常 熟 理 工 学 院 文 件

常理工信〔2022〕1号

关于印发《常熟理工学院落实网络安全工作责任制考核实施办法》的通知

各二级学院（部）、各部门、各直属单位：

《常熟理工学院落实网络安全工作责任制考核实施办法》已经校长办公会审议通过，现予印发，请遵照执行。

常熟理工学院

2022年7月13日

常熟理工学院
落实网络安全工作责任制考核实施办法

第一条 根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规，认真贯彻《关键信息基础设施安全保护条例》等文件精神，按照中共中央办公厅印发的《党委（党组）网络安全工作责任制实施办法》和中共教育部党组印发的《教育系统落实党委（党组）网络安全责任制的实施细则》《教育系统党委（党组）网络安全责任制落实考核评价办法》要求，为加强网络信息安全管理，落实网络安全主体责任，结合学校实际情况，制定本实施办法。

第二条 二级学院（部）党委书记、机关部门和直属部门负责人是网络信息安全工作的主要负责人，对本单位网络信息安全工作负总领导责任，同时负有组织、管理、监督、检查、奖惩的权利和责任。各单位应指定本单位网络安全联络员，负责本单位网络信息安全管理及日常事务工作。

第三条 考核对象为学校二级学院（部）、机关部门和直属单位。

第四条 考核以网络信息安全工作基本要求为底线指标，以日常工作为考核依据，充分发挥考核在促进学校网络信息安全工作责任制落实中的主导作用。

第五条 考核实施办法评分细则包括 8 个方面共 22 个子项，满分为 100 分。具体考核内容、分值和评分标准详见《常熟理工学院落实网络安全责任制考核评分细则》。

第六条 考核每年一次，考核事项时间范围为每年的 1 月至 12 月。

第七条 年度内发生严重网络信息安全事件，被上级主管部门问责的部门，当年网络信息安全考核实行一票否决，并按有关规定追责问责。

第八条 每年 12 月形成年度初评结果并报送学校各部门确认，初评结果根据各部门反馈情况进行完善后，形成年度考核建议结果；经学校党委审定后，形成年度考核结果。

第九条 考核结果纳入二级学院（部）、机关部门和直属单位年度综合考核。

第十条 考核工作由学校党委统一领导，信息化办公室负责具体实施。

常熟理工学院落实网络安全责任制考核评分细则

序号	内容	工作要求	分值	评分细则
1	领导责任制建设	落实网络安全责任主体，确定本单位网络安全主要负责人、网络安全联络员并及时上报。	5	按要求报送人员信息并及时上报变更信息，得满分； 未按要求报送或上报信息不准确或变更信息未及时报送，不得分。
2		网络安全主要负责人每年签订《常熟理工学院网络安全承诺书》，如发生人员变更，应重新签订《常熟理工学院网络安全承诺书》并及时上报。	4	签署承诺书，得满分； 未签订承诺书，或更换主要负责同志未及时重新签订承诺书，不得分。
3	工作研究部署	每年至少召开一次专题会议研究部署网络安全工作。	3	按要求召开专题会议，得满分； 未按要求召开专题会议，不得分。
4		主要负责人应参加学校每年组织的网络安全专题工作会议或培训。	3	按要求参加，得满分； 未按要求参加，每缺席一次扣 1 分。
5	信息系统管理	准确掌握本单位的信息资产信息，建立信息系统名录，并报信息化办公室备案，如信息有变更应及时上报。	5	按要求全面、准确报送信息，得满分； 未按要求报送信息，不得分； 报送信息不准确，每个系统扣 1 分。
6		加强信息系统工程技术资料的归档与管理，新建或新购系统应按如下技术资料归档并报信息化办公室。产品软件：采购合同、产品使用手册或技术手册；软件系统（自主研发或外包）：招投标文件、采购合同、需求分析文档、系统设计文档、系统数据字典、系统部署文档、安全测评报告、产品使用手册等。	5	按要求全面、准确报送信息，得满分； 未按要求报送信息，不得分； 报送信息不完整或不准确，每个系统扣 1 分。
7	网络安全日常检查	每半年组织开展一次网络安全自查，对各类问题隐患及时整改，形成自查报告并及时上报。	3	按要求开展网络安全自查并及时报送自查报告，得满分； 未按要求开展网络安全自查和及时报送自查报告，不得分。
8		积极配合学校以及上级部门开展网络安全现场检查，发现问题及时处置和整改，形成整改报告并及时上报。	3	未按要求配合现场检查或不及时整改和报送整改报告，不得分。
9		全面清理问题信息系统（僵尸信息系统、“双非”信息系统等）。	4	按要求全面清理问题信息系统，得满分； 未全面清理问题信息系统，每个问题系统扣 2 分。
10		各单位网站应通过学校站群统一对外提供服务，集中管理。	6	全部网站进学校站群，得满分； 未按要求进站群系统，一个扣 2 分。

11		严格执行补丁升级、及时修复漏洞、升级杀毒软件。	3	按要求严格执行安全措施，得满分； 未严格执行安全措施,每个系统扣1分。
12		及时维护本单位信息系统，优化安全策略，杜绝漏洞、后门、暗链、弱口令等。 避免通过远程桌面或远程登录后台管理系统。 设置账户登录次数限制，防止暴力破解。 杜绝弱口令、默认口令、通用口令、长期不变口令，防止高危漏洞不修复、非必要端口长期开启、陈旧版本基础软件和通用软件不更新、僵尸主机和系统不整改。	4	按要求严格执行安全措施，得满分； 未严格执行安全措施,每个系统扣1分。
13		保障个人隐私数据和重要业务数据安全。严格控制数据采集范围、数据访问授权，及时发现处置非授权访问、大流量数据异常外传等情况。	4	发生数据安全相关问题（隐私信息泄露、过量采集信息、数据管控漏洞等），一次扣2分。
14		加强公共区域LED显示屏和网络打印机等物联终端及其控制系统的管理，明确专人负责，避免使用远程或无线方式管理，防范内容被篡改。	3	按要求加强物联终端及其控制系统的管理或没有物联终端及其控制系统，得满分； 未按要求加强物联终端及其控制系统的管理，每个物联终端及其控制系统扣1分。
15		加强系统访问日志记录和日常审计，系统访问、操作日志保存6个月以上。	3	按要求加强系统访问日志记录和日常审计，日志留存6个月以上，得满分； 未实现系统访问日志记录和审计或日志留存不足6个月，每个系统扣1分。
16	等级保护工作	协助信息化办公室完成本单位信息系统的定级备案。	4	本单位信息系统均完成备案，得满分； 未完成备案，每个系统扣2分。
17		根据网络安全等级保护测评结果进行整改。	4	整改措施得当、通过等保测评,得满分； 整改不到位导致测评不合格，每个系统扣2分。
18	重要时期网络安全保障工作	重要时期信息系统应采取限制互联网访问控制措施。 在重要时期因实际工作需要提供互联网访问服务的应采取以下措施： 1）确保上线信息系统安全隐患清零； 2）设置专人专岗24小时值守； 3）执行零报告制度（每天16时报告前一天16点至当日16点网络安全工作情况、问题隐患及整改处理情况）。	10	采取限制互联网访问措施，得满分； 未采取限制互联网访问控制措施或措施落实不到位，按以下标准扣分； 未能确保安全隐患清零的,扣3分/系统； 未设置专人专岗24小时值守的，扣3分/系统； 未执行零报告制度，扣4分/系统。
19	网络安全事件处置	制定本单位的网络安全事件处置流程，并报信息化办公室。	3	按规定制定报送，得满分； 未制定或未报送，不得分。
20		配合学校开展网络安全应急演练。	3	按规定履行应急演练义务，得满分； 未按规定履行应急演练义务，不得分。

21		发生网络安全事件后，应按照学校《信息技术安全事件报告与处置流程》要求处置并报告信息化办公室。发生网络安全事件应及时报告、快速响应、科学处置，将影响降到最低（30 分钟内停止对外服务，在 5 个工作日内完成整改）。	10	本年度未发生网络安全事件，得满分； 发生网络安全事件，报告及时、处置得当，未造成负面影响，一次扣 2 分； 发生网络安全事件，漏报、瞒报或处置不及时，造成社会负面影响的，一次扣 4 分； 发生重大事件且处置不及时，造成社会负面影响的，不得分并追责问责。
22	网络安全相关宣传教育培训	积极组织本单位在职人员参加网络安全教育培训，年度人均培训时间不少于 4 个学时；信息化管理人员和技术人员年度人均培训时间不少于 8 个学时。	8	本单位在职人员人均学时低于 4 个学时，按达到 4 学时人数占单位在职人员总人数的比例记分。

1.信息系统：是指学校建设、运行、维护或管理，并支撑学校教学、科研和管理等各项业务的所有信息系统和网站，包括但不限于业务系统、网站、移动应用（APP）。其中移动应用（APP）是指教育行政部门和学校引入的，用于支撑学校教学、科研、管理、服务的校园移动互联网应用程序，包括但不限于基于移动设备操作系统的原生应用、微信企业号、QQ 校园号、具有业务交互功能的微信小程序、微信公众号、QQ 小程序、钉钉企业应用。

2.各项考核内容的扣分上限为该项的分值。