国开信息〔2017〕1号

## 关于印发《国家开放大学网络安全

## 管理规定（试行）》和成立国家开放大学

## 网络安全领导小组、工作小组的通知

## 校内各部门，出版集团、电大在线、数字化学习资源中心、对外汉语教学中心：

为落实国家和教育部对网络安全提出的一系列要求，建立网络安全长效机制，确保学校信息系统安全，根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）、《信息安全等级保护管理办法》（公通字〔2007〕43号）等法律法规，学校制定了《国家开放大学网络安全管理规定（试行）》（附件1），经3月6日校长办公会研究，决定印发施行，同时成立国家开放大学网络安全领导小组和工作小组（附件2），负责学校网络安全工作的领导和组织实施。

附件 ：1.国家开放大学网络安全管理规定（试行）

2.国家开放大学网络安全领导小组和工作小组组成

人员名单

国家开放大学

2017年4月10日

|  |
| --- |
| 国家开放大学校长办公室 依申请公开 2017年4月10日印发 |

附件1：

**国家开放大学网络安全管理规定**

**(试行)**

# 总　则

* 1. 为落实国家和教育部对网络安全提出的一系列要求，建立网络安全长效机制，确保学校信息系统安全，根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）、《信息安全等级保护管理办法》（公通字〔2007〕43号）等法律法规，制定本规定。
  2. 本规定涵盖的网站和信息系统是以国家开放大学为主办单位的网站和信息系统。
  3. 网络安全工作遵照“谁主管，谁负责；谁运维，谁负责”的原则，各司其责，建立事前防御、事中监测、事后审计的信息安全保障机制。

# 第二章　网络安全管理组织机构及其职责

* 1. 学校设立网络安全领导小组，负责统筹、部署、监督和协调国家开放大学的网络安全总体工作，组长由校长担任。网络安全领导小组的具体职责包括：

1. 确定网络安全工作的总体方向和目标，制定和发布信息系统安全发展规划；
2. 监督网络安全建设、管理和运行工作；
3. 指挥、协调和审查重大信息安全事件的处理；
   1. 网络安全领导小组下设网络安全工作小组，作为学校信息安全工作的日常管理执行机构，负责落实各项网络安全工作，组长由信息化部负责人担任。具体职责包括：
4. 贯彻执行上级机关和学校网络安全领导小组的决议和工作部署；
5. 制定和落实学校网络安全管理制度以及信息安全策略；处理信息系统建设、管理和运行中的安全问题；
6. 组织协调信息安全事件应急处置和相关恢复工作；
7. 组织协调开展信息安全等级保护工作；
8. 指导分部开展信息安全工作；
9. 开展信息安全检查和培训工作；
10. 完成网络安全领导小组交办的其他工作。

# 第三章　网络与信息系统安全责任制

* 1. 学校的网络与信息系统安全实行一把手责任制。网络安全领导小组组长全面负责学校的网络安全工作；网络安全工作小组组长承担日常的网络安全管理工作；信息系统的主管部门和运维部门是安全工作的责任主体，部门负责人须签订相应的安全责任书。信息系统建设与运维须遵照《国家开放大学信息系统建设运维管理规定》执行。

1. 主管部门须签署《信息系统主管安全责任书》，负责所主管信息系统的管理和信息发布审核等工作，监督运维单位保障信息系统特别是内容安全。运维单位或部门须签署《信息系统运维安全责任书》，负责信息系统的技术运维以及基础设施的安全运维。
2. 如果信息系统发生安全事件并被上级机关通报批评，相关主管、运维部门负责人年终考核不合格；如果发生重大或特别重大信息安全事件，学校对相关主管、运维部门负责人给予相应处罚。如由合作公司造成安全事件，按照合同约定进行处理。
   1. 信息系统在立项建设阶段须确定安全保护等级，系统的建设方案中包含按照等级保护要求设计的安全保护方案，系统的安全保护建设遵循“同步规划、同步建设、同步使用”原则，主管部门须在上线前提交安全保护等级定级报告与备案表，同时按照要求填报相关信息。
   2. 安全保护等级为二级及以上的信息系统在上线时须达到相应安全保护等级要求。信息系统主管部门有责任督促项目承建单位按照等级保护要求进行安全加固与评估。在信息系统验收时须提交安全评估报告，未达到相应安全等级要求的信息系统不能通过验收。
   3. 如系统被攻击或被通报存在安全漏洞，信息化部将根据情况采取封闭IP地址/端口和关停网站等措施，责成相关单位进行整改，直至整改符合要求为止。
   4. 网站主管部门负责监督和审核网站所发布的内容，教师须确保上传的网络课程资源不含非法或其他不当内容。
   5. 安全保护等级为二级及以上的信息系统在建设或运维时若涉及第三方单位或人员，信息系统主管部门应负责与具有独立法人资格的第三方单位签署委托服务合同和信息安全保密协议，同时第三方单位须与核心运维人员签署信息安全保密协议，并报信息化部。

# 第四章　信息安全事件应急响应与处置

* 1. 按照教育部办公厅印发的《信息技术安全事件报告与处置流程（试行）》要求，成立信息安全应急响应小组，对信息安全事件进行应急响应。应急响应小组由网络安全领导小组组长、网络安全工作小组组长、相关信息系统主管负责人和运维负责人等组成。
  2. 网络安全工作小组对信息安全事件的应急响应进行协调、处置和管理。一旦发生安全事件，运维或使用部门应第一时间采取断网等有效措施进行处置，保留现场，报告至本部门安全负责人及网络安全工作小组，确定安全事件级别。
  3. 安全事件根据其作用对象的重要程度和影响程度的不同分为四个等级：特别重大事件（I级）、重大事件（II级）、较大事件（III级）和一般事件（IV级）。

特别重大事件（I级）是指能够导致特别严重影响或破坏的信息安全事件；重大事件（II级）是指能够导致严重影响或破坏的信息安全事件；较大事件（III级）是指能够导致较严重影响或破坏的信息安全事件；一般事件（IV级）是指能够导致较小影响或破坏的信息安全事件。

* 1. 网络安全工作小组接到安全事件报告后，应立即组织技术人员赶赴现场进行处置，同时将相关情况上报，涉及人为破坏事件应及时报告网络安全领导小组，若有必要，经核准后报送当地公安机关处理。
  2. 安全事件的事中情况报告和事后整改报告由网络安全领导小组责成相关部门填写。安全事件的事中情况报告应在安全事件发生8小时内以书面报告的形式报送，安全事件的事后整改报告应在安全事件处置5个工作日内以书面形式报送。对于较大、重大和特别重大安全事件，报送教育部科技司。
  3. 信息系统主管部门及基础设施运维部门应设立安全员，保证在发生安全事件时能够及时联系到安全员。

# 第五章　附　则

* 1. 涉及分部、学院的网络安全相关管理办法另行制定。
  2. 本规定由国家开放大学负责解释、修订。
  3. 本规定自发布之日起执行。

附录：1.信息系统主管安全责任书

2.信息系统运维安全责任书

3.信息安全事件报告表

附录1：

信息系统主管安全责任书

为落实《国家开放大学网络安全管理规定（试行）》，明确网站和信息系统主管安全责任主体，网站和信息系统的主管部门负责人签署本责任书。

是 信息系统/网站的主管责任部门，作为部门负责人，严格遵守《国家开放大学网络安全管理规定（试行）》，履行规定的网络安全职责。

签字：

日期：

附录2：

信息系统运维安全责任书

为落实《国家开放大学网络安全管理规定（试行）》，明确网站和信息系统运维安全责任主体，网站和信息系统的运维部门/单位负责人签署本责任书。

是 信息系统/网站的运维责任单位，作为单位负责人，严格遵守《国家开放大学网络安全管理规定（试行）》，履行规定的网络安全职责。

签字：

日期：

附录3：

**信息安全事件报告表**

报告时间： 年 月 日 时 分

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 单位名称 |  | | 报告人 |  |
| 联系电话 |  | | 通讯地址 |  |
| 传 真 |  | | 电子邮件 |  |
| 发生信息安全事件的对象名称及用途 | 类型 | □网络 □应用系统 □其他 | | |
| 名称 |  | | |
| 用途 |  | | |
| 信息安全事件的简要描述（如以前出现过类似情况也应加以说明） | □有害程序事件 | □计算机病毒事件 □蠕虫事件 □特洛伊木马事件 □僵尸网络事件  □混合程序攻击事件 □网页内嵌恶意代码事件 □其他有害程序事件 | | |
| □网络攻击事件 | □拒绝服务攻击事件 □后门攻击事件 □漏洞攻击事件 □干扰事件  □网络扫描窃听事件 □网络钓鱼事件 □其他网络攻击事件 | | |
| □信息破坏事件 | □信息篡改事件 □信息假冒事件 □信息泄露事件 □信息窃取事件  □信息丢失事件 □其他信息破坏事件 | | |
| □信息内容安全事件 | □通过网络传播法律法规禁止信息 □组织非法串联、煽动集会游行  □炒作敏感问题并危害国家安全、社会稳定和公众利益的事件 | | |
| □设备设施故障 | □软硬件自身故障 □外围保障设施故障 □人为破坏事故  □其他设备设施故障 | | |
| □灾害性事件 | □由自然灾害等其他突发事件导致的网络与信息安全事件  □其他特殊灾害事件 | | |
| □其他事件 （注：不能归为以上6个基本分类的其他信息安全事件） |  | | |
| 初步判定的事故原因 |  | | | |
| 当前采取的应对措施 |  | | | |
| 本次信息安全事件的初步影响状况 | 事件后果 | □业务中断 □系统破坏 □数据丢失  □其他 | | |
| 影响范围 | □单台主机 □ 台主机 □整个信息系统 □整个局域网  □其他 | | |
| 严重程度 | □极严重 □很严重 □严重 □一般 □不严重  □其他 | | |
| 主管/运维部门安全员签字 |  | | | |
| 运维单位负责人意见 |  | | | |
| 主管部门负责人意见 |  | | | |
| 学校安全管理员签字 |  | | | |
| 安全工作组意见 | （Ⅰ级、Ⅱ、III级填写） | | | |
| 安全领导小组意见 | （Ⅰ级填写） | | | |

注：填写表格时根据实际情况选择相关选项，并在相应选项前的“□”中以“√”标记。

附件2：

**国家开放大学网络安全领导小组和工作小组**

**组成人员名单**

1.网络安全领导小组组成人员名单

组 长：杨志坚

副组长：李 凌、李林曙

成 员：亓彦伟、蒋国珍、叶志宏、马若龙、杜 若、孙福万、

鄢小平、陈海山、郭 鸿、郭晓霞、刘占荣、刘志敏、李 松、唐应山

2.网络安全工作小组组成人员名单

组 长：蒋国珍

副组长：杜 若、袁亚兴

成 员：叶志宏、马若龙、鄢小平、匡贵秋、汪启富、李国斌、单丛凯、杨永博、薛海峰。