

中共哈尔滨工程大学委员会文件

哈工程党发〔2018〕82号

中共哈尔滨工程大学委员会关于印发 《哈尔滨工程大学网络信息安全 管理办法（试行）》的通知

各分党委、党总支，各处级单位：

《哈尔滨工程大学网络信息安全管理办法（试行）》经学校第四届党委第17次常委会会议研究通过，现印发给你们，请遵照执行。

中共哈尔滨工程大学委员会

2018年12月24日



哈尔滨工程大学网络信息安全管理办法

（试行）

第一章 总 则

第一条 为深入贯彻中央关于网络安全工作的总体部署，保障哈尔滨工程大学网络信息安全，加强学校党委对网络信息安全工作的领导，促进学校信息化建设健康有序发展，根据《中华人民共和国网络安全法》等相关法律法规和文件要求，结合学校实际，制定本办法。

第二条 本办法所称网络信息安全工作，是指为使由学校建设、运行、维护或管理的网络基础设施、网站、信息系统及业务数据信息的机密性、完整性、可用性等得到保持、不被破坏所开展的相关管理和技术工作。

第三条 学校按照“谁使用谁负责，谁主管谁负责，谁运维谁负责”和“同步规划、同步建设、同步运行”的原则，明确和落实学校各单位网络安全责任，全面实施网络安全等级保护制度。

第四条 学校各单位和全体师生应严格遵守国家相关法律法规，并按照本办法要求及学校相关标准规范履行网络信息安全的义务和责任。

第二章 组织保障

第五条 哈尔滨工程大学网络安全和信息化领导小组是学校网络安全领导机构，贯彻落实中央和上级单位关于网络安全战略部署，组织领导学校网络安全工作，统筹、沟通、协调学校网络安全工作中的重大事项、重大问题，提出相关方案或建议。

第六条 信息化处作为学校网络安全和信息化领导小组办公室，负责网络信息安全管理，具体职责包括：

（一）负责领导小组日常工作，归口管理、协调网络安全，向领导小组提出工作建议。

（二）指导、监督、检查网络安全各项重点任务落实，统筹管理、推进学校网络安全和信息化工作。

（三）建立网络安全联络机制，负责联系学校相关部门、构建安全高效的联络渠道。

（四）及时向上一级网络安全和信息化办公室和所在地区网络安全职能部门报告网络安全信息。

（五）加强和规范网络安全信息汇集、分析和研判工作，建立网络安全专家咨询机构，分析、研判网络安全态势，服务网络安全决策。

第七条 相关单位职责

（一）党政办公室负责与上级部门的沟通协调、网络信息安全管理政策发文、学校重大突发网络安全事件的统筹协调等工作。

（二）党委宣传部负责网络意识形态阵地的舆情监管，负责对校园网络信息内容的编排、维护、语言使用规范等进行指导和监督。

（三）安全保卫处负责协助重大网络安全事件的调查处理，负责网络信息安全相关的安全保卫工作。

（四）保密处负责对学校网络信息安全保密工作落实情况进行监督、指导和检查。

（五）网络信息中心作为网络信息安全技术支撑单位，负责学校网络信息安全技术防护体系的建设、运行维护、技术指导和

服务支持。

第八条 各学院、机关和直属单位是本单位网络信息安全责任主体，负责本单位（含本单位的组织及个人）网络信息安全工作，各单位主要负责人是本单位网络信息安全工作第一责任人。具体职责包括：

（一）落实本单位网络安全等级保护相关工作。

（二）负责本单位网站和信息系统的日常监管与安全管理，及时处理安全隐患。

（三）明确网络信息安全工作的分管领导，并设置网络信息安全联系人，负责本单位网络信息安全具体工作，人员信息及时报信息化处备案。

第三章 校园网与 IT 基础环境安全管理

第九条 校园网与 IT 基础设施由信息化处统一规划、管理。网络信息中心负责学校核心机房的建设、运行和维护，实施 24 小时专人监管。学校核心机房的消防、视频监视录像、门禁等设施的规划、建设、运行和维护按学校安全保卫工作要求落实。

第十条 校园网接入实行审批和备案登记制度，校园网访问实行实名认证上网制度。

第十一条 学校按照网络安全等级保护相关要求将校园网划分网络安全域，并采取必要的安全隔离措施，按照规定留存相关网络日志不少于 6 个月。信息化处负责监测和检查校园网安全运行状况，紧急情况下，可采取“先断网、后处理”的应对措施。

第四章 网站与信息系统安全管理

第十二条 各单位应按照国家 and 学校相关要求，开展本单位网站和信息系统的网络安全等级保护相关工作，并接受学校和上

级有关部门监督检查。

第十三条 各单位在网站和信息系統建设阶段应确定网络安全保护等级，按照“积极防御、综合防范”的原则，按网站和信息系統已确定安全保护等级，同步落实网络安全等级保护要求。

第十四条 各单位网站应基于学校统一的站群管理平台建设。对于阶段性使用的网站或无人管理、无力维护、长期不更新的网站，应关闭网站以降低安全风险。

第十五条 使用“哈尔滨工程大学”中英文校名、“哈工程”简称、校徽、学校域名、学校 IP 地址等情况的网站和信息系統，原则上必须校内部署。存储学校教学、科研、财务、人事等重要信息及其它涉及学校基础数据、师生员工个人信息的信息系統，原则上必须校内部署且应在校园网环境下访问。特殊需求须报信息化处审批。

第十六条 网站和信息系統上线前，应进行登记备案。通过学校安全检测的网站和信息系統才能上线运行，并按照学校要求统一进行管理维护。

第十七条 网站和信息系統的内容安全由开办单位负责，各单位应建立完善的信息发布与审核制度，并报信息化处备案，定期全面检查网站信息发布情况，禁止发布涉密信息、个人隐私信息和其他敏感信息。

第五章 数据信息安全管理

第十八条 各单位对产生和使用的数据安全负责，不得收集与业务无关的个人信息，应当按照网络安全等级保护要求落实安全管理和技術措施，规范数据的收集、存储、传输和使用，确保数据安全。未经审批，不得对外发布和提供数据信息。

第十九条 各单位应严格管理业务数据的增加、修改、删除等变更操作，按照数据的重要程度，对数据进行分类管理，适时进行业务数据有效性检查，做好数据备份工作。

第六章 校园网用户与终端安全管理

第二十条 校园网用户必须本人实名认证上网，必须严格遵守国家相关法律法规，上网行为不得危害到学校网络信息安全，并对上网产生的一切行为负责。

第二十一条 校园网用户应做好计算机等使用终端的安全防护工作，应设置系统登录账号和复杂度高的密码，安装正版操作系统、办公软件和防病毒软件，及时更新系统补丁，修补漏洞。

第七章 账号密码与密钥安全管理

第二十二条 各单位应落实账号密码与密钥使用管理责任，账号应采用分级授权管理，根据用户角色创建相应级别账号，重要账号应建立 AB 角工作责任制。账号的权限设置应遵循“最小化”原则，即给用户能完成工作的最小权限。

第二十三条 不得使用默认账号密码，禁止所有匿名账号，应设置复杂度高的密码，并定期更换密码，不得共享、公开账号密码。各单位应及时收回离岗、离职人员的管理账号密码以及学校提供的数据存储介质、软硬件设备，并签署安全保密承诺书。

第八章 监测预警与应急处置

第二十四条 各单位应加强对所属网站和信息系统的日常监管，做到安全事件早发现、早报告、早控制、早解决。对发现的网络安全问题及时整改并报告信息化处。

第二十五条 信息化处负责对学校网络信息安全情况进行监测与检查，对于检查不合格的网站和信息系统，视其安全问题级

别进行关停、限制校内访问等处理。

第二十六条 信息化处负责制定网络信息安全事件应急预案，定期组织网络信息安全突发事件应急演练。学校各单位应做好网络信息安全应急响应工作。

第九章 附 则

第二十七条 对于违反本办法的，产生网络信息安全事件的单位及个人，给予通报批评；情节严重的，追究其主管领导、相关部门负责人及直接责任人的责任；构成犯罪的，依法追究刑事责任。网络信息失泄密事件按照国家和学校相关法律法规和规章制度处理。

第二十八条 本办法由学校信息化处负责解释。

第二十九条 本办法自 2019 年 1 月 1 日起施行。

哈尔滨工程大学党政办公室

2018 年 12 月 24 日印发