责人报送，并在审计过程中对出现的可疑事件应及时记录并报送至密码安全主管。

**第十二条** 密码管理人员及使用人员不得非法攻击商用密码应用或相关设备，不得利用持有的商用密码信息危害国家的安全和利益、

危害社会治安或者从事其他违法犯罪活动。

**第十三条** 学校应至少每年对密码系统负责人、密码安全主管、密钥管理员、密码安全审计员及密码操作员等关键岗位人员和预备人员进行密码相关的安全意识培训和保密意识培训，需采用考试、答辩、等方式对培训成果进行检测。

**第十四条** 密码系统负责人、密码安全主管、密钥管理员、密码安全审计员及密码操作员等关键岗位人员离岗时应经过学校网信办的审核与批准，同时应及时上交在岗期间持有的密钥、账户信息、令牌、文件材料等所有工作资料，未经批准或未完成材料交接时不应擅自离岗。

**第十五条** 密钥管理员、密码安全审计员及密码操作员等关键岗位人员离岗时应签署保密协议，不得随意传播在岗期间知晓或持有的任何信息。

## 第三章 建设管理

**第十六条** 在信息系统规划阶段，学校应依据国家密码管理部门发布的密码相关标准制定密码应用方案，并组织专家进行评审，评审意见作为项目规划立项的重要材料。

**第十七条** 通过专家审定的方案应作为建设、验收和测评的重要依据。

**第十八条** 商用密码应用的建设应当选择具有商用密码相关资质的单位。

**第十九条** 只能使用经国家密码管理部门核准的密码产品、许可

的密码服务，不得使用自行研制的或者境外生产的密码产品。

**第二十条** 应根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节。

**第二十一条** 使用商用密码开展网络安全等级保护应当制定商用密码应用建设方案。方案应当包括系统建设规划背景、系统现状分析、安全风险及控制需求、密码应用需求、总体方案设计、密码技术方案设计、商用密码产品清单（包括产品资质、功能及性能列表和产品生产单位等）管理体系设计与运维体系设计、安全与合规性分析、实施计划等几个部分。

**第二十二条** 信息系统的商用密码应用，应当通过国家密码管理部门指定测评机构的密码测评后方可投入运行。密码测评包括资料审查、系统分析、现场测评、综合评估等。学校应当将测评结果报相应的密码管理部门备案。

## 第四章 运维管理

**第二十三条** 学校应当积极配合密码管理部门组织开展的商用密码检查工作。

**第二十四条** 信息系统投入运行后，学校应每年委托密码测评机构开展密码应用安全性评估，并根据评估意见进行整改。

**第二十五条** 若在使用或检查过程中发现重大隐患的，应停止系统运行，启用备用系统或工作机制，及时对问题系统制定整改方案，整改完成并通过评估后方可再次投入运行。

**第二十六条** 第三级及以上信息系统发生重大变更时，学校应当

将变更情况及时报国家密码管理相关机构，并按照国家密码管理相关机构的要求办理相关事项。

**第二十七条** 第三级及以上信息系统的商用密码应用需要选择具有商用密码相关资质的第三方单位负责运维。

**第二十八条** 商用密码应用或相关设备发生故障，应及时交该产品的生产单位或销售单位维修，原则上应由厂商提供工作人员到现场进行维修并由学校派出相关人员对维修过程中厂商人员的操作进行监视，若需要返厂维修则生产单位或销售单位应签署具有法律效力的保密条款。

**第二十九条** 学校应每年组织针对商用密码应用和密码设备的攻防测试，可由单位自主举行或委托具有相关资质的第三方厂商进行，并对其中发现的问题及时进行整改。

## 第五章 密码设备管理

**第三十条** 学校选用的含有密码技术的产品，应当是通过国家密码管理部门指定测评机构密码测评的产品。

**第三十一条** 相关设备与系统的管理与使用账号需专人专用，不得多人共用。

**第三十二条** 使用密码产品的用户不得转借其使用的商用密码产品。

## 第六章 密钥管理

**第三十三条** 应根据《防灾科技学院电子公文项目密码应用建设方案》对相应密钥进行管理，覆盖密钥全生存周期的管理，包括密钥

的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节。

**第三十四条** 根据《防灾科技学院电子公文项目密码应用建设方案》，密钥的产生环节应由在地震局台网中心行业网部署 CA 系统，包括密钥管理系统、证书认证系统、业务应用系统。学校通过中国地震行业网，使用台网中心为各省局授权的业务操作员角色登录台网中心 RA，为各省局人员签发个人 USBKey 证书。

**第三十五条** 根据《防灾科技学院电子公文项目密码应用建设方案》，密钥的分发环节由证书签发系统接受来自 RA 中心的业务请求，提供证书的签发和管理功能，代表用户向密钥管理中心发出密钥产生、恢复请求；为用户签发用户证书。

**第三十六条** 根据《防灾科技学院电子公文项目密码应用建设方案》，密钥的存储环节中，系统私钥采用加密机进行安全保存，与私钥相关的所有操作均在加密机中进行，私钥不会以明文的方式从加密机中导出。

**第三十七条** 根据《防灾科技学院电子公文项目密码应用建设方案》，密钥的使用环节中用户可通过证书模板管理功能自定义证书的格式和内容，以满足不同组织的证书应用需求。

**第三十八条** 根据《防灾科技学院电子公文项目密码应用建设方案》，密钥的更新环节能够根据要求，实现证书的更新。包括证书用户信息更新，用户的密钥的更新等。

**第三十九条** 根据《防灾科技学院电子公文项目密码应用建设方

案》，密钥的归档环节中系统提供证书归档功能。管理员可以按照过期时间对证书库进行归档，将过期证书从当前证书库中转移到证书历史库中。

**第四十条** 根据《防灾科技学院电子公文项目密码应用建设方案》，密钥的撤销环节中，主要由管理方（RA 操作员、CA 中心管理员等）发起，对证书进行冻结，使证书列入黑名单，暂时因为失效而无法使用；同时，管理方也可对被冻结的证书进行解冻操作，使该证书恢复正常的使用功能。

**第四十一条** 根据《防灾科技学院电子公文项目密码应用建设方案》，密钥的备份环节中由 RA 系统还可以对用户资料进行管理、维护和备份工作。

**第四十二条** 根据《防灾科技学院电子公文项目密码应用建设方案》，密钥的恢复环节由证书签发系统来自注册与审核中心系统的业务请求，提供证书的签发和管理功能，代表用户向密钥管理中心发出密钥恢复请求，完成恢复操作。

**第四十三条** 根据《防灾科技学院电子公文项目密码应用建设方案》，密钥的销毁环节中，吊销实体证书，分为 CA 中心强制废除和用户申请废除。由于以下原因，证书应该被作废：

密钥泄密。证书的私钥泄密，或者怀疑泄密。为防止错误使用或被盗用，其对应的证书应该被作废。系统签发的 CRL 将指出证书未泄密的最后日期。

从属变更。某些关于证书的信息变更，但不怀疑泄密。

密钥已被取代。旧密钥对已被新密钥对取代，但不怀疑泄密。

终止使用。该密钥对已不再用于原来的用途，但不怀疑泄密。

暂时不使用。证书持有者由于某种原因短期内无法使用证书。

未说明的原因。因为不同于上述分类中的任何原因，该密钥对不再需要。

**第四十四条** 商用密码应用或密码产品的管理密钥应至少由三份构成，单独一份或两份均不可获得管理权限。

**第四十五条** 商用密码应用或密码产品的普通用户密钥应只能获得个人所需的最小授权。

**第四十六条** 配发的密钥应由学校密钥管理员进行登记并妥善保存相关记录，同时应至少一季度核对一次密钥使用情况是否与登记表内容一致。

**第四十七条** 密钥丢失时，持有人应及时向密钥管理员报告，对隐瞒不报并造成学校经济财产损失或造成法律责任的情况，学校将根据相关法律依法进行追责和处罚。

## 第七章 应急处置

**第四十八条** 当商用密码应用或密码设备发生紧急情况，如系统宕机、设备掉线、业务离线等紧急情况时，系统管理员或操作员应立刻将情况汇报学校网信办，不应自行操作。

**第四十九条** 学校网信办经分析后需决定事件级别，并采用对应级别的应急处置预案。

**第五十条** 在处置应急事件时应及时做好相关记录，并妥善保存。

**第五十一条** 应急事件处置中，应做到以人为本、安全第一、统一领导、分级负责、依靠科学、依法规范的原则。

**第五十二条** 应急事件处置完毕后，由学校网信办判断是否需要向上级领导单位和国家密码管理部门报备。

## 第八章 附则

**第五十三条** 本制度由学校网络安全和信息化领导小组办公室负责制定、解释、修订并完善。

**第五十四条** 本制度自发布之日起施行。

防灾科技学院信息化管理中心 2021 年 12 月 9 日印发