黄河水利职业技术学院网络信息安全管理办法

第一章 总　则

第一条　为加强学校网络信息安全管理，推进学校信息系统（含各部门门户网站）安全等级保护工作，提高网络信息安全防护能力和水平，保障学校各项事业健康有序发展，根据《中华人民共和国网络安全法》《教育部关于加强教育行业网络与信息安全工作的指导意见》（教技〔2014〕4号）、河南省教育厅、公安厅《关于深入开展教育行业信息系统安全等级保护工作的通知》（教科技〔2015〕710号）等文件要求，结合我校实际，特制定本办法。

第二条　本办法所称网络信息安全工作是指为使由学校产生的各项信息资产（信息及信息系统）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，建立健全网络信息安全责任体系，学校各部门、各单位依照本办法要求履行网络信息安全的义务和责任。

第二章 组织机构与职责

第四条　成立网络安全与信息化工作领导小组，该小组是学校网络信息安全归口管理机构，负责统筹学校网络安全与信息化建设工作。

第五条　学校主要负责人是学校网络信息安全的第一责任人，分管网络安全与信息化工作的校领导协助主要负责人履行学校网络信息安全责任。

第六条　信息化管理办公室（大数据管理中心）（以下简称信管办）是网络信息安全技术支撑部门，负责学校网络信息安全防护体系的建设、运行维护、技术指导和服务支持。

第七条　学校各部门是本部门网络安全和信息化工作的责任主体，各部门主要负责人是本部门网络安全和信息化工作第一责任人，负责人需按本办法落实网络信息安全工作。

第三章 校园网络管理

第八条　校园网络是指校园范围内连接各种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网络。

第九条　校园网络总体规划由网络安全与信息化工作领导小组办公室制定。涉及综合布线、网络机房、网络设备、网管系统、域名管理、安全防护、认证计费、网络接入与运维等方面，由信管办负责建设、运行、维护和管理。学校所有基建、修缮工程需将工程范围内校园网络建设纳入工程设计、实施和竣工验收范畴。

第十条　校园网络与互联网及其他公共信息网络实行逻辑隔离，由信管办统一出口、统一管理和统一防护。未经批准，学

校各部门、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。如需使用网络资源，各部门需按要求认真填写《黄河水利职业技术学院网络资源使用申请表》（详见附件 1）或《黄河水利职业技术学院上网登记表》（详见附件 2），并按申请表要求进行签字、审批，递交信管办统一办理。申请接入公共网络流程图详见附件 3。

第十一条　信管办采取访问控制、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。

第十二条　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。网络接入实名管理制度经分管信息化工作的校领导批准后，由信管办负责实施，涉密信息系统不得接入校园网络。（申请接入校园网络流程详见附件 4）

第十三条　校园网络使用部门负责提供本部门所需的网络设备间和电源保障，协助解决网络布线和设备安装所需空间，负责安防和消防安全管理。

第十四条　严禁任何单位、部门和个人利用校园网络及设施开展经营性活动。

第四章 数据中心管理

第十五条　数据中心主要包括支撑学校信息系统的物理环境（其中包含机房）、软硬件设备设施、云资源服务平台、学校

数据共享中心（其中包含基础数据库）、数据共享交换平台、统一身份认证平台及统一信息门户等信息化基础设施和平台。信管办负责数据中心的建设、运行、维护和管理。

第十六条　信管办负责数据中心物理环境、软硬件设备设施和云计算平台的建设和安全管理；根据信息系统安全等级的不同，对数据中心进行分区、分域管理，采取必要的技术措施对不同等级分区进行防护、对不同安全域之间实施访问控制。

第十七条　信管办负责学校数据共享中心、数据共享交换平台的建设和安全管理，负责基础数据库与各部门业务数据库之间的交换和共享。各部门负责建设、维护本部门业务应用系统所配套的业务数据库，并对本部门业务数据库及所申请的共享数据的安全负责。

第十八条　统一身份认证平台为学校信息系统提供统一的身份管理、安全的认证机制、审计及标准接口。学校各部门在建设面向师生服务的应用系统时，使用统一身份认证平台进行身份认证。信管办负责统一身份认证平台的安全，学校各部门负责本部门应用系统的权限管理及安全。

第十九条　原则上，学校各部门依托学校数据共享中心开展信息系统建设。涉及学校基础数据、师生员工个人信息或敏感信息的信息系统，不得在校外部署数据中心，严禁建立和使用境外数据中心。

第二十条　信管办对学校数据共享中心的使用实施准入管理，负责制定使用数据共享中心的技术规范和标准，由各部门提出申请信管办审核并上报分管信息化工作的校领导批准后，开放数据接口过滤敏感数据，通过系统数据接口方式使用校本数据中心数据。（申请使用数据共享中心数据流程图详见附件 5）

第二十一条　数据共享中心的使用部门遵循数据中心相关管理制度和技术标准，按需申请、有序使用，不得利用数据共享中心资源从事任何与申请项目无关或危害网络信息安全的活动。

第五章 信息系统建设、运行和维护管理

第二十二条　学校根据同步规划、同步建设、同步运行的原则，规划、设计、建设、运行、管理信息安全设施，建立健全网络信息安全防护体系，全面实施信息系统安全等级保护制度。

第二十三条　网络安全与信息化工作领导小组办公室负责制定学校信息系统项目规划和顶层设计。学校各部门根据本部门业务需求，提出信息系统建设申请，学校信息化建设经费优先支持纳入学校规划的核心信息系统建设。

第二十四条　网络安全与信息化工作领导小组办公室负责统筹学校信息系统安全等级保护工作，组织学校各部门开展信息系统定级、系统备案、等级测评、建设整改，具体负责信息系统台账管理、等级评审、系统备案、监督检查工作。按照“自主定级、自主保护”的原则，信息系统建设部门是信息系统安全等级

保护的责任主体，具体负责系统定级、建设整改、安全自查，协助系统备案、等级测评并接受有关部门监督检查。信管办是信息系统安全等级保护工作的技术支撑保障部门，负责网络信息安全防护体系建设和等级测评组织工作，参与监督检查工作，并协助学校各部门进行系统定级、建设和整改。

第二十五条 信息系统建设部门在立项阶段就必须确定安全保护等级，由网络安全与信息化工作领导小组办公室对建设方案进行单独的安全论证和评审。对于安全等级第二级以上（含第二级）的信息系统，由网络安全与信息化工作领导小组办公室统一办理系统备案。（信息系统安全保护等级评审流程图详见附件6）

第二十六条 学校鼓励信息化建设部门优先采购安全可靠、技术成熟和服务优质的成品软件用于信息系统建设。没有相应成品软件或成品软件不适应实际需求的，可按照学校采购与招标相关管理办法，经分管信息化工作的校领导批准后，按照相关流程委托资质和信誉良好的软件开发公司进行定制开发。

第二十七条 信息系统在建设阶段按照已确定安全保护等级，同步落实安全保护措施。信息系统投入试运行后，由建设部门初步验收，出具初步验收报告。对于安全等级第二级（含第二级）以上的信息系统，由网络安全与信息化工作领导小组办公室会同信管办组织等级测评。信息系统通过初步验收和信息安全保

护等级测评后，由网络安全与信息化工作领导小组办公室组织竣工验收。

第二十八条 信息系统开发环境、测试环境和运行环境严格隔离，信管办负责上述环境的建设、运行、维护和管理。

第二十九条 信息系统建设部门可自行或委托信管办维护信息系统。亦可根据实际需要，经分管信息化工作的校领导批准后，委托外单位维护信息系统。涉及重要业务或大量师生员工信息的核心信息系统以及安全等级第二级（含第二级）以上的信息系统，原则上由信管办维护。

第三十条 信息系统建设部门定期对终端计算机和承担网络与信息系统运行的关键设备（服务器、安全设备、网络设备）进行安全审计，通过记录、检查系统和用户活动信息，及时发现系统漏洞，处置异常访问和操作。

第三十一条 信息系统建设部门制定信息系统使用与维护的管理制度，规范信息系统使用者和维护者的操作行为。

第三十二条 对于安全等级第二级（含第二级）以上的信息系统，网络安全与信息化工作领导小组办公室将定期组织开展等级测评，查找、发现并及时整改安全问题、漏洞和隐患。根据国家和教育行业有关标准规范，四级系统每年进行两次测评，三级系统每年进行一次测评，二级系统每两年进行一次测评。

第六章 信息系统数据安全管理

第三十三条　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。

第三十四条　信息系统数据的所有者是数据安全管理的责任主体，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。

第三十五条　信息系统数据收集遵循“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，谁维护，谁负责”的原则，收集信息的部门是信息保护的责任主体，对其收集的信息严格保密，并建立健全保护制度。

第三十六条　信管办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。

第七章 互联网网站安全管理

第三十七条　学校各部门开办互联网网站，使用学校互联网域名和互联网 IP 地址，并遵守《黄河水利职业技术学院校园网管理规定》及相关规章制度。

第三十八条　信管办统一建设学校网站群系统并负责站群系统的安全管理。未纳入学校网站群系统的网站，其安全管理由网站主管部门负责。

第三十九条　学校各部门开办互联网网站优先选择学校网站群系统，站群系统不能满足需求时，经分管信息化工作的校领导批准后，可委托第三方建设。网站投入使用前，通过信管办组织的安全检查方可正式上线。

第四十条　互联网网站运行维护部门必须建立网站值守制度，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。

第四十一条　互联网网站的内容安全由网站主管部门负责。互联网网站主管部门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。

第四十二条　原则上学校各部门不得提供电子公告服务。确有需要，须经分管信息化和宣传工作的校领导批准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部门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内容审核、专项安全管理和技术措施。

第四十三条　对于使用频度不大、阶段性使用的网站，互联网网站开办部门可采取非工作时间或寒暑假、节假日关闭的方式运行。对于无人管理、无力维护、长期不更新的网站，互联网网站开办部门须关闭网站以降低安全风险。

第八章 电子邮件安全管理

第四十四条　信管办为学校各部门和师生员工提供电子邮箱，并负责学校电子邮件的安全管理。学校各部门和师生员工使用学校电子邮箱遵守学校电子邮箱相关规章制度。

第四十五条　信管办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。

第四十六条　师生员工须妥善保管本人使用的电子邮箱账号和密码，确保密码强度并定期更换，并对使用电子邮箱开展的所有活动负责。师生员工如发现他人未经许可使用其电子邮箱，立即通知信管办处理。对于盗用他人邮箱的行行为人将追究其责任，将根据学校有关规定给予以纪律处分。造成恶劣影响或触犯刑律的，将移交司法机关追究其刑事责任。

第九章 终端计算机安全管理

第四十七条　终端计算机是指由学校师生员工在校内使用并从事教学、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设备。

第四十八条　终端计算机使用人按照“谁使用，谁维护、谁负责”的原则，对其终端计算机负有保管和安全使用的责任。信管办对终端计算机的安全管理提供技术支持和指导。

第四十九条　信管办建立终端计算机统一管理平台，实现常用正版软件下载分发、系统补丁安装、病毒软件安装升级及漏洞管理等监管职能。

第五十条　终端计算机设备上安装、运行的软件须为正版软件。在终端计算机上使用盗版软件带来的安全和法律责任由终端计算机使用人承担。

第五十一条　终端计算机需设置系统登录账号和密码，禁止自动登录，登录密码具有一定强度并定期更改。

第五十二条　终端计算机使用人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。

第五十三条　终端计算机使用人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，必须立即断网后进行处置。

第五十四条　使用人需要对终端计算机妥善保管。若发生损坏丢失，按学校仪器设备相关管理规定处理。

第十章 存储介质安全管理

第五十五条　存储介质是指存储数据的载体，主要包括硬盘、存储阵列、磁带库等不可移动存储介质，以及移动硬盘、U盘等可移动存储介质。

第五十六条　原则上，存储阵列、磁带库等大容量介质托管在学校数据中心，并由信管办统一运行、维护和管理。相关部门须配合信管办采取必要技术措施防范数据泄漏风险，确保存储数据安全。

第五十七条　学校各部门建立移动介质管理制度，记录介质

领用、交回、维修、报废、损毁等情况。介质使用人按照“谁使用，谁维护、谁负责”的原则，对其移动介质负有保管和安全使用的责任。

第五十八条　非涉密移动存储介质不得用于存储涉密信息，不得在涉密计算机上使用。

第五十九条　移动存储介质在接入终端计算机和信息系统前，先进行查杀病毒、木马等恶意程序或代码。

第六十条　介质使用人注意移动存储介质的内容管理，对送出维修或销毁的介质事须先清除敏感信息。

第六十一条　信管办配备必要的电子信息消除和销毁设备。存储介质履行必要的审批程序后，经分管信息化工作的校领导批准后，可由信管办集中销毁。

第十一章 人员安全管理

第六十二条　学校各部门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。关键岗位的计算机使用和管理人员签订信息安全与保密协议，明确信息安全与保密要求和责任。

第六十三条　学校各部门加强人员离岗、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，收回发放的各种身份证件、钥匙、徽章以及学校提供的软硬件设备，并签署信息安全保密承诺书。

第六十四条　学校各部门定期对网络信息安全岗位的人员进行安全知识和技能的培训和考核，并对考核结果进行记录和保存。

第六十五条　学校各部门建立外部人员访问机房等重要区域的审批制度，外部人员必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。

第十二章 外包服务安全管理

第六十六条　网络信息外包服务是指信息系统的开发和运维的外包。

第六十七条　外包服务需求部门与网络信息外包服务提供商签订服务合同和网络及信息系统安全责任协议（详见附件7）、网站安全责任协议详见附件8）、数据保密协议（详见附件9）等相关协议，明确信息安全与保密责任，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，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。网络信息外包服务合同和信息安全与保密协议按学校合同管理办法的有关要求，经分管信息化工作的校领导批准后，报送网络安全与信息化工作领导小组办公室审核。

第六十八条　网络信息现场服务过程中，外包服务需求部门须安排专人陪同，并详细记录服务过程。

第六十九条　外包开发的系统、软件上线应用前，外包服务需求部门须组织安全检查，要求系统厂商及时提供系统、软件的升级、漏洞等信息和相应服务。

第七十条　信管办负责远程在线运维管理设备的统一购置、运维和管理。信息系统运维如需采用远程方式进行，必须通过远程在线运维管理设备统一进行管理。

第十三章 信息安全应急管理

第七十一条　网络安全与信息化工作领导小组办公室负责学校信息安全应急工作的统筹管理，信管办负责信息安全应急工作的技术支撑和保障。

第七十二条　网络安全与信息化工作领导小组办公室依据《信息技术安全事件报告与处置流程（试行）》（教科技〔2017〕438号），制定学校网络信息安全事件报告与处置流程，信管办负责制订学校网络信息安全应急预案；若学校网络信息安全应急预案不能满足需求，相关部门可制订本部门网络信息安全应急预案。网络信息安全应急预案制修订后经分管信息化工作的校领导批准后，及时报网络安全与信息化工作领导小组办公室备案。

第七十三条　网络安全与信息化工作领导小组办公室定期组织网络信息安全应急演练，评估并适时组织网络信息安全应急预案修订。学校各部门组织开展网络信息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。

第七十四条　信管办负责组建学校信息安全应急技术支援队伍，完善24小时应急值守制度，提高信息安全事件的预防、预警和应对能力，预防和减轻信息安全事件造成的损失和危害。

第七十五条　学校各部门、各单位按照学校网络信息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。

第七十六条　学校教职员工和学生均有义务及时向信管办报告信息安全事件，不得在未授权情况下对外公布、尝试或利用所发现的网络信息安全漏洞或安全问题。

第十四章 信息安全教育培训

第七十七条　网络安全与信息化工作领导小组办公室负责组织学校信息安全宣传和教育培训工作，建立健全相关制度。

第七十八条　网络安全与信息化工作领导小组办公室定期组织开展针对师生员工的信息安全教育，提高师生员工的安全和防范意识。

第七十九条　网络安全与信息化工作领导小组办公室定期开展针对信息安全管理人员和技术人员的专业技能培训，提高信息安全工作能力和水平。

第十五章 信息安全检查监督

第八十条　学校各部门定期对本部门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，并配合有关部门的信息安全检查、信息内容检查、保密检查与审批等工作。

第八十一条　网络安全与信息化工作领导小组办公室联合信管办对学校各部门的网络信息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，责成相关部门按时制订整改方案并落实到位。

第八十二条　网络安全与信息化工作领导小组办公室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有关信息安全分管部门。

第十六章 信息安全责任追究

第八十三条　学校建立网络信息安全责任追究和倒查机制。

第八十四条　有关部门在收到网络信息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，依据《网络安全法》追究相关人员的责任。

第八十五条　学校各部门按照网络信息安全事件报告与处置流程及时、如实地报告和妥善处置网络信息安全事件。如有瞒报、缓报、处置和整改不力等情况，学校将对相关部门责任人进行约谈或通报。

第八十六条　师生员工违反本办法规定的，由网络安全与信息化工作领导小组办公室督促改正，并通报批评；拒不改正或者导致危害网络信息安全等严重后果的，根据学校有关规定给予以

纪律处分。触犯刑律的，移交司法机关处理。

第十七章 网络舆情管控

第八十七条　学校各部门、各单位指定专门责任人，在党委宣传部的指导下，对以学校和部门名义开设的网站、微博、公众号、博客、论坛、BBS 等重点信息领域发布或涉及的热点问题开展网络舆情监控，进行 24 小时跟踪监控，发现问题必须第一时间上报。

第八十八条　学校各部门、各单位应加强网络舆情监控平台建设，收集处理舆情，定期汇总舆情报告，分析研判舆情，为校党委研究重大舆情决策提供参考。

第八十九条　学校各部门、各单位在网络舆情跟踪监控过程中，要及时对网络各类信息进行汇集、分类、整合、筛选，为学校决策层全面掌握舆情动态，做出正确舆论引导，提供分析依据，将监控分析结果及数据分析报告，推送至相关职能部门，以供制定对策。

第十八章 附　则

第九十条　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，由学校网络安全与信息化工作领导小组监督指导。

第九十一条　学校各部门可参照本办法制订本部门的实施细则。

第九十二条　本办法自发布之日起实施，由信管办负责解释。学校原有相关规定与本办法不一致的，按本办法执行。

附件：1.黄河水利职业技术学院网络资源使用申请表

2.黄河水利职业技术学院上网登记表

3.申请接入公共网络流程图

4.申请接入校园网络流程图

5.申请使用数据共享中心数据流程图

6.信息系统安全保护等级评审流程图

7.黄河水利职业技术学院网络及信息系统安全责任协议

8.黄河水利职业技术学院网站安全责任协议

9.黄河水利职业技术学院数据保密协议

附件 1

黄河水利职业技术学院网络资源使用申请表

申请表编号：

申请部门		申请人	
使用时限		联系电话	
申请虚拟机	处理器数量（核）____内存数量（GB）____存储空间容量（GB）____		
申请其他资源	□ 二级域名 □ 外网访问 □ 特殊端口		
申请理由及具体需求	理由及需求（文字性描述，含主要用途及进度安排）		
申请部门意见（盖章）	部门负责人签字： 日期：		
申请部门分管校领导意见	签字： 日期：		
信管办实施意见			
备注： 1.新申请虚拟机资源的需要所在部门领导签字； 2.新申请二级域名、外网访问权限、开放外部特殊端口，需申请部门分管校领导签字； 3.校外可访问系统原则上必须进行信息系统安全等级评定，系统安全事故责任人为资源申请人。			

附件 2

黄河水利职业技术学院上网登记表

<table>
<tr><td>公司名称</td><td colspan="5">（盖章）</td></tr>
<tr><td>校内地址</td><td colspan="3"></td><td>房间号</td><td></td></tr>
<tr><td>公司法人</td><td></td><td>身份证号</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>指导老师</td><td></td><td>联系电话</td><td colspan="3"></td></tr>
<tr><td colspan="6">主管部门意见：

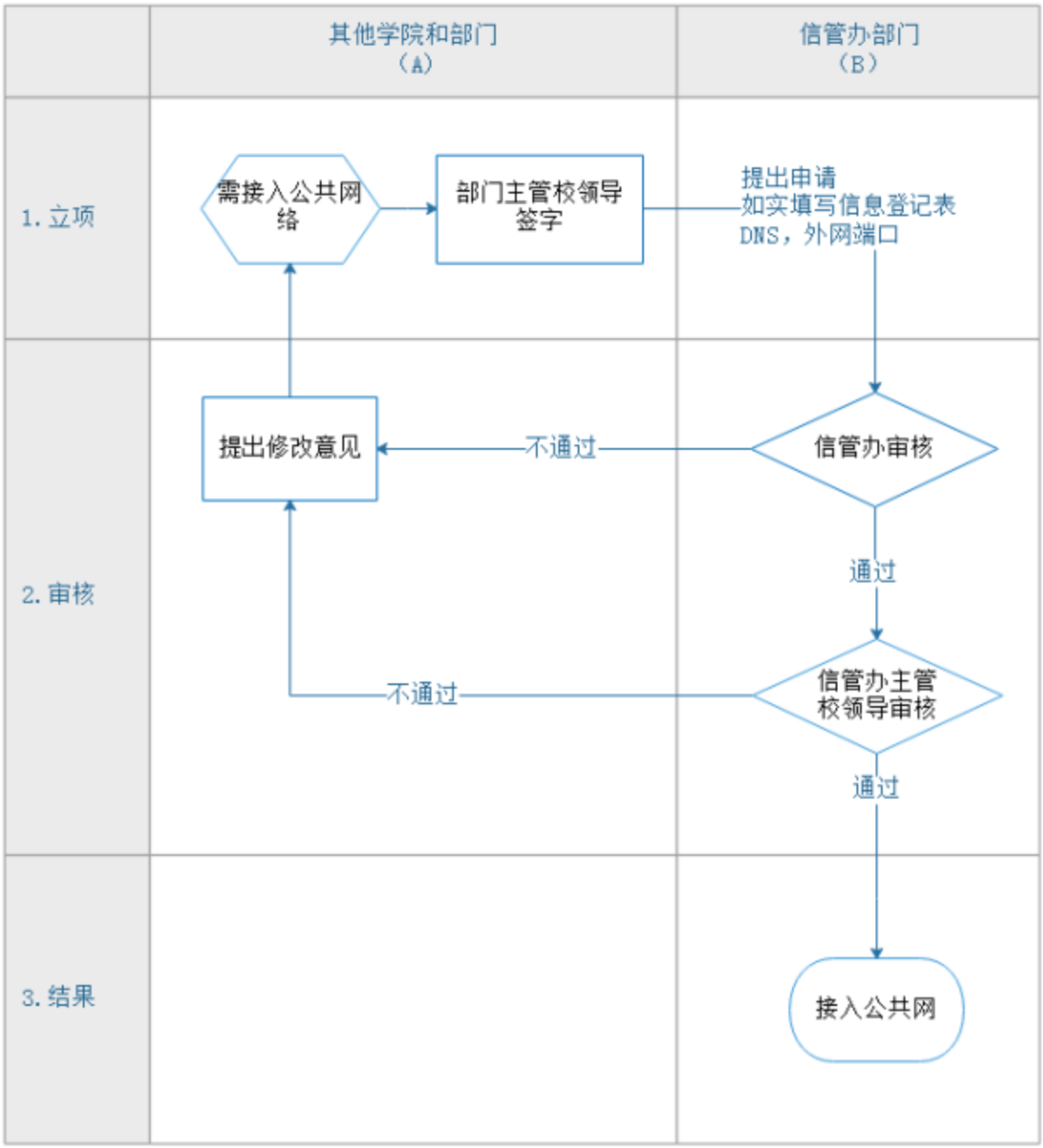
年　　月　　日</td></tr>
<tr><td colspan="6">所属分管部门意见

年　　月　　日</td></tr>
<tr><td>申请人</td><td>学号</td><td colspan="2">身份证号</td><td colspan="2">手机号</td></tr>
<tr><td></td><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td colspan="2"></td></tr>
</table>

注：本表适用于校企合作、对外经营类需要接入校园网的个人。

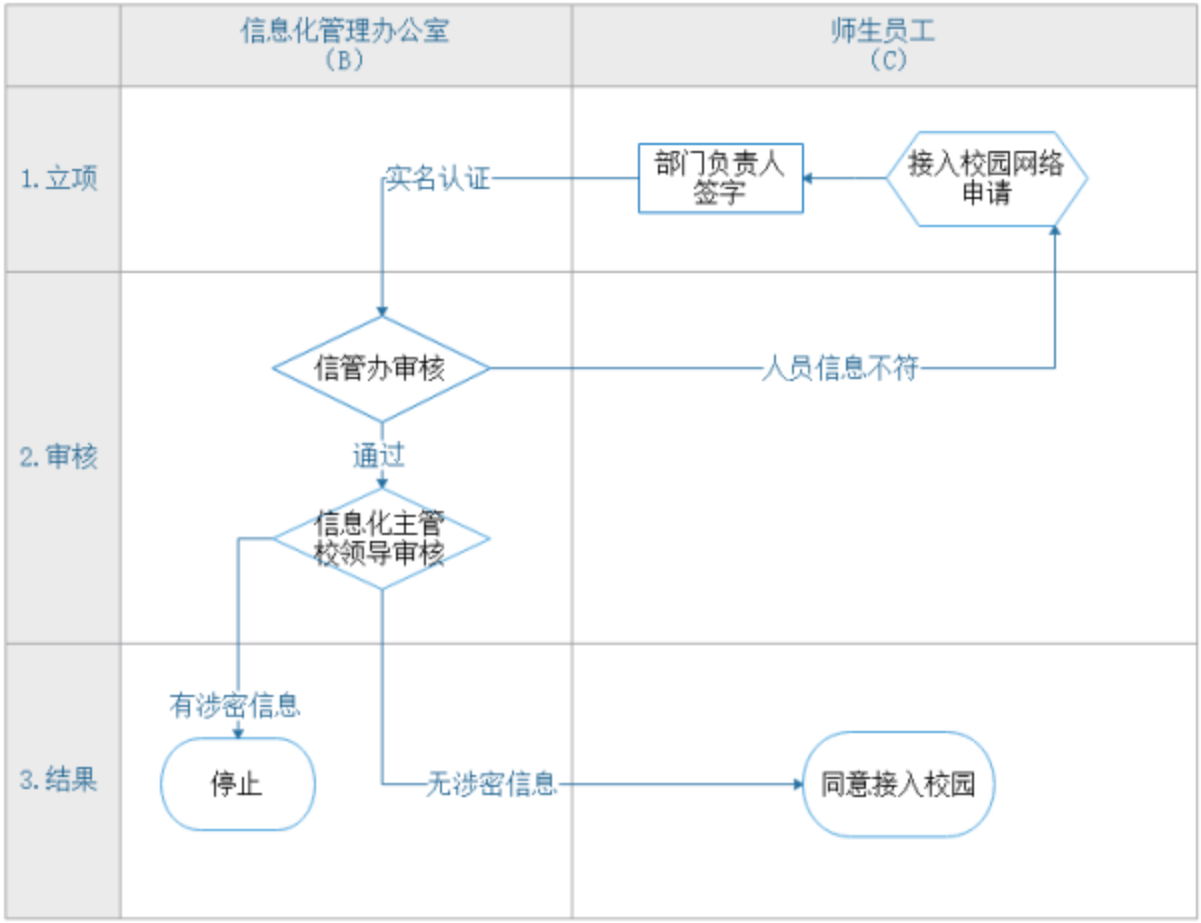
附件 3

申请接入公共网络流程图



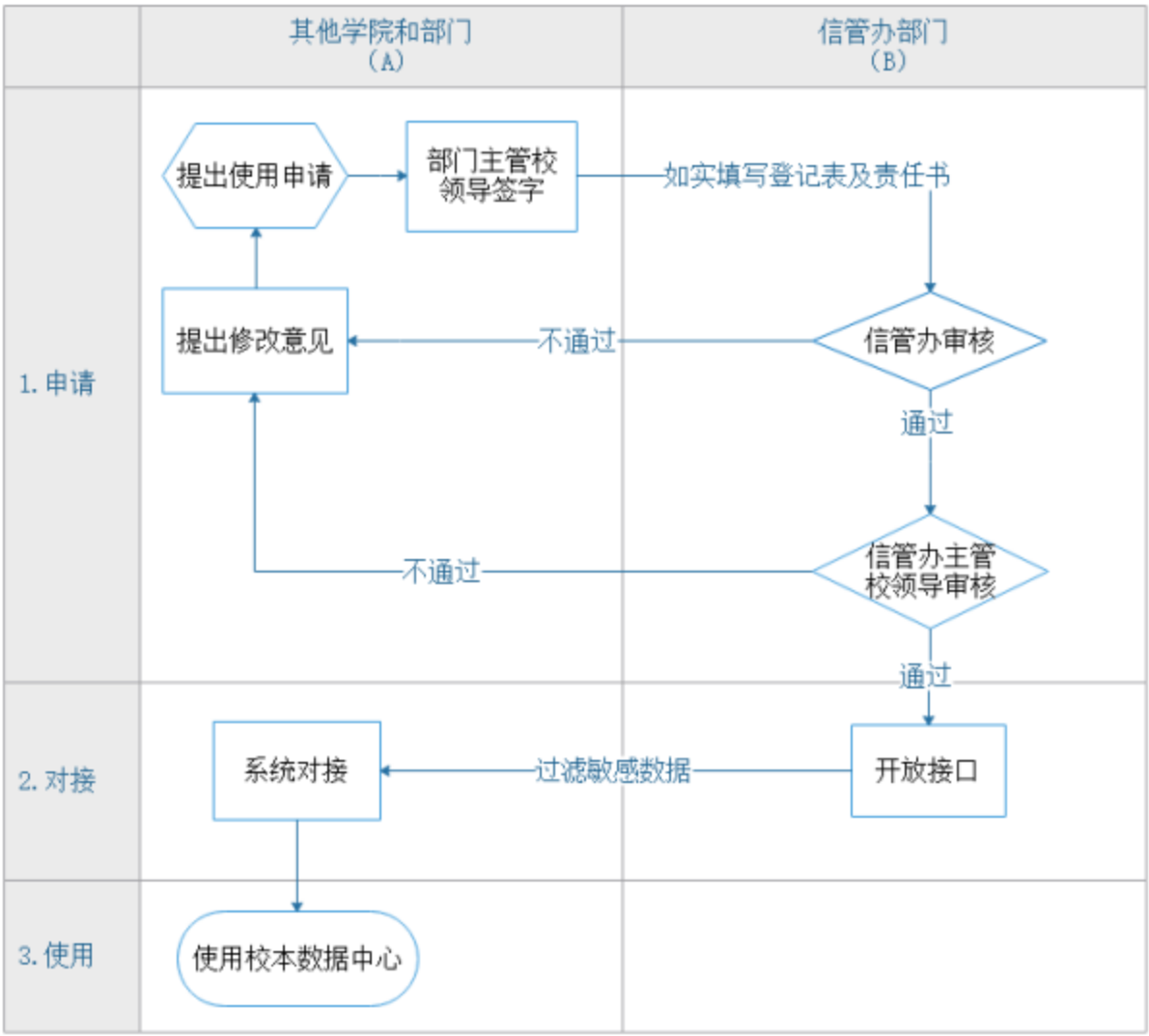
附件 4

申请接入校园网络流程图



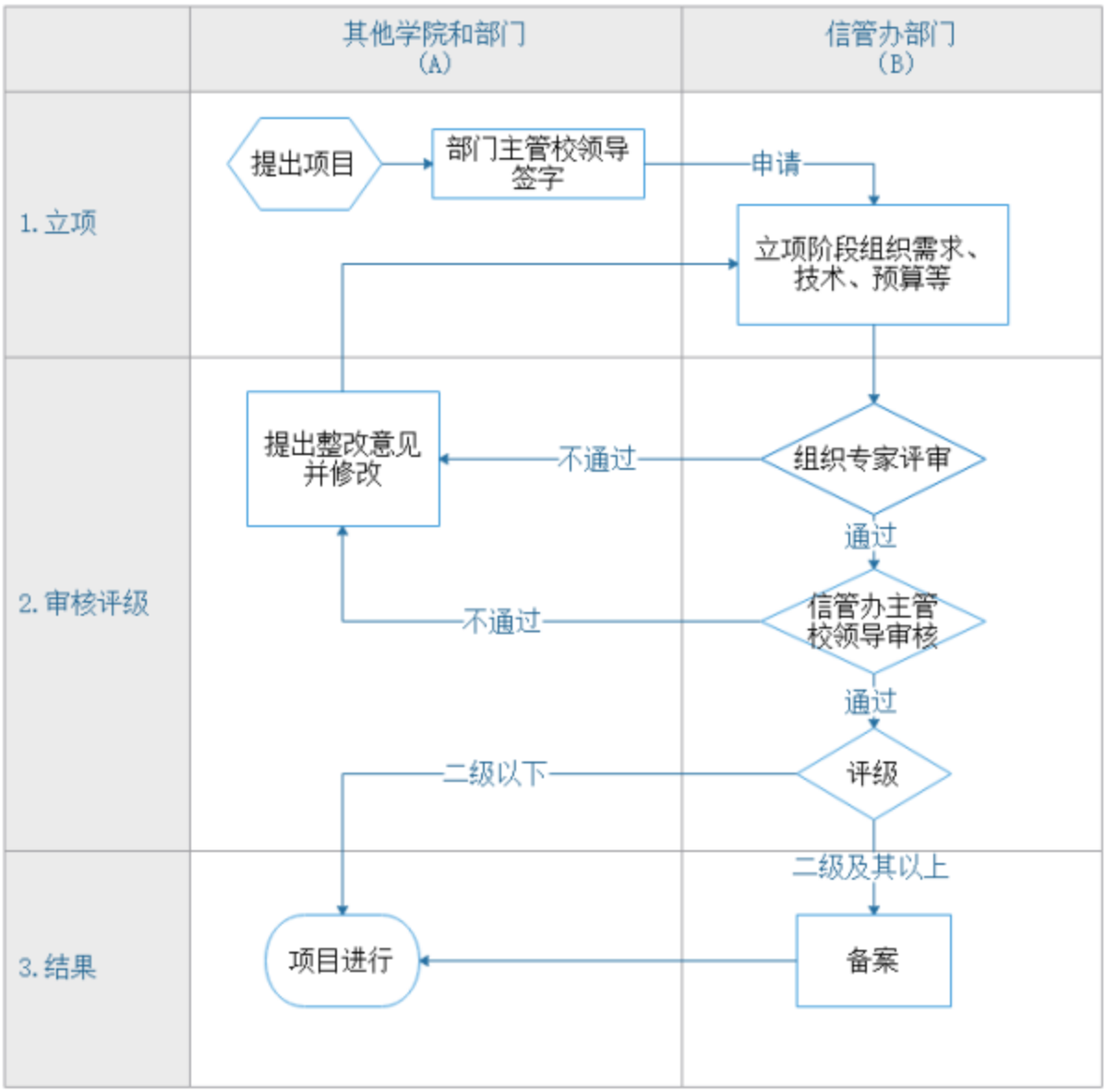
附件 5

申请使用数据共享中心数据流程图



附件 6

信息系统安全保护等级评审流程图



附件 7

黄河水利职业技术学院

YELLOW RIVER CONSERVANCY TECHNICAL INSTITUTE

网络及信息系统安全责任协议

信息化管理办公室　制

二〇一八年九月

项目名称：_____

甲　　方：_____

乙　　方：_____

乙方必须严格遵守黄河水利职业技术学院网络信息安全管理办法，合理、规范、安全地使用计算机、网络、数据和信息资源。乙方承诺在管理、开发、实施、维护维修项目的过程中，承担安全责任如下。

第一条　乙方对系统的硬件、操作系统、网络承担安全责任。包括但不限于：（1）保障硬件系统的安全运行状态；（2）对操作系统进行漏洞修补、安全更新；（3）对系统所需的各类网络协议与服务端口进行安全设置；（4）对数据进行备份和加密；（5）对病毒、木马程序及网络上出现的各类攻击手段进行事前防范、应急响应、事后处置等工作。最大限度地保障系统所用软硬件环境的安全。

第二条　乙方对所提供的信息系统及相关辅助软件（如数据库、Web容器、第三方组件等）承担安全责任。包括但不限于：（1）符合学校信息安全技术要求，对学校信息安全环境和其他系统不造成负面影响；（2）对系统进行严格的安全检测、并对安全事件和隐患进行处置；（3）负责落实甲方对系统提出的安全工作指令。

第三条　乙方对乙方工作人员的技术行为承担安全责任。包括但不限于：（1）在对系统进行建设、开发、安装、维护等各类必要的工作过程中，不得在服务器上安装各类与建设维护内容无关的软件（如QQ、支付宝、各类游戏等）；（2）不得在服务器上进行与建设维护内容无关的各类操作（如打游戏、查询股票等）；（3）必须按照甲方提供的登录方式进行工作，不得擅自开启任何后门程序进入；（4）在系统上线之后进行维护操作对系

统访问产生影响的，应知会甲方，为甲方提供合理的业务处置时间；（5）做好账号管理工作，防止账号泄露、侵入等事件的发生；（6）履行甲方的安全责任有关要求。

第四条　乙方对安全检测、应急响应和安全事件处置承担。包括但不限于：（1）对系统进行经常性的安全检测和监控（每季度不少于一次），并将结果以书面形式报告给甲方；（2）系统被检测出或发生安全问题时，乙方必须在1小时内做出响应，24小时内完成应急处置，有效防止损失的进一步扩大。

第五条 乙方无法在规定时间内响应和完成相关安全工作时，甲方可自行组织开展相关工作，由乙方承担相关费用。

第六条　本协议一式六份，甲方业务部门、乙方、学校信息化管理办公室各执二份，经签字确认后生效。乙方若违反本协议愿意承担黄河水利职业技术学院因此而产生的一切损失。

甲方（盖章）：　　乙方（盖章）：

部门负责人（签字）：　　法人或授权代表（签字）：

签字日期：　　签字日期：

附件 8

黄河水利职业技术学院

YELLOW RIVER CONSERVANCY TECHNICAL INSTITUTE

网站安全责任协议

信息化管理办公室　制

二〇一八年九月

为保障学校各类网站的系统安全和内容安全，维护校园稳定和正常教学秩序，根据《中华人民共和国计算机信息安全保护条例》、《中华人民共和国计算机信息网络管理暂行规定》和教育行政主管部门的相关规定，本单位遵守如下规定。

第一条 各单位党政负责人为各自网络信息发布的第一责任人。开通或关闭网站、微博、微信平台之前需到宣传部和信息化管理办公室履行登记备案手续；如实登记用途，不提供代理和涉嫌侵权的资源服务；一旦开通需做到及时更新、认真管理、注重质量。

第二条 按照“统一规范、先审后上、保证质量”的要求，严肃开展网络信息发布、转载和链接管理工作。在学校网站、微博、微信等平台上发布的网络信息由宣传部审核后才可发布；不以学校名义在其他传播平台上擅自发布网络信息；不发布与学校、部门职责无关的信息内容和外部链接。

第三条 按照如下要求开展网站安全建设和管理工作

（一）本部门所开设的网站统一使用学校站群系统开发、制作、发布，使用学校域名（yrcti.edu.cn、yrcit.cn）和IP地址，并使用学校服务器资源部署于学校数据中心内。特殊情况下须经宣传部和信息化管理办公室技术审核后方可调整方案。

（二）合理设置栏目，公开并及时更新单位概况、职能职责、规章制度、办事指南、工作通知、单位动态等内容；未经批准，不开设聊天室、论坛等开放式交互栏目，一旦批准开设，需安排人员认真审核留言内容，做到如实反映群众意见、过滤不良信息、积极引导网上舆论。

（三）采用安全的网络信息发布技术，避免传播带毒文件；引用、转发外部资讯时做到严格审核，并注明来源。

（四）妥善保管网站管理账户信息，使用高强度的密码，并定期更新；对网站管理人员和用户加强网络安全意识教育和业务培训。

（五）始终关注网站的安全状况，及时联系信息化管理办公室处置各种安全问题，配合宣传部和信息化管理办公室开展网络信息安全工作。

（六）执行读网制度。安排人员每天登录网站读网（包括微博、微信等网络传播平台），认真查看页面显示状况，查看各项功能的有效性，查看所发布的信息特别是重要信息是否存在错漏，查看是否存在暗链，发现问题立即纠正。关注校园网上发布的各类信息，加强沟通合作，做到学校网站与部门网站、部门网站与学校网站、部门网站与部门网站之间信息的准确性、一致性与恰当性。定期检查网站到其他网站的链接，防止因其他网站失效、被篡改等原因导致不良社会影响。

（七）严格落实网站维护管理制度。做到只在校园网内进行运维管理，若需要远程运维或第三方单位（如网站开发单位）协助运维，需要采用 VPN 加密、堡垒机登录等安全方式接入，不得直接远程桌面或直接开放管理端口到互联网。

第四条 校内各单位如违反以上条款，宣传部、信息化管理办公室将对违规网站或信息服务进行处理，并上报学校。

宣传部（签字）　　单位（盖章）

日期:

信息化管理办公室（签字）　　单位（盖章）

日期:

单位主要负责人（签字）　　单位(盖章)

日期:

附件 9

黄河水利职业技术学院

YELLOW RIVER CONSERVANCY TECHNICAL INSTITUTE

数据保密协议

信息化管理办公室　制

二〇一八年九月

第一条　责任人必须严格遵守黄河水利职业技术学院相关管理规定，合理、规范、安全地使用计算机、网络、数据和信息资源。责任人承诺在管理、开发、实施_____项目的过程中，视所接触到的资料、数据和项目信息为保密内容，承担保密责任。

第二条　来源于黄河水利职业技术学院的所有资料、数据和项目信息，包括但不限于教职工、学生个人身份信息、黄河水利职业技术学院组织架构信息、教学、科研、管理、服务等相关业务信息，以及项目建设内部文件、建设规划和建设方案资料。

第三条　责任人未经允许，不得访问、删除、修改、增加、复制、备份、摄录、摘抄、打印数据和资料，不擅自传播保密信息。

第四条　责任人保存数据、资料的存储介质（云盘、U 盘、终端存储等）不可交由其他人使用，或作其它用途，必须妥善保管，严防丢失。

第五条　责任人未经允许，不得进行影响系统运行的操作，如关闭主机（设备）、关闭关键服务、大量数据查询、修改数据库、修改系统配置等。

第六条　责任人对自己管理的账号，必须加强密码管理，要求管理员账号使用字符、数字、符号组合的复杂密码，长度不小于 8 位，口令 30 天定期更换。

第七条　存有保密信息的介质（硬盘、U 盘、磁盘、闪存、光盘等）如需送到单位外维修时，要将涉密资料备份后，对介质进行技术处理（如低级格式化、写零处理等），以防泄密。

第八条　责任人在承担项目工作完成以后，不得保留保密信息的副本，一切关于保密信息的资料销毁或返还信息提供部门，保证信息不会外流；责任人承诺若中途不再从事项目有关工作，仍对保密信息承担保密责

任。

第九条　若违反本承诺书内容，一经发现，学校可视行为严重程度进行行政处分或经济处罚。后果严重者，学校将通过法律途径向责任人索赔，或向司法机关报案处理。

第十条　责任人的保密义务自本协议盖章之日起开始生效，至保密信息公开或被公众知悉时止。责任人的保密义务并不因双方合作关系的解除而免除。

第十一条　本责任书一式三份，责任部门、责任人、信息化管理办公室各执一份，经签字确认后生效。责任人若违反本协议愿意承担黄河水利职业技术学院因此而产生的一切损失。

责任部门（盖章）：　　责任人（签字）：

责任部门负责人（签字）：　　责任人身份证号：

签字日期：　　签字日期：

黄河水利职业技术学院党政办公室　　2019 年 1 月 2 日印发