

# 教育行业信息系统安全等级保护定级工作指南

(试行)

## 1 总则

本指南依据国家信息安全等级保护相关政策和标准,结合教育行业信息化工作的特点和具体实际,对教育行业信息系统进行分类,提出安全等级保护的定级思路,给出建议等级,明确工作流程。

本指南适用于各级教育行政部门及其直属事业单位、各级各类学校的非涉密信息系统安全等级保护定级工作。

信息系统的定级工作应在信息系统设计阶段完成,与信息系统建设同步实施。

## 2 定级依据

《中华人民共和国计算机信息系统安全保护条例》(国务院第 147 号令)

《信息系统安全等级保护定级指南》(GB/T 22240-2008)

《信息系统安全等级保护实施指南》(GB/T 25058-2010)

《关于开展全国重要信息系统安全等级保护定级工作的通知》(公信安〔2007〕861号)

《信息安全等级保护管理办法》(公通字〔2007〕43号)

## 3 信息系统的类型划分

信息系统的类型划分是进行信息系统安全等级划分的前提和基础。按照信息系统的主管单位、业务对象、部署模式对教育行业信息系统进行分类,形成信息系统分类表。

### 3.1 按信息系统主管单位划分

按照信息系统主管单位的不同，信息系统分为“教育行政部门及其直属事业单位信息系统”（简称“部门信息系统”）和“学校信息系统”两类。

部门信息系统可分为教育部机关及其直属事业单位信息系统（部级系统）、省级教育行政部门及其直属事业单位信息系统（省级系统）、地市级教育行政部门及其直属事业单位信息系统（市级系统）和区县级教育行政部门及其直属事业单位信息系统（县级系统）；学校信息系统可分为重点建设类高等学校信息系统（I类）、高等学校信息系统（II类）、中小学校（含中职中专院校）信息系统（III类）。

### 3.2 按信息系统业务对象划分

根据信息系统业务对象不同，部门信息系统可分为政务管理类、学校管理类、学生管理类、教师管理类、综合服务类；学校信息系统可分为校务管理类、教学科研类、招生就业类、综合服务类。

### 3.3 按信息系统部署模式划分

根据信息系统的部署模式，信息系统可以分为内部系统和统一运行系统。内部系统是指仅供本单位内部使用，实现本单位业务管理与服务的信息系统。统一运行系统是指供多家（级）单位共同使用，实现某项业务的跨单位统一管理和服务的信息系统。

统一运行系统可进一步分为集中式系统和分布式系统。集中式信息系统逻辑上是一套系统，在一个单位统一部署、管理和运行，多家（级）单位共同使用，实现信息系统、业务流程和数据的集中式管理；

分布式信息系统逻辑上是多套系统在多家（级）单位分别部署、管理和运行，通过技术接口实现信息系统、业务流程和数据的分布式管理。

## 4 信息系统的定级思路

信息系统的定级思路是在信息系统分类的基础上，参照国家对信息系统的安全保护等级标准的等级划分，形成教育行业信息系统安全等级划分建议。按主管单位不同，分别对部门信息系统和学校信息系统采取不同的思路进行分析，分别形成信息系统安全等级建议表。实际定级工作中，信息系统所定等级原则上不应低于建议等级。如遇未能涵盖的信息系统，可按照下述定级思路综合分析，确定安全等级。

### 4.1 定级思路概述

部门信息系统与学校信息系统分别定级。由于面向的对象不同、承载的业务不同、受到破坏后造成的侵害程度不同，采取不同的定级思路。

信息系统受到破坏后造成的危害程度与其安全等级正相关，造成的危害程度越大，安全等级应越高。

### 4.2 部门信息系统定级思路

部门信息系统根据行政级别、部署模式和业务类型与性质三个维度分析受到破坏后造成的危害程度。

行政级别与危害程度分析。行政级别与信息系统受到破坏后造成的危害程度正相关，级别越高则危害程度越严重，反之则相对较轻。

部署模式与危害程度分析。部署模式与信息系统受到破坏后造成的危

害程度正相关，涉及的单位越多则危害程度越严重，统一运行信息系统大于内部信息系统。

业务类型与性质的判断分析详见 4.4

### 4.3 学校信息系统定级思路

学校信息系统根据办学规模、社会影响力、业务类型三个维度分析受到破坏后造成的危害程度。

办学规模与危害程度分析。办学规模与信息系统受到破坏后造成的危害程度正相关，规模越大则危害程度越严重，高等学校信息系统大于中小学校信息系统。

社会影响力与危害程度分析。社会影响力与信息系统受到破坏后造成的危害程度正相关，影响力越大则危害程度越严重，“985 工程”学校和“211 工程”学校大于其他高等学校。

业务类型与性质的判断分析详见 4.4。

### 4.4 业务类型与性质的判断分析

业务类型与危害程度分析。承载教育教学管理与服务核心业务的信息系统较承载一般业务的信息系统受到破坏后造成的危害程度严重。教育教学管理与服务的核心业务包括学籍学历管理、学位管理、招生录取管理、考试考务管理、教师管理、门户网站管理等。

业务连续性与危害程度分析。业务的连续性要求与信息系统受到破坏后造成的危害程度正相关，连续性要求越高，其受破坏危害越严重；

业务数据重要性与危害程度分析。业务数据的重要性要求与信息

系统受到破坏后造成的危害程度正相关，涉及的国家安全、个人隐私和相关数据的信息系统，其受破坏危害更严重。

## 5 信息系统的定级工作流程

教育行业信息系统安全等级保护应坚持“自主定级、自主保护”的原则，依据《信息系统安全等级保护定级指南》的定级原理、方法，参照本指南的信息系统类型划分、定级思路组织开展信息系统定级工作。

### 5.1 确定定级责任主体

信息系统应明确定级工作的责任主体。按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，信息系统的主管单位为定级工作的责任主体，负责组织运维单位、使用单位开展信息系统定级工作。集中式信息系统由信息系统牵头建设单位负责组织信息系统定级工作。分布式信息系统由牵头建设单位负责组织信息系统定级工作，确定中心信息系统安全保护等级；各分支信息系统的主管单位参照中心系统的安全保护等级自主组织定级工作。信息系统的运维单位应协助主管单位完成定级过程中的具体技术支撑工作。

### 5.2 自主定级

主管单位对本单位信息系统进行梳理分析，参考附表 2 的建议等级进行自主定级，确定信息系统安全保护等级。对于承载复杂业务的信息系统，安全保护等级可高于建议等级；对于承载多个业务的信息系统，应以所承载业务的信息系统的最高建议等级进行定级。

### 5.3 专家评审

主管单位完成信息系统自主定级后，需聘请有关信息安全等级保护专家对信息系统自主定级情况进行评审，形成评审意见。拟确定为第四级及以上的信息系统，由教育部邀请国家信息安全保护等级专家评审委员会进行评审；拟确定为其他等级信息系统可由定级责任主体自行聘请专家进行评审。

#### 5.4 主管部门审核批准

主管单位完成信息系统专家评审后，需填写《信息系统安全等级保护定级报告》、《信息系统安全等级保护备案表》和信息系统安全等级保护专家评审意见等材料。各级教育行政部门将相关材料报送至上一级教育行政部门进行审核，直属事业单位和各级各类学校按照隶属关系将相关材料报送至所属教育行政部门或有关部门进行审批。

#### 5.5 公安机关备案

经审核批准的二级以上信息系统，由其主管单位负责组织到所在地设区的市级以上公安机关办理备案手续。教育部全国联网统一运行系统由教育部统一向公安部备案，其在各地运行、应用的分支系统，由主管单位组织向所在地公安部门备案，确定为三级以上信息系统同时报教育部备案。

### 6 等级变更

信息系统运行过程中，当系统状态变化可能导致业务信息安全或系统服务受到破坏后的受侵害对象和受侵害程度有较大的变化时，应根据具体情况重新定级，并变更等级。