哈尔滨工业大学网络安全实施细则

（试行）

第一章 总则

第一条 为加强学校对网络安全工作的组织管理，提高网络安全防护能力和水平，保障各项事业健康有序发展，根据国家、教育部有关网络安全文件要求，结合近年来实际工作，特制定本细则。

第二条 学校网络安全，包括校园计算机网络（以下简称校园网络）与信息系统（含网站，下同）的运行安全和信息内容的安全。

本细则适用于使用校园网及使用学校信息系统的任何用户，本实施细则所指学校各单位包括各机关部、处、室，学部、学院、直附属单位以及有关科研机构等。

第三条 按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，建立健全网络安全责任体系，学校各单位、全体师生员工应依照本实施细则要求及相关标准规范履行网络安全的义务和责任。

第二章 管理体制和职责

第四条 学校网络安全和信息化领导小组负责统一领导、统一谋划、统一部署全校网络安全和信息化发展，统筹制定网络安全和信息化发展战略、宏观规划和重大政策，研究解决网络安全和信息化重要问题，建立网络安全长效监督机制。

第五条 网络与信息中心作为学校网络安全技术支撑部门，受学校网络安全和信息化领导小组监管，负责学校网络安全防护系统的建设、运行维护、技术指导和服务支持，保障网络与信息系统的正常运行；保存网络运行日志，配合调查取证；负责入网单位和个人办理入网登记手续，签署相应的安全责任书。

第六条 党委宣传部依据学校《落实意识形态工作责任制实施细则》《全媒体管理办法》《重大舆情处置办法》等相关规定，统筹网络舆论正向引导和网络重大舆情处置，必要时启动追责问责程序。

第七条 党委安全保卫部负责对网络违规行为进行调查、 取证、处理，根据相关证据及事态影响或破坏程度，对违规者按照有关规定进行处理。

第八条 网络与信息系统的主办单位承担安全监管责任，包括内容安全监管、技术安全保障和监督检查等职责；网络与信息系统的使用单位和个人对系统操作与信息内容的安全监管承担直接责任。网络与信息系统通过外包服务方式进行维护的，主办单位负责督促外包服务单位做好安全运维工作，网络与信息系统的安全监管责任主体仍为主办单位。

第九条 各单位应明确主管领导为本单位网络安全工作的负责人，负责落实本单位网络安全工作。各单位应指定专人担任网络安全管理员，负责本单位及下属单位的网络安全保护措施的落实，对上网人员进行网络安全教育和培训，与网络与信息中心协同配合，共同做好本单位网络安全运行、管理和维护工作。

第三章 校园网络安全

第十条 校园网络是指连接学校各单位信息系统及信息终端的计算机网络，包括校园有线网络、无线网络和各种虚拟专网。

第十一条 校园网络由网络与信息中心统一出口、统一管理和统一防护。未经批准，学校各单位在校园内不得擅自通过其他渠道接入互联网及其他公共信息网络。

第十二条 校园网络设备，其管理、维护等均由网络与信息中心统一负责，未经网络与信息中心批准，不得以任何方式试图登录、修改、设置、破坏校园网内的交换机、路由器和服务器等。

第十三条 网络与信息中心应采取访问控制、安全审计、完整性检查、入侵防范、恶意代码防范等措施加强校园网络边界防护。

第十四条 网络与信息中心负责校园网信息系统（网站）的上线和互联网访问的承载和管理，任何单位和个人不得私自承载。根据教学和科研实际工作需求，确实需要建立信息系统（网站）承载业务的，经网络与信息中心批准后方可承载运行。

第十五条 需要承载信息系统（网站）业务的单位，须向网络与信息中心提出书面申请，由网络与信息中心进行环境安全评估、备案后方可提供承载服务；网络安全方面受学校网络安全和信息化领导小组、信息化工作办公室监管，须遵守国家法律法规和校内有关规章制度，按照要求建立应急响应机制，落实网络安全责任人联系制度，依法提供网络服务。

第十六条 师生员工接入校园网络，实行“实名注册、认证上网”制度；学校非涉密信息系统接入校园网络，实行接入审批和备案登记制度。涉密信息系统不得接入校园网络。

任何单位和个人不得窃取或盗用他人的用户名、口令、IP 地址和 MAC 地址等。

第十七条 接入校园网的机房、电子阅览室等一律不准对社会开放，上网人员必须持有校园“一卡通”或凭学生证、工作证等有效证件登记后，方可上网。机房必须安装管理软件，自动记录上网人员身份和上下网时间、机号、IP 地址等，网络使用记录保持时间不得少于 6 个月。

第十八条 校园网络接入单位负责提供本单位所需的网络设备间和电源保障，负责其安防和消防安全管理。

第四章 信息系统及其数据安全

第十九条 信息系统数据是指信息系统收集、存储、传输、处理和产生的各种电子数据，包括但不限于网站内容、业务数据、网络课程、图书资源、日志记录等。

第二十条 信息系统数据的所有者是数据安全管理的责任主体，应当落实管理和技术措施，规范数据的收集、存储、传输和使用，确保数据安全。

第二十一条 信息系统数据收集应遵循“最少够用”原则，不得收集与信息系统业务服务无关的个人信息。按照“谁收集，谁负责”的原则，收集个人信息的单位是个人信息保护的责任主体，应当对其收集的个人信息严格保密，并建立健全相关保护制度。

第二十二条 网络与信息中心负责学校核心信息系统的备份与恢复管理，制订备份与恢复计划，根据业务实际需要对重要数据和信息系统进行备份，定期测试备份与恢复计划，并确保备份数据和备用资源的有效性。

第二十三条 任何单位和个人，不得私自设立校园网服务器或自建联网的应用系统。根据教学和科研实际工作需求，确实需要建立应用系统的，经网络与信息中心批准后方可联网运行。

第二十四条 需要开设联网信息服务的单位，须向网络与信息中心提出书面申请，由网络与信息中心进行技术评估、备案后方可对外提供服务；应遵守《哈尔滨工业大学校园网信息系统（网站）安全管理条例》及相关规章制度；服务器必须具有保持日志记录功能，历史记录保持时间不得低于 6 个月。

第二十五条 接入互联网的服务器及应用系统，应该采取必要的网络安全防护措施、安装防护软件，并将防护措施上报网络与信息中心备案。

第二十六条 网络与信息中心有权对各单位服务器和应用系统进行必要的安全检查和评测，对达不到安全要求的，关闭对外服务，整改合格后系统方可上线运行。

第五章 互联网网站安全

第二十七条 学校各单位开办互联网网站，应使用学校互联网域名和互联网 IP 地址，并遵守《哈尔滨工业大学校园网信息系统（网站）安全管理条例》及相关规章制度。

第二十八条 网络与信息中心统一建设学校网站集群平台并负责纳入该平台网站的技术安全。未纳入学校网站集群平台的网站，其技术安全由网站开办单位负责。

第二十九条 学校各单位开办互联网网站应优先选择学校网站集群平台，集群平台不能满足需求时可委托其他供应商管理。网站投入试运行后，通过网络与信息中心组织的安全检查方可正式上线。

第三十条 互联网网站运行维护单位应建立网站值守制度，制订应急处置流程，组织专人对网站进行监测，发现网站运行异常及时处置。

第三十一条 互联网网站的内容安全由网站开办单位负责。互联网网站开办单位应建立完善的网站信息发布与审核制度，确定负责内容编辑、内容审核、内容发布的人员名单，明确审核与发布程序，保存相关操作记录。

第三十二条 原则上，学校各单位不得提供电子公告服务。确有需要，经批准备案后方能提供电子公告服务。提供电子公告服务的互联网网站开办单位承担电子公告服务内容管理的主体责任，并按国家有关规定落实专项安全管理和技术措施。

第六章 电子邮件安全

第三十三条 网络与信息中心为学校各单位和师生员工提供电子邮箱服务，并负责学校电子邮件的安全管理。学校各单位和师生员工使用学校电子邮箱应遵守学校电子邮箱管理等相关规章制度。

第三十四条 网络与信息中心应采取必要的技术和管理措施，加强电子邮件系统安全防护，减少垃圾邮件、病毒邮件侵袭。

第三十五条 全校师生员工须对使用其电子邮件帐号开展的所有活动负责，应妥善保管本人使用的电子邮箱账号和密码，确保密码具有一定强度并定期更换。师生员工如发现他人未经许可使用其电子邮箱，应立即通知网络与信息中心处理。

第七章 终端计算机安全

第三十六条 终端计算机是指由学校师生员工使用并从事学校教学、科研、管理等活动的各类计算机及附属设备，包括台式电脑、笔记本电脑及其他移动终端。

第三十七条 终端计算机使用人按照“谁使用，谁负责”的原则，对其终端负有保管和安全使用的责任。网络与信息中心对终端计算机的安全管理提供技术支持和指导。

第三十八条 终端计算机设备上安装、运行的软件应为正版软件。在终端上使用盗版软件带来的安全和法律责任由终端使用人承担。

第三十九条 终端计算机应当设置系统登录账号和密码，登录密码应具有一定强度并定期更改。

第四十条 终端计算机使用人应做好数据日常管理和保护，定期进行数据备份。非涉密计算机不得存储和处理涉密信息。

第四十一条 终端使用人应做好终端计算机的安全防范，如发现终端计算机出现可能由病毒或攻击导致的异常系统行为或其他安全问题，应立即断网后进行处置。

第八章 人员安全管理

第四十二条 学校各单位应建立健全本单位的岗位网络安全责任制度，明确岗位及人员的网络安全责任。关键岗位的计算机使用和管理人员应签订网络安全与保密协议，明确网络安全与保密要求和责任。

第四十三条 学校各单位应加强人员离岗、离职管理，严格规范人员离岗、离职过程，及时终止相关人员的所有访问权限，收回学校提供的软硬件设备，并签署安全保密承诺书。

第四十四条 学校各单位应定期对网络安全岗位的人员进行安全知识和技能的考核，并对考核结果进行记录和保存。

第四十五条 学校各单位应建立外部人员访问机房等重要区域的审批制度，外部人员须经审批后方可进入，并安排工作人员现场陪同，对访问活动进行记录和保存。

第四十六条 学校各外包服务需求单位应与网络信息系统开发和运维服务提供商签订网络安全与保密协议，明确网络安全与保密责任，要求服务提供商不得将服务转包，不得泄露、扩散、转让服务过程中获知的敏感信息和各类电子数据，不得占有服务过程中产生的任何信息资产，不得以服务为由强制要求委托方购买、使用指定产品。各单位签署外包服务合同时，应将学校统一制定的网络安全与保密协议作为合同附件。

第九章 网络安全应急管理

第四十七条 网络与信息中心负责学校网络安全应急工作的统筹管理，制定学校网络安全事件报告与处置流程，以及安全应急工作的技术支撑和保障。

第四十八条 网络与信息中心定期组织网络安全应急演练，评估并适时组织网络安全应急预案修订。学校各单位应组织开展网络安全应急预案的宣传、教育和培训，确保相关人员熟悉应急预案。

第四十九条 网络与信息中心负责组建学校网络安全应急队伍，完善 24 小时应急值守制度，提高网络安全事件的预防、预警和应对能力，预防和减轻网络安全事件造成的损失和危害。

第五十条 学校各单位应按照学校网络安全事件报告与处置流程，做好事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置工作。做到安全事件早发现、早报告、早控制、早解决。

第五十一条 学校各单位及师生员工均有义务及时向网络与信息中心报告网络安全事件，不得在未授权情况下对外公布、尝试或利用所发现的安全漏洞或安全问题。

第十章 网络安全教育培训

第五十二条 网络与信息中心负责组织学校网络安全宣传和教育培训工作，建立健全相关制度。

第五十三条 网络与信息中心定期组织开展针对师生员工的网络安全教育，提高师生员工的安全和防范意识。

第五十四条 网络与信息中心定期开展针对网络安全管理人员和技术人员的专业技能培训，提高网络安全工作能力和水平。

第十一章 网络安全检查监督

第五十五条 学校各单位定期对本单位信息系统的安全状况、安全保护制度及措施的落实情况进行自查，并配合有关部门的网络安全检查、信息内容检查、保密检查与审批等工作。

第五十六条 网络与信息中心对学校各单位的网络安全工作落实情况进行检查，对发现的问题下达限期整改通知书，责成相关单位制订整改方案并落实到位。

第五十七条 网络与信息中心对年度安全检查情况进行全面总结，按照要求完成检查报告并报学校网络安全工作委员会。

第十二章 网络安全责任追究

第五十八条 学校建立网络安全责任追究和倒查机制。

第五十九条 有关单位在收到网络安全限期整改通知书后，整改不力的，学校给予通报批评；玩忽职守、失职渎职造成严重后果的，依纪依法追究相关人员的责任。

第六十条 学校各单位应按照网络安全事件报告与处置流程及时、如实报告和妥善处置网络安全事件。如有瞒报、缓报、处置和整改不力等情况，学校将对相关单位责任人进行约谈或通报。

第六十一条 师生员工违反本实施细则规定的，由网络与信息中心责令改正，并通报批评；拒不改正或者导致危害网络安全

等严重后果的，根据学校有关规定给予以纪律处分。触犯法律的，移交司法机关处理。

第十三章 其它

第六十二条 涉及国家秘密的信息系统，执行国家保密工作的相关规定和标准，由校党委保密委员会办公室监督指导。

第六十三条 本实施细则在实施中若与国家有关法律、法规有不一致的，以国家法律、法规为准。

第六十四条 本实施细则自下发之日起实施，由网络与信息中心负责解释。学校原有相关规定与本实施细则不一致的，按本实施细则执行。