

# 安徽理工大学现代教育技术中心文件

教技〔2021〕12号

## 安徽理工大学网络安全监测预警和信息通报 实施办法

### 第一章 总则

第一条 为了切实加强网络安全保障工作，有效防范网络安全事件的发生，维护学校网络和信息系统安全，依据《中华人民共和国网络安全法》和安徽省教育系统党委（党组）网络安全责任制落实考核评价相关文件中对安全监测预警和信息通报工作的要求，结合学校实际情况制定本办法。

第二条 网络安全监测预警和信息通报工作应遵循“及时发现、科学认定、有效处置”的原则，通过建立监测预警和信息通报机制，对风险进行预警，做到“早发现、早报告、早处置”，防止和减少不良信息的传播，确保信息网络的畅通和安全。

第三条 本办法中所包含的监测预警和信息通报工作的内容指网络和信息系统技术安全事件和安全隐患，不包含信息内容安全事件及网络舆情监测预警。

第四条 网络安全监测预警和信息通报工作由现代教育技

术中心负责。

## 第二章 监测机制

第五条 现代教育技术中心通过网络监测设备对全校网络环境进行实时监测，监测内容主要包含通信线路状态、网络设备运行状况、网络流量和网络基础服务等，发现异常情况，及时处理。

第六条 现代教育技术中心通过技术手段对全校信息系统和网站进行安全监测及防护，监测内容主要包含弱口令、信息泄露、服务器及信息系统漏洞、恶意攻击等各类网络安全隐患。

第七条 各单位按照“谁主管谁负责”的原则负责对本单位信息系统及网站开展日常安全检测。检测范围包括但不限于以下内容：

1. 信息系统和网站有无异常情况；
2. 账号密码管理是否规范，是否存在弱密码，重要业务系统是否定期更换管理账号的密码；
3. 服务器重要数据是否定期进行备份；
4. 网站及信息系统发生变更时及时备案，对新变更的系统部分及时跟踪；
5. 确保信息先审后发；
6. 是否定期对服务器操作系统、杀毒软件进行升级。

## 第三章 预警机制

第八条 网络安全预警信息来源以教育部、省教育厅等上级机关以及国内外安全组织发布的网络安全威胁信息为主。

第九条 现代教育技术中心负责汇集可能对我校网络安全产生威胁的有关网络安全信息，在进行分析和研判的基础上制

定解决方案。

#### **第四章 信息通报机制**

第十条 信息通报内容的来源主要包括上级有关部门通报的和现代教育技术中心自主监测发现的安全问题。

第十一条 现代教育技术中心在发现学校网络和信息系統存在安全隐患或发生安全事件后，将安全通报发送给责任部门，并协助事发单位确定事件规模和影响范围。

第十二条 各单位在收到网络安全事件通报后，应根据《安徽理工大学网络信息类突发事件应急处置预案》立即进行处置，在规定时间内完成整改并撰写整改报告，整改报告由网络安全第一责任人签字并加盖公章后报送至现代教育技术中心，现代教育技术中心复核整改情况，向分管网络安全的校领导汇报，根据需要向上级部门报送相关材料。

第十三条 发生网络安全事件的部门应当按照流程及时且如实地报告事件的有关信息，积极完成整改工作，不得瞒报、缓报。对出现瞒报、缓报、漏报和整改不力等失职情况，学校将予以通报批评。对造成严重后果的，将视情节追究相关领导和人员责任。

#### **第五章 附则**

第十四条 本办法自发布之日起执行。

第十五条 本办法由现代教育技术中心负责解释。