目　录

迁安职教中心网络安全领导小组及其职能

为了加强信息安全保障工作，全面提高信息安全防护能力，加强对我校校园网的运行和使用管理，防止有害信息侵害，促进我校校园网的健康发展，学校决定健全和完善学校统一领导、分级负责、各司其责的信息安全管理体系，完善各项规章制度，建立校园网络信息管理和运行安全防范监控机制，切实做好我校网络信息安全保障工作。学校特成立校园网络安全管理小组。

一．组织机构

组 长：凌志杰

副组长：郑立冬

组 员：李树贵、刘大彩、刘荣良、宁文军、乔玉丰、叶发友、崔健飞、刘文合、张书峰

网管中心：张书峰

二．工作职责

组 长：负责校园网络的政策性指导，执行上级文件精神和要求，及时在组内传达贯彻，分解任务指标。

副组长：负责相关制度的审核工作，指导小组成员及信息员开展工作,；负责对师生进行网络安全教育和法制教育。

组 员：负责相应版块的新闻上传、审核及管理；组织实施相关教育培训等。

网络中心：全面负责学校网络安全管理及信息化相关技术实施。处理突发网络事件及网络故障。

三．工作要求

1.强化领导

校园网络建设关系学校形象，网络安全关系国家政治稳定和社会稳定，要充分认识到网络安全保卫工作的重要性和长期性。网络安全领导小组负责校园网络和信息化建设及信息的审核、发布，组长负总责。

2.各负其责

按照“谁分管，谁负责；谁使用，谁负责”的原则，各领导小组成员要认真履行网络安全管理职责。

3.严格审核

完善网站的信息发布程序，不符合相关规定的信息不得在网上发布。定期巡查校园网信息，发现不良信息应及时作好记录并按程序上报处理。

迁安市职教中心

2021 年 10 月修定

网管中心管理制度

1、网管中心是校园网运行、控制、管理的中心，是保障校园网正常运行、集中放置校园网核心设备之重地，非网管人员不得随意进入。

2、要保持良好的网络设备运行环境，不准在网管中心吸烟、饮食、喧哗。严禁在网管室内存放易燃、易爆、有毒物品、腐蚀性物品、强磁场物品、放射性物品。

3、要定期做好软件备份和计算机病毒检查处理，任何外来软件必须进行计算机病毒检查，确认无病毒后方可使用。

4、网管中心要装置调温、调湿、稳压、防火、防盗等设备，保证网络设备的安全运行。

5、网管中心要建立完整、规范的校园网设备运行情况档案及网络设备帐目，认真做好各项资料（软件）的记录、分类和妥善保存工作。

6、网管中心内设备均属专用设备，一律不许外借和挪做它用。对违反规定者要追究责任。

7、要建立日常和节假日值班制度，做到防火、防盗等防范措施，严防出现恶性事故。

8、网管中心工作人员调入调出时，要及时做好有关网络设备运行情况档案资料、室内设备清点和帐目交接手续。

迁安市职教中心

2021 年 10 月修定

迁安职教中心日常网络管理制度

校园网是学校重要的基础设施之一，是教学和管理工作的重要支撑。为规范学校网络管理，充分发挥校园网作用，降低网络安全风险，根据 2017 年 6 月国家颁布的《网络安全法》，结合学校实际，特制订本条例，望广大师生共同遵守。

第一条 任何人使用学校网络过程中必须遵守国家法规和学校有关规定。禁止用户浏览不良网站，禁止发布传播妨碍社会治安及其它非法信息。因在网上发布或传播违反国家政策内容被上级追查的，涉事个人负全部责任。

第二条 禁止通过聊天、邮件或其它方式传播网络病毒及其它非法程序，严禁利用学校网络安装测试黑客软件等威胁学校网络安全的程序，一经发现所用电脑将禁止联网。

第三条 为确保学校网络传输的信息符合国家有关政策规定，网管中心在必要时可采取技术手段，对流量和网络资源进行配额管理，对用户的查询信息及所浏览的网站内容进行过滤。

第四条 在学校网站或公众号发布信息由信息员采编、上传，学校审核员审核。信息审核员要严格把关。保证发布的信息符合相关规定。

第五条 学校网络服务主要用于教育教学工作和管理工作，用户应自觉控制查阅娱乐性内容播放下载大量占用网络流量的影视等多媒体信息。

第六条 学校相关文件档案资料，未经学校相关部门同意，不可随意上网发布。

第七条 学校不定期对接入计算机进行检查。对安装不健康内容、危害网络安全和一些软件和游戏及时清除。

第八条 网络管理员为各处室统一分配 IP 地址，其他人不得随意更改，如有需要报维护人员进行修改。

第九条 学校计算机网络设备为公共财产，任何人不得私自拆卸，不得将任何学校信息设备带出学校。确有需要的，须经学校批准。

第十条 放假期间，除行政楼、餐厅、培训楼以外，其它各楼网络均断开，若确有加班或培训等特殊情况，须提前向学校申请并告知网管中心

第十一条 网管中心制定网络安全应急预案，不定期进行网络安全检查，及时果断地处置网上突发事件。

迁安市职教中心

2021 年 10 月修定

迁安职教中心数据安全管理制度

学校校园网是为教学及学校管理而建立的计算机信息网络，目的在于利用先进实用的计算机技术和网络通信技术，实现校园内计算机互联、资源共享，并为师生提供丰富的网上资源。为了保护校园网络系统的安全、促进学校计算机网络的应用和发展，保证校园网络的正常运行和网络用户的使用权益，更好的为教育教学服务，特制定如下管理条例。

第一章总则

1、本管理制度所称的校园网络系统，是指由校园网络设备、配套的网络线缆设施、网络服务器、工作站所构成的，为校园网络应用而服务的硬件、软件的集成系统。

2、校园网络的安全管理， 应当保障计算机网络设备和配套设施的安全， 保障信息的安全和运行环境的安全，保障网络系统的正常运行，保障信息系统的安全运行。

3、网络中心负责相应的网络安全和信息安全工作， 定期对相应的网络用户进行有关信息安全和网络安全教育并对上网信息进行审查和监控。

4、任何单位和个人，未经校园网网络中心同意，不得擅自安装、拆卸或改变网络设备。

5、所有上网用户必须遵守国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。任何单位和个人不得利用联网计算机从事危害校园网及本地局域网服务器、工作站的活动。

6、进入校园网的全体学生、教职员工必须接受并配合国家有关部门及学校依法进行的监督检查， 必须接受学校网络中心进行的网络系统及信息系统的安全检查。

7、使用校园网的全体师生有义务向网络中心和有关部门报告违法行为和有害信息。

第二章网络安全管理

1、校园网由学校网络中心统一管理及维护。连入校园网的各部门、处室、教室和个人使用者必须严格使用由网络中心分配的 IP 地址。网络管理员对入网计算机和使用者进行登记， 由网络中心负责对其进行监督和检查。任何人不得更改 IP 及网络设置，不得盗用 IP 地址及用户帐号。

2、与校园网相连的计算机用户建设应当符合国家的有关标准和规定，校园内从事施工、建设，不得危害计算机网络系统的安全。

3、网络管理员负责全校网络及信息的安全工作， 建立网络事故报告并定期汇报，及时解决突发事件和问题。校园网各服务器发生案件、以及遭到黑客攻击后，网络中心必须及时备案并向公安机关报告。

4、对所有联网计算机要及时、准确登记备案。网络教室不准对社会开放。

5、校园网中对外发布信息的 Web 服务器中的内容必须经领导审核， 由负责人签署意见后再由信息员发布。新闻公布、公文发布权限要经过校领导的批准。

6、校园网各类服务器中开设的帐户和口令为个人用户所拥有， 网络中心对用户口令保密， 不得向任何单位和个人提供这些信息。校园网及子网的系统软件、应用软件及信息数据要实施保密措施。

7、加强对师生用户上网安全教育指导和监督：

（1）校园网内必须安装网络版监控和防范不良信息的过滤软件系统，监控日志至少保存半年。

（2）加强对学生开放互联网以及全校教职工上网的监管。

（3）专用的财务工作电脑和重要管理数据的电脑最好不要接入网络工作。

8、网络中心统一在每台计算机上安装防病毒软件，各部门、教研组、办公室要切实做好防病毒措施，随时注意杀毒软件是否开启，及时在线升级杀毒软件，及时向网络中心报告陌生、可疑邮件和计算机非正常运行等情况。

9、禁止私自安装、卸载程序， 在校园网上， 禁止使用盗版软件， 不允许玩电子游戏， 不允许无关人员使用，也不允许进行与工作无关的操作，禁止任意修改和删除计算机的系统文件和系统设置。

10、严禁在校园网内使用来历不明、引发病毒传染的软件或文件；对于外来光盘、优盘、软盘上的文件应使用合格的杀毒软件进行检查、消毒。

11、任何单位和个人不得在校园网及其连网计算机上录阅传送有政治问题和淫秽色情内容的信息。

12、未经校园网络中心及各子网网管的同意，不得将有关服务器、工作站上的系统软件、应用软件转录、传递到校外。

13、需在校内交流和存档的数据，按规定地址存放，不得存放在硬盘的 C 盘区，私人文件不得保存在工作电脑中，由此造成的文件丢失损坏等后果自负。

14、保护校园网的设备和线路，不准擅自改动计算机的连接线，不准打开计算机主机的机箱，不准擅自移动计算机、线路设备及附属设备，不准擅自把计算机设备外借。

15、各处室部门和教研组必须加强对计算机的管理，指定专人负责管理。管理员应经常测试计算机设备的性能，发现故障及时通知网络中心处理。

16、各处室部门和教研组应认真做好本单位计算机的养护和清洁卫生工作。

第三章网络用户安全守则

1、使用校园网的全体师生必须对所提供的信息负责。严禁制造和输入计算机病毒，以及其他有害数据，危害计算机信息系统的安全，不得利用计算机联网从事危害家安全、泄露秘密等犯罪活动，不得制作、查阅、复制和传播有碍社会治安和有伤风化的信息。

2、除校园网负责人员外， 其他单位或个人不得以任何方式试图登陆进入校园网服务器或计算机等设备进行修改、设置、删除等操作；任何单位和个人不得以任何借口盗窃、破坏网络设施，这些行为被视为对校园网安全运行的破坏行为。

3、用户要严格遵守校园网络管理规定和网络用户行为规范，不随意把户头借给他人使用， 增强自我保护意识，经常更换口令，保护好户头和 IP 地址。严禁用各种手段破解他人口令、盗用户头和 IP 地址。

4、网络用户不得利用各种网络设备或软件技术从事用户帐户及口令的侦听、盗用活动， 该活动被认为是对网络用户权益的侵犯。

5、使用校园网的全体师生有义务向网络中心报告违法行为和有害的、不健康的信息。

第四章处罚办法

违反本制度规定，有下列行为之一者，学校可提出警告、停止其上网，情节严重者给予行政处分，或提交司法部门处理。

1、查阅、复制或传播下列信息者：

（1）煽动分裂国家、破坏国家统一和民族团结、推翻社会主义制度；

（2）煽动抗拒、破坏宪法和国家法律、行政法规的实施；

（3）捏造或者歪曲事实，故意散布谣言，扰乱社会秩序；

（4）公然侮辱他人或者捏造事实诽谤他人；

（5）宣扬封建迷信、淫秽、色情、暴力、凶杀、恐怖等。

2、破坏、盗用计算机网络中的信息资源和进行危害计算机网络安全的活动。

3、盗用他人帐号或私自转借、转让用户帐号造成危害者；

4、故意制作、传播计算机病毒等破坏性程序者。

5、上网信息审查不严，造成严重后果者。

6、使用任何工具破坏网络正常运行或窃取他人信息者。

7、有盗用 IP 地址、盗用帐号和口令、破解用户口令等危及网络安全运行与管理的恶劣行径者。

迁安市职教中心

2021 年 10 月修定

迁安职教中心网络运行管理制度

一、总则

1.网络运行管理是指对网络结构、网络设备、网络信息、网络安全及网络用户的管理

2.学校网络中心在校园网领导小组领导下,负责校园网络的规划设计、建设、管理与运行的协调,是学校的网络管理部门

3.学校的各个部门和个人在使用网络过程中必遵守国家有关法律、法规和本院网络中心的有关规定

4 用户在使用网络过程中违反网络中心有关规定的,网络中心将视情节给予劝告、警告及冻结账号等相应处罚。悄节严重的报请院校园网领导小组进行处理

5.用户在使用网絡中违反国家法律和行政法规的情节轻重给予警告

通报批评或冻结账户等处罚,情节特别严重构成犯罪的,报有关部门依法追光刑事责任

二、网络用户管理

1.使用网络的部门及个人都是网络的用户

2 学校鼓励各部门及本校教职工、学生用户使用网络资源

3.学校网络中心为要接入网络的用户统一分配 IP 地址。各部门及教职工、学生用户使用网络填写入网中请,由网络中心备案后分配 IP 地址。

三、网络设备管理

1.网络设备管理指对接入网络的通信主干设备、公共服务器、计算机和打印机等设备

2.网络的主干通信设备、网络线路、公共服务器及其它公共设备由网络中心管理。部门中的网络服务器和网络打印机等设备由网管人员负责管理。

4 接入网络的计算机,由该设备的责任人员负责管理,并在网络中心备案

5、.共享设备的使用设备的使用范围进行限定,禁止无限制地开放共享设备

6.用户设备接入网絡由网络中心统一规划和实施,用户将设备接入网络时,经所在部门领导批准后,并向网络中心提出中申请

7.网络中心对入网设备的名称、入网软硬件配置、入网接入端口和安装的软件实行统一规范和管理,不定期检查其使用情况

四、网络信息管理

1 网络信息是指通过网络发布、传递及存储在网络设备中的信息学校网络使用的 Internet 域名由网絡管理部门统一规划和管理

3.网络中心按照有关网站和信息上网的管理办法负责学校网站的运行管理，学校

的各类信息系统实行分级安全管理,不同的用户根据不同的授权获得授权范围的信息

5.学校的 Internet 电子邮件服务仅限于与工作有关的通信业务,不得通过电子邮件传输涉密信息

6.学校的 Internet 信息服务主要用于与学校教学、科研和管理工作有关的通信业务，用户应控制查阅娱乐性的内容和调阅下载大量占用网络通信流量的影视和音乐等多媒体信息

7 任何人不得利用学校网络提供的各种信息服务从事危害国家安全、泄露国家秘密等犯罪活动,不得制作、查阅、复制和传播危害国家安全、妨碍社会治安和淫秽色情的

8 为了确保学校网络传输的信息符合有关规定,确保学校的公共财产不被滥用,网络中心在必要时可采取技术于段,对用户使用的信息流量和网络资源进行配额管理,对用户的电子邮件和 Internet 查询的信息进行过滤

五、信息上网与网站管理

1.网站管理机构

1)学校网站在校园网领导小组领导下由网絡中心负责管理

(2)网络中心负责制定网络管理办法,规划网站公共栏目的设置,负责审核批准公共栏目上网内容,重要内容校园网领导小组同意批准

(3)网络中心兼顾网络技术与网络编辑两种功能。网站各承包栏目的上网信息由栏目的承包部门负责组织和审核。网络中心负责校园网站的网页面设计、网页制作、网页更新、上网信息技术编辑、信息上网发布和网站技术管理

2.信息发布管理

(1)学校网站栏日的信息上网发布实行分级管理,每个栏目均设立负责部门和信息员。各部门在网络中心有关人员的协同指导下,按照规定的格式编排本部门负责的栏目并组织上网信息

(2)各部门信息员负责提供本部门分管栏日的上网稿件

(3)上网发布的信息不得违反国家和本院有关保密的规定

(4)上网稿件提交给学校网站,同时提交与电子文本稿件内容相同的纸质稿件,并注明供稿人和审核人。重要信息送校园网领导小组及分管领导审阅和签署意见后,再交网络中心技术人员上网发布上网稿件由学校分管领导终审签发,部门级栏目的上网稿件由部门主管领导终审签发。

(5)为确保网站内容的时效性,上网信息要及时更新

(6)信息上网与网站运行的日常工作由网络中心技术人员负责

迁安市职教中心

2021 年 10 月修定

迁安市职业技术教育中心

网络信息安全责任追究制度

第一章 总 则

第一条 为明确网络与信息安全事故责任主体(以下简称“责任主体”)，追究网络与信息安全事故的责任，结合学院实际情况，制定本制度。责任主体的范围包括二级学院、系、部门、科室或个人等。

第二条 负责追究责任主体事故责任的单位或个人统称为责任追究主体，包括各级网络安全与信息化领导小组、各级网络安全与信息化领导小组办公室、学院各级部门或各级领导等。

第三条 本制度适用于所有部门，各部门应根据本制度制定具体实施细则。

第四条 网络与信息安全事故责任认定实行“谁主管谁负责、谁使用谁负责”的原则。

第五条 发生网络与信息安全事故后，应根据安全事件造成的影响及相关责任主体的态度，作出如下处理：

(一) 批评教育。包括责令责任主体检查、诫勉谈话等；

(二) 书面检查。责令责任主体向上级主管领导作出书面检查；

(三) 通报批评。在部门范围内对责任主体发文通报，责令整改；

(四) 一般处理。降低或扣除责任主体的月薪补贴，将事故写入月度或年度考核中；

(五) 严肃处理。追究网络与信息安全事故发生负有领导责任的负责人的管理责任，发生严重网络与信息安全事故的，对相关责任人处以罚款、责令其赔偿事故损失、全院通报批评、降职处理、直至开除。

(六) 报警处理。严重损坏社会或国家利益的，上报当地公安部门处理。

第六条 责任追究应当坚持公平公正、有责必究、过罚相当、教育与惩戒相结合的原则。

第二章 责任追究范围和适用

第七条 责任主体有下列行为之一者，应对其进行批评教育或责令作出书面检查：

(一) 发生一般或较大安全事件，未按要求上报的；

(二) 未按规定落实相关网络与信息安全管理制度及技术规范，且未导致安全事件发生的；

(三) 发生重大安全事件后，对调查工作配合不力的。

第八条 责任主体有下列行为之一者，应当责令其作出书面检查或通报批评：

(一) 发生重大安全事件，未按要求上报的；

(二) 未按规定落实相关网络与信息安全管理制度技术规范，导致一般或较大安全

事件发生的；

（三）发生重大或特别重大安全事件，且发生安全事件后处理及时，未对学院财产或声誉造成影响的；

（四）经过批评教育或责令作出书面检查后，仍不按规定落实相关网络与信息安全管理制度及技术规范的；

（五）发生特别重大安全事件后，对调查工作配合不力的。

第九条 责任主体有下列行为之一者，应当予以通报批评或一般处理：

（一）发生特别重大安全事件，未按要求上报的；

（二）发生重大或特别重大安全事件，且发生安全事件后处理不及时，给学院财产或声誉带来一定影响的；

（三）发生特别重大安全事件后，对调查工作不配合的。

第十条 责任主体有下列行为之一者，应当予严肃处理，情况十分严重者应报警处理：

（一）发生重大或特别重大安全事件造成后果严重并刻意隐瞒或谎报，造成恶劣影响的；

（二）未按规定落实相关网络与信息安全管理制度及技术规范导致发生重大或特别重大安全事件，且发生安全事件后处理不及时，给学院财产或声誉带来恶劣影响的；

（三）发生安全事件后销毁证据、弄虚作假的。

第十一条 对应追究责任主体责任而敷衍结案、弄虚作假的，应当对责任追究主体通报批评。

第十二条 有下列情形之一者，不追究责任主体的责任：

（一）因不可抗力导致发生的网络与信息安全事故；

（二）有充分证据证明完全落实了相关安全要求，由未知原因导致网络与信息安全事故发生的。

第十三条 责任主体主动承认过错并及时修补管理或技术漏洞，减少损失、挽回影响，态度非常好的，应当予以从轻或减轻责任追究。

第三章 责任追究程序和实施

第十四条 责任追究过程采用层层负责制，下级责任追究主体对上级责任追究主体负责。

第十五条 责任追究程序包括调查、对调查报告审核、作出责任追究决定等。

第十六条 对网络与信息安全事故的调查和对事故责任的初步定性由学院各级网络安全与信息化领导小组办公室及相应的主管部门共同负责，并对调查报告进行审核。

第十七条 调查报告的审核重点：

（一）事故的事实是否清楚；

（二）证据是否确实、充分；

（三）性质认定是否准确；

（四）责任划分是否明确。

第十八条 责任追究决定：

（一）对责任主体作出批评教育、责令作出书面检查、通报批评时，由责任主体所在部门网络安全与信息化领导小组办公室或上级网络安全与信息化领导小组办公室直接决定。

（二）对责任主体作出一般处理、严肃处理时，由责任主体所在部门或上级部门网络安全与信息化领导小组安全办公室、人事、主管部门共同作出决定，并报网络安全与信息化领导小组审批通过后执行。

第十九条 对责任主体的追究决定由人事、财务、相对应的主管部门、网络安全与信息化领导小组办公室等职能部门分别负责实施。

第四章 附 则

第二十条 本制度解释权归属太原师范学院网络安全与信息化领导小组办公室。

第二十一条 本制度自发布之日起执行。

迁安市职教中心

2021 年 10 月修定

迁安职教中心网络信息监管制度

一、严格执行国家及地方制定的信息安全条例。

二、上网用户必须严格遵循网络安全保密制度。

三、提供的上网信息，必须经过网络中心审核后方可上网，并及时予以登记。

四、用户必须配合有关部门依法进行信息安全检查。

五、建立健全的网络安全管理制度，采取安全技术措施、落实安全管理责任、加强对各类网络平台信息发布的审核、网络运行日志的管理、并将系统运行日志完整保存 6 个月以上，以备上级的监督检查。

六、加强网络信息的检测，定期检查安全情况。检测计算机是否感染病毒并及时清除，同时应配合网络管理员对各开通服务器的系统日志进行不定期检查，及时发现隐患、及时汇报与处理。

七、对网络上的有害信息及时控制并删除。严防非法用户侵入我方网络从事非法

活动，一经发现应及时进行相应的技术处理，如及时清除有害的传播途径、关闭相应的服务器等，同时要保护好相关的日志等数据，并及时向有关部门报告。

八、出现有关网络安全隐患要及时上报网络中心，及时处理并作日志。

九、加强对用户数据的管理，发现异常用户，及时处理并上报网络中心备案。

十、定期组织网络管理人员进行安全管理学习和培训。

迁安市职教中心

2021 年 10 月修定

迁安职教中心网络病毒和安全漏洞检测制度

为保证我校校园网的正常运行，防止各类病毒、黑客软件对我校联网主机构成威胁，最大限度地减少此类损失，特制定本制度：

一、各接入单位计算机内安装防病毒软件、防黑客软件及垃圾邮件消除软件，并对软件定期升级。

二、各接入单位计算机内严禁安装病毒软件、黑客软件，严禁攻击其它联网主机，严禁散布黑客软件和病毒。

三、网络中心应定期发布病毒信息，检测网内病毒和安全漏洞，并采取必要的措施加以防治。

四、校园网内主要服务器应当安装防火墙系统，加强网络安全管理。

五、网络中心定期对网络安全和病毒检测进行检查，发现问题及时处理。

迁安市职教中心

2021 年 10 月修定

迁安市职业技术教育中心学生上网管理规定

为了规范我校学生网络行为，引导学生科学、合理地使用我校网络资源，进一步加强我校网络管理，维护网络安全，提高网络使用率，维护校园公共秩序，让校园网更好地为我校的教学、科研、生活服务。根据《中华人民共和国网络安全法》、《互联网信息服务管理办法》等文件精神，结合我校实际，特制定本规定。

本规定实施对象为我校所有在册学生。规定所称“上网行为”是指我校学生利用我校校园网资源所进行的一切网上活动。

学生上网应当遵守国家和学校关于网络使用的有关法律和规定，严格遵守网络公

约和道德规范。不得发布、传播、复制以下信息:

（一）煽动颠覆国家政权，推翻社会主义制度的言论；

（二）煽动分裂国家、破坏祖国统一的言论；

（三）损害国家利益，危害国家安全的言论；

（四）煽动民族仇恨、民族歧视、破坏民族团结的言论；

（五）使用网络从事危害公共安全、损害公众利益、侵害他人正当权益、窃取和泄露他人秘密的活动；

（六）在校园网上发布未经证实、无法确定来源的消息。捏造或歪曲事实，散布谣言，扰乱社会秩序和校园秩序的言论；

（七）宣扬封建迷信、淫秽、色情、暴力、恐怖、赌博以及教唆犯罪的言论；

（八）公然侮辱他人或捏造事实诽谤他人的言论；

（九）其他违反宪法、法律和学校规定的言论、信息和网络行为。

学生使用网络时，不得进行下列危害网络系统运行和安全的操作：

（一）不得攻击、侵入他人计算机和移动通讯网络系统；

（二）不得人为损坏学校网络设施（包括面板模块、布线管、光纤、交换机、配线柜、网线等）；

（三）未经允许，不得私架服务器对外提供各种服务；

（四）未经允许，不得进入任何未经授权的校内或校外网络管理平台获取非公开信息和数据；

（五）未经允许，不得进入任何未经授权的校内或校外网络管理平台从事非法获利行为；

（六）不得制造和故意传播计算机病毒或发布、传播依附有计算机病毒的信息；

（七）不得故意制造或使用攻击手段使他人网络系统或联网计算机发生阻塞、溢出、瘫痪和资源异常。不得非法进行网络端口扫描，扰乱网络正常秩序。

学生有权对使用网络时发现的违反有关法律、法规和规章制度的人或者事予以制止或者向学校反映、举报。并有义务协助学校有关部门对上述人或事进行调查、取证、处理。

对于违反本规定条款者，将依照《学生违纪处分办法》进行处理。构成违反治安管理条例的，送交公安机关依照《中华人民共和国治安处罚条例》的有关规定处罚；构成犯罪的，移交司法机关依法追究刑事责任。

迁安市职教中心

2021 年 10 月修定

迁安职教中心网络安全培训制度

一、网络中心定期组织校园网管理员认真学习《计算机信息网络国际互联网安全保护管理办法》及校园网管理相关规章制度，提高工作人员的维护网络安全的警惕性和自觉性。

二、网络中心负责对校园网用户进行安全教育和培训，使用户自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，使他们具备基本的网络安全知识。

三、网络中心对校园网接入单位进行安全教育和培训，使他们自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，杜绝发布违反《计算机信息网络国际互联网安全保护管理办法》的信息内容。

四、不定期地安排专业技术人员进行信息安全方面的培训，加强对有害信息，特别是映射性有害信息的识别能力，提高防范能力。

五、网络中心应定期召开网络安全会议，通报网络安全状况，解决网络安全问题。

迁安市职业技术教育中心

2021 年 10 月修订

迁安市职业技术教育中心岗位网络安全责任制度

为加强我校信息化岗位管理，保证校计算机信息系统安全，制定本制度。

第一条校信息化岗位管理遵循“谁主管谁负责、谁运行谁负责、谁公开谁负责”的原则，实行安全和保密管理工作责任制。岗位所在部门负责人作为第一责任人，负责其职责范围内的计算机信息系统安全和保密管理。

第二条本规定中的信息化岗位指承载校计算机信息系统建设、管理和维护的岗位，主要包括校办公室和校信息工作人员，以及负有信息安全和保密责任的信息安全员和兼职保密员。

第三条校信息化岗位安全和保密管理按照国家保密法和国家信息安全等级保护的要求进行。

第四条信息化岗位实行岗位职责分离制度，岗位操作权限严格受岗位职责限制。除非主管领导批准，信息化岗位人员不得打听、了解或参与职责以外的任何涉及岗位安全和保密的内容。

第五条信息化岗位人员应保管好自己的信息系统操作口令，不定期予以更换。严禁向他人泄露自己的信息系统操作口令。因工作需要必须告知他人的，应在使用完毕

后即时更换口令。

第六条信息化岗位人员使用的台式和便携式计算机必须有密码保护措施，工作中离开岗位时计算机应置于屏幕保护状态。计算机无人使用时不得置于上网状态。

第七条非经主管领导批准，信息化岗位工作人员不得携带存有工作信息的便携式计算机外出。经主管领导批准携带便携式计算机外出的，应采取措施保证机内信息安全。携带外出的便携式计算机禁止留存涉及国家秘密和工作秘密的内容。

第八条重要的信息化岗位休息日和节假日安排人员值班，重大事件期间应组织安排 24 小时值班。值班期间，重点监控提供公共服务的信息子系统（如网站）运行状况，发现异常按局信息安全应急预案处理，并即时向主管领导报告。

第九条办公室应组织开展经常性的保密教育培训，提高校机关工作人员，尤其是信息化岗位工作人员的计算机信息安全保密意识与技能。

第十条校办公室负责校计算机信息系统安全和保密管理情况的监督。为此，应不定期地组织专业技术人员对信息化岗位人员使用的台式和便携式计算机应进行安全检查，发现并排除病毒、木马等安全隐患。

第十一条信息化岗位工作人员离岗离职，按以下程序办理：

1、整理好涉及信息安全和保密的资料或文档，形成信息交接档案，移交给指定的工作交接人员；

2、逐项取消其拥有的信息系统访问授权；

3、收回其使用的计算机存储介质，包括光盘、U 盘、移动硬盘等；

4、全部移交过程必须有完整的移交记录，经主管领导签字确认后生效。未完成以上程序，信息化岗位工作人员不得办理离岗离职手续。第十二条对违反本规定的人员将责令限期整改。引发信息系统运行异常、工作信息丢失损坏等安全事故的，追究相关人员的行政责任；造成泄密事件的，根据国家相关保密法律法规进行查处。

迁安市职业技术教育中心

2021 年 10 月修订

迁安职教中心网络信息安全保密协议书

甲方：迁安市职业技术教育中心（迁安市技师学院）

乙方：

根据《中华人民共和国计算机信息系统安全保护条例》以及其他相关法律法规规定，甲方因为工作关系向乙方提供设备，乙方不得利用甲方提供的电脑和网络系统进行违法犯罪活动。据此双方签订本协议：

一、乙方承诺不利用甲方提供的电脑制作、复制、发布、转摘、传播含有下列内容的信息：

⑴反对宪法基本原则的；

⑵危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

⑶损害国家荣誉和利益的；

⑷煽动民族仇恨、民族歧视，破坏民族团结的；

⑸破坏国家宗教政策，宣扬邪教和封建迷信活动的；

⑹散布谣言，扰乱社会秩序，破坏社会稳定的；

⑺散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

⑻侮辱或者诽谤他人，侵害他人权益的；

⑼含有法律法规禁止的其他内容的；

二、乙方不得利用甲方网络侵犯国家的、社会的、集体的利益和公民的合法权益。

三、乙方不得利用甲方提供的电脑和网络系统发送垃圾邮件、攻击其他网络和计算机系统传播计算机病毒，以及其他危害互联网信息安全的行为。

四、乙方不得通过甲方网络系统利用学校微信群、QQ 群发表、转摘、传播不负责任、造谣滋事、煽动偏激情绪、制造恐慌气氛、扰乱正常工作秩序等各种有害信息。

五、乙方使用电子函件进行网上信息交流，应当遵守学校保密规定，不得利用电子函件向与学校业务无关的第三人传递、转发或抄送医院机密信息。

六、乙方应当时刻提高保密意识，不得与单位业务无关的任何人在聊天室、电子公告系统、网络新闻上发布、谈论和传播学校机密信息。

七、乙方应当做好存有学校秘密信息的 u 盘、硬盘、笔记本电脑等其它相关设备的保管与维护工作。

八、乙方违反上述规定情节严重的，甲方有权进行处理，构成犯罪的送交司法机关。

甲方：　　乙方：

代表签名：　　签名：

年　月　日　　年　月　日

迁安职教中心网络管理负责人任命书

根据学校岗位需求和管理需要，经学校会议决议，现任命张书峰同志为学校网络管理负责人，对学校网络系统进行日常维护及安全管理。并授予以下职责和权限：

1、负责学校网络设备年度预算，对校园网络系统各部门、各机进行经常性的维护、保养工作，保障网络中心及各终端机正常运转。

2、对于系统硬件及软件出现故障、错误及时处理，并报告本部门主管领导，并尽快恢复正常。

3、对任何操作要认真、细致、准确，不准抱有尝试，进行无把握及非授权的指令操作。

4、安排人员认真完成数据的备份工作和各种资料归档工作，协助有关部门处理各类子系统问题，并做好数据保密工作。

5、负责培训和辅导各部门使用电脑人员正确操作硬件及使用软件，熟悉操作程序，提高部门业务水平。

6、保证网络的安全性，及时查杀各种病毒，密切注意特殊日期病毒的发作。

7、做好计算机设备维修所需备品、备件计划和机房用品计划，并做好所有资料、文件、数据的归类存档的管理工作。

8、掌握各系统管理密码，并做好定期修改工作。

迁安市职教中心

2021 年 10 月修订

迁安职教中心信息安全人员离岗管理办法

1.工作人员离岗离职时，有关部门应即时取消其计算机涉密信息系统访问授权。工作人员离岗离职之后，仍对其在任职期间接触、知悉的属于我校负有保密义务的秘密信息，承担如同任职期间一样的保密义务和不擅自使用的义务，直至该秘密信息成为公开信息，而无论离职人员因何种原因离职。

2.离岗人员因职务上的需要所持有或保管的一切记录着本单位秘密信息的文件、资料、图表、笔记、报告、信件、传真、磁带、磁盘、仪器以及其他任何形式的载体，均归学校所有，而无论这些秘密信息有无商业上的价值。

3.离职人员因工作需要离岗时，或者向学校提出请求时，返还全部属于学校的财物，包括记载着学校秘密信息的一切载体。若记录着秘密信息的载体是由离职人员自备的，则视为离职人员已同意将这些载体物的所有权转让给本单位，学校应当在离职

人员返还这些载体时，给予离职人员相当于载体本身价值的经济补偿；但秘密信息可以从载体上消除或复制出来时，可以由学校将秘密信息复制到本单位享有所有权的其他载体上，并把原载体上的秘密信息消除，此种情况下离职人员无须将载体返还，学校也无须给予离职人员经济补偿。

4.离职人员离职时，应将工作时使用的电脑、u 盘及其他一切存储设备中关于工作相关或与我校会有利益关系的信息、文件等内容交接给本部门领导，不得在离职后以任何形式带走相关信息。

5.离职人员因使用学校相关资料造成违法行为的，学校保留追究其法律责任的权利；

迁安市职业技术教育中心

2021 年 10 月修订

迁安职教中心计算机网络安全保密管理规定

为进一步加强学校计算机互联网络的管理，保障校内外计算机信息交流的健康发展，在网络使用中维护国家安全和做好保密工作，特制定本规定：

一、校内外计算机互联网络的单位、部门和个人，应当遵守《国家安全法》和《保密法》，严格执行学校关于安全保密的工作要求，不得利用互联网络从事危害国家安全、泄露国家秘密等违法犯罪活动，不得制作、查阅、复制和传播妨碍社会治安的信息及淫秽色情等信息。

二、加强计算机互联网络的安全保密管理，凡学校使用互联网络、装有节点的部门，必须有一位领导分管并指定专人负责安全保密工作，经常进行监督、检查，处理本部门涉及网络安全保密的有关事宜，并协助学校主管部门开展安全保密工作的检查指导。

三、各部门要及时、有效地做好入网人员的安全保密宣传教育工作，不断增强入网人员的国家安全意识和保密观念，网络操作人员应参加以安全保密为内容的学习培训，把好网络入口关，切实做到警钟长鸣。常备不懈，自觉维护国家利益。

四、凡属国家秘密文件、资料一律不得输入计算机互联网络，各部门涉密人员必须做好秘密文件、资料及涉密科研项目、成果的保管工作，管好秘密源头。

五、凡属预备上网资料，必须首先送校分管领导审查，经审核通过后方可上网。

六、各部门要加强对计算机介质(U 盘光盘移动硬盘等) 管理，对贮存有秘密文件、资料的计算机等设备要有专人或兼职人员操作，采取必要的防范措施，严格对涉密贮介质的管理，建立规范和管理制度，存贮有涉密内容的介质一律不得进入互联网络使用。

七、各部门和个人在网络使用过程中无意识地收到反动宣传品和具有淫秽色情内容的东西，要及时采取删除措施，报告主管领导，并将收到的材料送学校有关部门集中处理，不得扩散。

八、学校各部门应根据本部门具体情况，制定相应的管理制度并大力加强计算机网络安全保密防护方法的研究，在加强安全保密工作的同时，逐步配备现代化的保密设备，利用现代化的科学技术，保证涉密信息的安全，防止泄露事件的发生。

九、学校主管部门将对各部门贯彻执行《校园网安全保密管理规定》的情况进行检查，凡违反本规定的部门或个人，学校将视情节轻重，给予严肃处理。

迁安市职教中心

2021 年 10 月修订

外部人员访问机房等重要区域审批制度

为维护信息系统安全， 确保各应用系统安全稳定运行和重要区域信息安全，制定本审批制度。

一、非本单位机房工作人员进出机房等重要区域，须按本制度进行审批。

二、因工作需要进出机房等重要区域，相关区域负责人员应根据操作内容，确定进入人员，重大操作原则上应放在业务数据录入或备份之后进行。进入人员需填写登记表，整个工作过程需由相关科室工作人员陪同进行。

三、非本科室人员,严禁单独进入机房等重要区域,确需进入的,相关机房值班人员必须全程跟踪， 严禁从事非业务范围内的其它任何操作。

四、外部参观人员出入机房等重要区域，由单位领导或科室负责人陪同进行参观，相关区域工作人员需做好登记备案工作。

五、进入机房的人员要保持机房的清洁、卫生。严禁在机房内吵闹、吸烟、吃零食，严禁携带任何易燃、易爆、腐蚀性、强电磁、辐射性、流体物质等进入，避免对机房设备构成威胁。

六、相关业务人员进入机房，原则上须两人同时进出，并按规定进行相关业务操作，严禁随意对设备进行操作，严禁接触与业务无关的设备，如违规造成网络和业务系统事故的，将追究操作人员的责任。

七、进入机房人员在机房内完成相关工作时，需保证机房正常的环境秩序，认真填写机房内工作内容后方可退出。

八、机房等重要区域配备监控设施，未按规定进入者，如造成损失和泄密等不安全后果的，相关重要区域负责人和相关重要区域工作人员，给予严肃处理。损失后果情节严重的，由相关规定进行处理；如触犯国家有关法律、法规者，移交公安、司法机关处理。违反本规定，给国家、集体或者他人财产或人身安全造成损失的，应当依法承担民事或刑事责任。

外部人员进入机房等重要区域审批登记表

序号	日期	单位或部门	姓名	进出事由	起止时间	审批领导

迁安市职教中心

2021 年 10 月修订

迁安职教中心网络安全事件应急预案

一．预防措施

1、加强领导，健全组织，强化工作职责，完善各项应急预案的制定和各项措施的落实。

2、充分利用各种渠道进行网络安全知识的宣传教育，组织、指导全校网络安全常识的普及教育，广泛开展网络安全和有关技能训练，不断提高广大师生的防范意识和基本技能。

3、认真搞好各项物资保障，严格按照预案要求积极配备网络安全设施设备，落实网络线路、交换设备、网络安全设备等物资，强化管理，使之保持良好工作状态。

4、采取一切必要手段，组织各方面力量全面进行网络安全事故处理工作，把不良影响与损失降到最低点。

5、调动一切积极因素，全面保证和促进学校网络安全稳定地运行。

二．现场处置及救援措施

1、发现出现网络恶意攻击，立刻确定该攻击来自校内还是校外；受攻击的设备有哪些；影响范围有多大。并迅速推断出此次攻击的最坏结果，判断是否需要紧急切断校园网的服务器及公网的网络连接，以保护重要数据及信息；

2、如果攻击来自校外，立刻从防火墙中查出对方 IP 地址并过滤，同时对防火墙设置对此类攻击的过滤，并视情况严重程度决定是否报警。

3、如果攻击来自校内，立刻确定攻击源，查出该攻击出自哪台交换机，出自哪台电脑，出自哪位教师或学生。接着立刻赶到现场，关闭该计算机网络连接，并立刻对该计算机进行分析处理，确定攻击出于无意、有意还是被利用。暂时扣留该电脑。

4、重新启动该电脑所连接的网络设备，直至完全恢复网络通信。

5、对该电脑进行分析，清除所有病毒、恶意程序、木马程序以及垃圾文件，测试运行该电脑 5 小时以上，并同时进行监控，无问题后归还该电脑。

6、从事故一发生到处理事件的整个过程，必须保持向领导小组组长汇报、解释此次事故的发生情况、发生原因、处理过程。

三．事故报告及现场保护

1、确保 WEB 网站信息安全为首要任务：关闭 WEB 服务器的外网连接、学校公网连接。迅速发出紧急警报，所有相关成员集中进行事故分析，确定处理方案。

2、分析网络，确定事故源：使用各种网络管理工具，迅速确定事故源，按相关程序进行处理。

3、事故源处理完成后，逐步恢复网络运行，监控事故源是否仍然存在。

4、针对此次事故，进一步确定相关安全措施、总结经验，加强防范。

5、从事故一发生到处理的整个过程，必须及时向领导小组组长以及教务处以及校长汇报，听从安排，注意做好保密工作。

四．事故调查及处理

1、在应急行动中，各部门要密切配合，服从指挥，确保政令畅通和各项工作的落实。

2、事后迅速查清事件发生原因，查明责任人，并报领导小组根据责任情况进行处理。

迁安市职教中心

2021 年 10 月修定

迁安职教中心网络突发事件及有害信息处置预案

按照国家相关部门关于校园网络和互联网有害信息专项清理整治工作的要求，为做好校园网络信息安全应急处置工作，并适时处理好校园网络突发事件，以维护校园稳定，最大限度地减轻突发事件造成的损失与影响，特制定本预案。

一、校园网络突发事件应急处置小组组成及相关部门和职责，当发生下列情况之一时，校园网络突发事件应急处置小组开始应急处置工作，突发事件处置预案启动：

1、校园网络系统设备及相关设施遭受严重破坏。

2、校园网络信息系统及服务遭受反动组织、法轮功组织攻击，散布反动言论和有害信息造成严重影响、损失和破坏。

3、校园网络信息系统及服务遭受黑客、病毒攻击或黄色信息及其他有害信息的干扰致使网络用户受到干扰，造成严重影响、损失和破坏。

（一）校园网络突发事件应急处置小组人员

组 长：凌志杰、闫学东

副组长：田与光　陈小宝 郑立冬

成员：各系部主任、党办主任、宣传科主任、网络中心主管

主要职责：

1、及时了解和掌握突发事件起因、经过和发展态势。

2、根据校园网络相关部门的监控预报意见，研究制定突发事件解决方案。

3、通知校园网络相关部门及人员做好应急处置准备，并做好校园网络维护专业队伍的组织协调工作。

4、及时传达上级党委、政府对校园网络和互联网安全的各项指示。

5、编写校园网络破坏及损失评估报告，报上级部门或相关安全部门。

（二）各部门领导及技术负责人职责

1、及时向学校反馈校园网络中遇到的突发问题。

2、最大限度减小和消除突发事件造成的损害范围和突发事件造成的不良影响。

3、通过堵、删、管、查、监并举，严防反动、黄色、法轮功等有害信息和黑客对网络和计算机系统的入侵和攻击。

4、保持日常网络和计算机系统的病毒检测，发现病毒感染应及时进行清除，防止扩散和蔓延。

（三）网络中心工作职责

1、负责校园网络及信息的安全技术指导、支持和保障工作，及时解决突发事件和问题，保证校园网络的正常使用。

2、通过堵、删、管、查、监并举，严防反动、黄色、法轮功等有害信息和黑客对网络和计算机系统的入侵和攻击。

3、保持日常网络和计算机系统的病毒检测，发现病毒感染应及时进行清除，防止扩散和蔓延。

4、建立健全网络事故报告制度，并及时向上级领导、上级部门和安全部门报告。

5、配合公安及安全部门做好截源堵头工作。

二、 应急处置反应预案的实施 预案程序:

（一）接报后，立即由组长或副组长召开校园网络突发事件应急处置小组成员紧急会议。

1、会议听取有关部门汇报突发事件情况。

2、部署突发事件应急处置工作，组织校园网络维护专业队伍及时进入现场。

3、向省教育厅、公安部门、安全部门报告事件情况，特殊情况请求支援。

（二）组长或副组长立即率有关人员赶赴现场，成立现场指挥部，直接负责应急处置工作。

（三）各专业人员接到领导小组通知后立即赶赴现场开展救援维护工作。

1、尽快恢复网络系统、信息系统和网络服务的正常运转。

2、严格实行 24 小时值(守)班制度，对计算机系统和网络系统进行实时维护，确保计算机系统和数据库正常运行。

3、值班人员做好值班日志和相关记录，建立应急处置工作档案。

4、切实保证校园网络突发事件的有效解决，并健全防范措施。

(四）编写校园网络突发事件损失评估报告，及时上报相关部门。

(五）拟定重建规划方案，经相关部门审批后，对校园网络进行修复。

(六）待校园网络突发事件完全解决后，取消应急状态。

三、其它

1、本预案由迁安职教中心负责解释。

2、应急处置预案启动后，严格执行领导责任制，专人负责制。

迁安市职教中心

2021 年 10 月修定