哈尔滨商业大学网络安全和信息化建设管理办法(试行)

第一章 总 则

第一条 为规范和加强学校网络安全、信息化建设和管理工作，保证网络安全和信息化建设的实效性与可持续发展，充分发挥信息化、数字化、数智化在教学、科研及管理方面的保障支撑作用，根据《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《信息安全等级保护管理办法》等法律法规精神，结合学校实际情况，制定本办法。

第二条 学校信息化建设坚持在学校党委领导下“统一领导、统一标准、统一平台、归口管理、分级负责、确保安全”的原则，实行学校、业务主管部门、使用部门分级管理制度，明确各部门职责范围与责任。

第二章 管理机构与工作职责

第三条 学校成立网络安全和信息化领导小组，领导小组下设办公室（简称网信办），办公室设在网络与教育技术中心。

第四条 网络安全和信息化领导小组负责统一领导、统一谋划、统一部署学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建设重要问题。其主要职责是:

（一）负责宣传贯彻上级网络安全和信息化建设方针、政策;

（二）审定学校网络安全和信息化建设发展的中长期规划;

（三）审定批准学校网络安全和信息化建设的重大项目立项;

（四）制定发布学校网络安全和信息化建设、运行管理的各项规章制度;

（五）推进网络安全和信息化工作及软硬件正版化国产化进程;

（六）统筹协调组织学校网络和信息系统安全事件的预防、监测、报告和应急处置工作;

（七）网络安全和信息化建设的其他工作。

第五条 网信办职责是:

（一）负责学校网络安全和信息化领导小组的日常工作;

（二）负责召集网信办联席会议，审定批准学校网络安全和信息化建设一般项目;

（三）领导小组指定的其他具体工作。

第六条 网络安全和信息化工作应列入学校各部门年度工作计划。各部门党委负责人是本部门网络安全和信息化建设工作第一责任人，负责本部门网络安全和信息化工作的推进和落实；各部门必须设置网络安全和信息化管理员（简称网信管理员），并报备学校网信办。网信管理员负责本部门网站及信息系统的日常管理、相关业务系统数据的更新和维护等具体工作。

第三章 信息标准和编码的管理

第七条 网信办参照国家、教育部相关标准制定并发布本校的信息标准、数据共享和交换规范，对信息标准实施统一管理，协调解决信息标准编制中的冲突，有权责令编制冲突相关部门进行整改。

第八条 各部门新开发的信息系统必须使用统一的信息编码，保持学校编码的唯一性，严格执行统一的信息编码，不得随意增加、删除编码。如需修订，须报网信办审核后统一修订。

第九条 已上线运行的信息系统，若信息编码规则与学校信息标准不一致，应使用学校信息标准进行替换，存在替换困难的，可暂时通过代码转换接入使用，待系统升级时更正。

第四章 网络安全和信息化建设项目管理

第十条 网络与教育技术中心负责管理、维护学校公共基础平台，包括但不限于校园网络、网络安全、VPN、域名、门户网站、统一身份认证、数据中心、虚拟机、云桌面、高性能计算、数据中心机房、学校综合业务应用服务管理信息系统等。

第十一条 数据中心是学校集成、共享公共基础数据的平台，校内各部门均须按网信办要求提供必要数据，以便实现各业务系统之间的数据共享，支撑数据分析及应用。

第十二条 各部门网络安全和信息系统建设必须符合学校信息化建设规划和有关规章制度的要求，按照学校统一的信息标准、数据交换规范进行建设，确保业务协同和系统共享，杜绝信息孤岛。网信办对建设项目进行技术支持、监督和检查评估。

第十三条 根据《国务院办公厅关于加强专家参与公共决策行为监督管理的指导意见》（国办发〔2024〕2号），学校建立信息化专家评审制度，设立专家库，配套评审预算。

第十四条 各部门网络安全和信息系统建设项目须报网信办审核汇总并经专家组论证后，按照项目类别分别报领导小组或网信办联席会议审议。

第五章 信息基础设施建设与管理

第十五条 学校信息化基础设施是指为学校师生提供网络信息服务的物质工程设施，包括：数据中心机房（含空调、UPS 等设备设施）、校园网络（含有线和无线）、信息化设备(含网络设备、安全设备、服务器、终端设备等)、云平台（私有云、云桌面、高性能计算）、校园范围内建设的各类通讯管线、通讯电缆和光缆、弱电设备间、楼内弱电布线等。

第十六条 学校信息化基础设施建设由网络与教育技术中心牵头组织实施，校内所有涉及信息化基础设施的建设均由使用部门向网络与教育技术中心申请资源，资源不足的由网络与教育技术中心向学校申请资金建设。

第十七条 学校基建工程应将工程范围内的信息化基础设施（如楼宇网络等）建设纳入工程预算及实施验收范畴。学校信息基础设施管理权属于网信办，校园信息基础设施的新建、扩建、改造、使用、变更等，由网信办负责组织实施。

第十八条 学校与各运营商之间的各项合作事宜由网信办统一归口管理。现有各运营商独立或与学校合作已建设的设施管理权限，按照相关合作协议执行并报网信办备案，学校有权对运营商进行监督，确保

运营商经营管理行为不违反国家相关法律法规和学校相关规章制度。

第六章 网络信息安全管理

第十九条 学校网络信息安全管理工作分为网络安全、系统安全和内容安全三个方面。网络安全是指校园网基础设施的安全。系统安全是指承载信息系统的服务器、软件运行环境、系统数据、大模型以及应用算法的安全。内容安全是指通过网络发布的各种信息中具体内容的安全。学校设置网络安全保障经费预算，专项用于学校网络安全建设、维护。

第二十条 学校网络信息安全工作按照“谁使用、谁负责，谁运营、谁负责，谁主管、谁负责”的原则进行。各部门党委负责人为本部门的网络信息安全责任人，网信管理员和普通使用者承担相应的网络信息安全责任。

第二十一条 网络与教育技术中心承担关键网络设施、核心信息系统、数据存储与处理设施等的安全防护工作。各部门需负责其主管的信息系统的安全管理和网站内容的安全性，并执行必要的数据备份和归档措施，以确保信息系统的稳定运行和信息安全。

第二十二条 各部门应定期对本部门信息系统进行安全检查，及时修补系统漏洞和处置异常访问等操

作，相应的管理人员应及时完善自身业务技能以满足岗位要求，并配合网络与教育技术中心安全检查工作。

第二十三条 校园网用户应遵守国家有关法律法规，不得利用校园网从事违反国家法律法规和学校规章制度的活动，应妥善保管自己的校内个人系统账号，不得因个人账号管理不善对信息安全造成危害。

第二十四条 学校对网络发布信息实行分级分类审核制度。学校党委宣传部负责审核发布学校信息，各部门负责审核发布本部门信息。未经审核的信息不得擅自在网上发布。

第二十五条 各部门应建立健全本部门的岗位信息安全责任制度，明确岗位及人员的信息安全责任。关键岗位人员应与学校签订信息安全与保密协议，明确信息安全与保密责任，各部门应与信息化软硬件供应商签订信息安全与保密协议。

第二十六条 各部门收集、使用个人信息，应当遵循合法、正当、必要的原则。应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第二十七条 涉密信息系统根据国家涉密信息保护的要求，按照学校保密工作部门有关涉密信息系统保护管理规定和技术标准进行保护。

第二十八条 校园网和信息系统用户实行“实名认证”制度。

第七章 信息系统安全测评

第二十九条 信息安全等级保护按国家《信息安全技术网络安全等级保护基本要求》进行，由网络与教育技术中心牵头做好学校信息系统安全等级保护工作，制定相关工作规范，提供技术支持和保障；各信息系统责任部门配合落实完成系统定级、系统备案、等级测评建设、整改等各项工作。

第三十条 信息系统常规安全测评按学校《信息系统安全测评管理办法》进行，由网络与教育技术中心组织对新建（购买或开发）的信息系统进行安全测评，不合格的不予验收、不准上线使用；对已建成并上线运行的信息系统定期进行安全测评，测评不合格的，限期整改，整改后仍未达标的不准上线使用。

第八章 移动互联网应用程序备案

第三十一条 学校使用的移动互联网应用程序（含手机 APP、微信小程序等）按照教育部《教育移动互联网应用程序备案管理办法》进行管理。

第三十二条 网信办负责学校教育移动应用审核和备案工作，未经审核和备案的移动应用不准使用。

第九章 附 则

第三十三条 本办法自发布之日起施行。

第三十四条 本办法由学校网信办负责解释。学校原有规定与本办法不一致的，按照本办法执行。