

河南工业大学

网络与信息系统安全日常监测管理规程

为加强河南工业大学网络与信息系统安全日常监测管理工作，依照国家法律法规和《河南工业大学网络系统安全管理办法》，制定本实施细则。

一、人员管理

1、信息化管理中心作为校园网网络与信息系统的主管单位，负责全校信息化建设与管理。核心机房必须设置专人管理，严格执行《河南工业大学核心机房日常运行及环境安全监控制度》，做好网络和信息 systems 安全日常监测管理。

2、信息化管理中心要健全各类规章制度，对网络与信息系统安全管理员（以下简称“安全管理员”）开展规范管理。安全管理员要严格执行《河南工业大学网络系统安全管理规定》、《河南工业大学信息系统测试通报制度及系统版本管理办法》等相关规定。

3、做好全面的安全管理员登记。安全管理员岗位变动时，及时更改安全管理员权限，防止信息泄露。通过学习、培训等形式，加强安全管理员业务能力与水平提升。

4、各单位网络与信息系统安全责任人应签订《河南工业大学网络及信息系统安全责任协议》，并报信息化管理中心登记备案。各单位网络与信息安全相关重点岗位人员，如网站与系统管理员、网络管理员、网络与信息安全管理等，须签订《河南工业大学数据保密协议》，并报信息化管理中心登记备案。

5、非管理人员访问核心机房等重要区域，须经过信息化管理中心批准，由核心机房管理人员陪同，并做好进出记录。

二、系统管理

1、信息化相关软硬件设备、系统采购，需报信息化管理中心审批，并严格遵守国家相关法律法规。

2、信息化相关软硬件应在测试环境下经过运行测试和安全检测，未经测试、验收或验收不合格的不得交付使用。

3、学校各网络信息系统的建设管理单位作为安全等级保护的责任主体，应当按照国家等级保护相关管理规范、技术标准确定网络信息系统的安全等级，以及各级别安全和管理的内容。涉密信息系统应当根据国家涉密信息保护的基本要求，按照学校保密工作部门有关涉密信息系统分级保护管理规定和技术标准进行建设和保护。

4、对新建、改建、扩建的网络信息系统，信息化管理中心应当在规划、设计阶段确定信息系统的安全等级，并要求同步建设符合该安全等级要求的信息安全设施。

5、信息化管理中心应当建立信息系统安全状况日常检测工作制度，应当按照国家有关管理规范和技术标准，定期对信息系统安全状况、安全制度及措施的落实情况进行自查。

6、信息化管理中心应落实以下安全管理措施：

（一）安全教育和安全培训，核实、登记并及时更新用户注册信息；

（二）系统重要数据管理、备份、容灾恢复措施，做好信息发布审核、登记、保存、清除和备份；

（三）计算机病毒等破坏性程序的防治措施，防范网络入侵、攻击破坏等危害网络安全行为的措施，密钥、密码安全管理措施，确保网络信息安全；

（四）系统运行和用户使用日志备份并保存六十日以上的措施，协助违法案件查处；

（五）国家和河南省规定的其他安全技术措施。

三、监测管理

1、运用现有的安全设备、技术手段对校园网网络和信息系统进行防护。主要包括出口防火墙，入侵保护系统 IPS，网页防火墙 WAF，漏洞扫描，日志审计，运维监控管理，上网行为管理，堡垒机等。

2、综合运用各项技术，提高信息系统的防护能力。利用核心机房展示大屏，实时监控和展示各项系统应用的运行状态。

3、建立日常监测管理制度。安全管理员严格执行日常监测管理制度，做到早发现，早隔离，早处理。

四、校外技术人员管理

1、实行信息技术服务外包的单位，应重视外包服务的保密管理工作，选择具有国家专业资质认证的外包服务提供商，与其签订网络与信息系统安全保密协议，并在外包服务合同中明确安全与保密责任。

2、外包服务原则上不得采用远程在线方式，确需远程服务时须采取书面审批、访问控制、在线监测、日志审计等安全防护措施。现场服务过程中也须安排专人管理，并记录服务过程。

3、外包开发的系统、软件上线前，必须通过信息化管理中心的安全测评。

五、其他

本实施细则自发布之日起实施，由信息化管理中心负责解释。

信息化管理中心

2020年4月21日