**海南健康管理职业技术学院**

**信息技术部规章制度**

**目录**

[信息技术部工作职责 1](#_Toc504858284)

[信息技术部规章制度 2](#_Toc504858285)

[信息技术部教职工考勤与请假制度规定 6](#_Toc504858286)

[信息技术部经费管理办法 9](#_Toc504858287)

[信息技术部固定资产管理办法 11](#_Toc504858288)

[信息技术部重大事项议事规则 14](#_Toc504858289)

[信息技术部核心机房管理办法 17](#_Toc504858290)

[智慧教室、多媒体教室设备管理制度 20](#_Toc504858291)

[网络与信息安全类突发公共事件应急预案 21](#_Toc504858292)

# 信息技术部工作职责

一、负责本校信息化建设的策划与制定、实施与推广工作。负责数字化校园平台规划、设计与建设，组织专业教师和技术人员对数字校园平台及所集成系统的管理、维护、用户培训及应用推广工作。

二、负责面向全校的计算机基础与应用及其它各相关专业基础课程教学工作。

三、承担学校教育信息化技术培训工作。

四、制定本校信息化发展规划并指导具体实施。

五、负责本校网络与教育技术中心规划、建设的指导工作，为各学科开展数字化实验教学工作并为相应信息化研究提供技术支撑。

五、承担全校教职员工信息技术素养提升的培训工作。

六、与科教处协作负责指导本校所属单位的数字化课程建设、应用及研究等工作。

七、负责本校信息化相关师资队伍建设、人才引进和培养工作。

# 信息技术部规章制度

1. 总则
2. 为了加强海南健康管理职业技术学院信息技术部内部建设，促进信息技术部管理专业化、制度化，增强团队凝聚力和执行力，更好地服务于学校教育教学工作，特制订本规章制度。
3. 海南健康管理职业技术学院信息技术部是推进学校教育信息化建设和应用，为学校教学、科研提供教育技术、网络技术与信息技术的教学管理机构，是学校公共教学体系的重要组成部分。
4. 本规章制度适用于海南健康管理职业技术学院信息技术部全体人员。
5. 工作职责
6. 海南健康管理职业技术学院信息技术部人员应根据各自岗位认真履行以下工作职责。
7. 应负责信息技术部各项日常工作，包括信息技术部年度工作计划、工作总结、办公室会议纪要和会议简报的起草和发布；
8. 应督查信息技术部工作计划、阶段目标、决定决议、领导指示的执行、落实情况；
9. 应做好信息技术部对外联系和接待工作。协调对接学校各级单位工作，草拟和统稿涉及信息技术部整体情况的各类文件；
10. 应做好信息技术部经费管理、印章管理、档案管理工作；
11. 应做好信息技术部内外文件的收发、登记、办理、归档等工作；
12. 应做好信息技术部考勤、考纪，来信来访，处理服务质量投诉；数据统计和宣传工作；中心网站的维护工作；
13. 应做好信息技术部固定资产、低值易耗器材及办公用品的管理、使用分配等工作。
14. 应负责校园网规划、设计与建设；
15. 应负责校园网骨干网络和中心机房的管理、运行和维护，以及互联网出口维护。
16. 应负责数据中心、网络存储和高性能计算机系统、认证计费、远程接入等网络基础平台的建设、运行与维护；
17. 应负责为各职能部门信息系统提供网络技术支持和服务器托管服务。
18. 应负责校园网络的安全监测。
19. 应负责数字化校园平台规划、设计与建设，数字校园平台及被集成系统的管理、维护、用户培训及应用推广。
20. 应负责电子邮件、软件正版化等网络基础平台的建设、运行与维护。
21. 应协助网站群系统推广和学校二级网站的质量考核与评比，指导学校二级网站建设，提供部门级应用系统建设的技术支撑。
22. 应负责数字校园信息系统及其他相关信息系统的安全监测，按国家网络安全法要求做好各信息系统的等保备案、定级、测评和整改工作。
23. 应积极探索信息技术在教育教学领域的应用实践，指导或协助开发相关应用系统。
24. 应负责学校数字课程视频媒体采集、编辑制作；
25. 应负责配合相关单位与部门做好教学资源库的建设等业务。
26. 应负责或协助数字化教学资源建设，为教师自建教学资源提供技术支持。
27. 应积极探索新媒体技术在教学资源领域的应用实践，指导或协助开发相关教学资源应用系统。
28. 应负责全校多媒体教室设备的管理和维护。
29. 工作纪律
30. 严格遵守工作纪律，按时上下班，不迟到，不早退，不擅自离岗，不在工作时间做与工作和业务不相关的事情。值班期间，按时到岗，不擅自离岗，并时刻保持工作电话畅通。
31. 严格遵守请假制度，不无故旷工。
32. 信息技术部工作人员接到设备报修或应用维护申请后，应立即处理。如遇紧急情况无法及时处理，应说明情况。
33. 应保持良好的服务态度，认真耐心地解决问题，严禁与师生发生任何冲突或争吵。
34. 应认真及时地完成部门安排的任务，不得无故拖延。对于确实存在困难一时无法完成的任务，应及时向分管领导进行反馈。

# 信息技术部教职工考勤与请假制度规定

为了加强管理，强化教职工“岗位”意识，调动教职工工作积极性并提高工作效率，妥善处理岗外事务与岗位职责的关系，确保各项工作的顺利完成，根据中心实际情况作如下规定：

由综合办公室负责考勤,并按时上报学校人事处。

一、关于迟到、早退、旷工的规定

（一）迟到

教职工应在上午8：00、下午3：00之前（多媒体教室管理部门教职工上午应提前20分钟，下午提前10分钟）上班，超过规定时间20分钟仍未到岗者视为迟到。每月迟到三次以上的人员名单由综合办公室在中心内部进行公示。

（二）早退

教职工应在中午12：00、下午6：00之后（多媒体教室管理部门教职工下午可提前30分钟）下班。在不向三级部门负责人请假的情况下，提前半小时之内离岗者视为早退。早退人员名单由综合办公室在中心内部进行公示。

（三）旷工

没有假条又没有履行相关手续而无故未在岗者视为旷工。如无特殊情况，迟到或早退半小时以上３小时以内又没按规定请假者视为旷工半天；迟到或早退３小时以上又没按规定请假者视为旷工一天。

注：在年终绩效考核实施细则中“勤”考核共30分，其中设置考勤５分。全年累计迟到公示０次考勤为５分；迟到公示１次考勤为４分；迟到公示２次考勤为３分；迟到公示３次考勤为２分；迟到公示４次考勤为１分；迟到公示５次及以上考勤为０分。

二、关于事假、病假的规定

（一）事假

　　教职工如遇私事必须利用工作时间办理的，可请事假。教职工应提前办理请假手续，来不及办理请假手续的，要及时打电话声明，回单位后及时补办，否则按旷工处理。

（二）病假

教职工因病不能上班，应请病假。请病假须填写请假审批表，来不及办理请假手续的，要及时打电话声明，回单位后及时补办，否则按旷工处理。

（三）教职工请事假（病假）要填写请假审批表（附件１），履行以下请假手续。

1、二日以内请假：个人提出申请、部门负责人审核、主任审批；

2、三日以上请假按海南健康管理职业技术学院考勤管理办法执行。

3、口头请假无效，特别紧急情况无法请假的，可以在口头征得主任同意后，事后补办请假手续并说明原因。请假审批表中要特别注明请假事由和起止时间，无起止时间视为无效。事后由请假人把审批后的请假申请表交由综合办公室备案。

5、三天以上（含三天）应提供正规医院开具的病假诊断证明，假后交由办公室备案。教职工不得采取欺骗手段获取病假，一经发现，将严肃处理。

三、特殊情况处理

如有晚间加班、出差或因学校班车延误等特殊情况引起的迟到、早退等事项，由部门负责人或主任向办公室说明情况，办公室备案，不做迟到或早退记录。如有特殊情况有正当理由确需延长请假时间，可将具体情况报至办公室，经中心领导班子讨论后可在不耽误工作的情况下在家办公。

四、关于其它规定

丧假、探亲假、婚假、生育假、工伤假、销假和旷工等按照海南健康管理职业技术学院教职工考勤管理规定执行。

# 信息技术部经费管理办法

第一章  总　  则

第一条 为规范海南健康管理职业技术学院信息技术部经费管理工作，根据学校的财务管理制度和相关规定，制订本办法。

第二条 信息技术部的经费管理实行主任负责制，信息技术部主任是经费管理工作第一责任人。

第三条 办公室负责财务日常工作，定期公开各类经费收支状况。

第二章 开支审批

第四条 办公设备（电脑、打印机等）的添置与办公日常消耗品购买经主任同意后由信息技术部办公室具体经办。报账时，发票上须有项目负责人或设备管理人签字。

第五条 信息技术部的招待费，严格按学校相关规定执行，因工作需要经主任同意的可以发生招待费用，但要力行节约，招待费单据上要注明事由及参加人员等。

第六条 信息技术部编制外用工、勤工助学学生工资等开支按学校规定或聘用合同约定执行。

第七条 信息技术部工作人员的年终二次分配等需经信息技术部办公会议研究决定后执行。

第三章  报账程序

第八条 办公易耗品购买费用报销由办公室统一办理。

第九条 差旅费报销

（一）信息技术部主任出差，且无信息技术部其他人员随同的，相关差旅费报销由办公室办理。

（二）有信息技术部人员随同的，由随同人员需提供经由领导批准签字的出差通知、本人签字的交通住宿等费用票据，报销材料齐全后交由办公室统一办理。

# 信息技术部固定资产管理办法

第一章  总　  则

第一条 为加强海南健康管理职业技术学院信息技术部固定资产管理，提高资产使用效益，依据中心实际，特制定本办法。

第二章 适用范围

第二条 本办法所称固定资产包括单价在200元以上的家具、500 元以上的一般设备和800 元以上的专用设备等，能独立使用且使用年限在1年以上，并在使用过程中基本保持原来物质形态的资产。具体范围为：

（一）办公自动化设备：计算机、打印机、传真机、复印机、速印机、投影仪、扫描仪、通讯设备等。

（二）电器设备：摄影、摄像器材、空气调节设备等。

（三）机房、办公室、会议室家具。

（四）支撑基本业务运行的各类软硬件设备

（五）重要图书资料。

（六）其它未列入设备。

第三章 管理职责分工

第三条 信息技术部办公室负责固定资产实物登记统计工作；负责组织对固定资产进行定期盘点、清理核对工作；协助对固定资产调拨、报废、残值处理工作；负责向学校相关部门办理固定资产采购结算工作；负责对固定资产增减变动并及时进行账务申报；负责对固定资产总账及明细分类账核算等管理工作。

第四条 各部门负责支撑本部门基本业务的固定资产采购、验收、保管、维修保养工作；配合信息技术部办公室对本部门固定资产进行定期盘点、清理核对工作；配合信息技术部办公室做好固定资产调拨、报废、残值处理等有关管理工作。

第四章 购置计划编制

第五条 由各部门根据当年业务需要结合中心经费状况，制订固定资产购置计划，报主任审定或经信息技术部办公会研究通过、主管部门审批后执行。

第五章  固定资产采购

第六条 属学校招标采购范围内的固定资产，不得自行采购。先填报设备采购申请表，再向学校总务处和财务科等部门办理购置、结算手续。

第七条 不属于学校招标采购范围的固定资产，应在进行广泛的市场询价基础上择优购置。

第六章  固定资产验收、保管、使用、借用、报废

第八条 新购入的固定资产，应先做好验收工作。由使用部门及使用人验收，验收人员要严格把关，对所验固定资产的数量、质量、附件、资料等都要认真检查。

第九条 各部门使用的固定资产，领用及保管要明确责任人。贵重财产除安排专人保管外，还要落实安全保管措施。固定资产外借必须经部门负责人批准，未经批准不得随意转借，并要有登记手续。

第十条 固定资产变更使用管理部门，必须经主任同意并在信息技术部办公室办理相关手续。

第十一条 固定资产的减少变动（调出、变卖、报废、丢失、损坏）都必须按规定履行报批手续。

第七章  固定资产清查

第十二条 要坚持固定资产定期清理、清查制度。各部门使用的固定资产应每半年自查一次，每年全面清查一次，做到账物卡相符。

# 信息技术部重大事项议事规则

第一条 为加强中心领导班子民主集中制建设，规范和监督领导班子的议事决策行为，不断提高决策的民主化、科学化水平，促进中心工作全面协调发展，结合中心实际特点制定本规则。

第二条 信息技术部领导班子研究决定重大事项，必须严格遵守民主集中制的原则，实行集体议事、集体决策，决策须服从于学校总体工作部署向学校总务处和财务科等部门办理购置，须与学校的发展规划相一致。

第三条 规则所指的重大事项包括：

（一）贯彻落实上级有关部门重大决策和重要工作部署的意见和措施。

（二）信息技术部的发展规划和年度计划、年度总结，重要规章制度。

（三）人事调配、岗位聘任、专业技术职务评聘、奖惩等，包括：领导班子分工调整、部门内工作职责调整、人员调整、岗位聘任、技术职务聘任、各项奖惩评选等。

（四）信息技术部岗位职责和服务制度制定和修订、各项业务管理流程制定和修订。

（五）年度经费预算、重大项目资金使用。

（六）信息技术部新建、改造、升级及维修项目的确定。

（七）需要信息技术部内各部门间协调的事项。

（八）其他需要集体讨论决定的重要事项。

第四条 重大事项议事决策前，要充分听取各方面的意见和建议，并加强沟通联系，必要时组织专家、专业机构进行评估论证，做到有备而议，慎重决策。

第五条 领导班子研究决定重大事项时，必须按下列程序进行：

（一）会议形式。领导班子以召开领导班子会议的形式研究决定重大事项并作出决策。涉及研究重大事项的领导班子会议根据工作需要随时召开。

（二）出席成员：根据议题研究内容确定列席人员；会议由信息技术部主任主持。

（三）确定议题。议题由主任提出，应在班子成员之间事先沟通，由信息技术部主任确认是否需要上报学校领导或由中心领导班子确定。

（四）会前准备。办公室准备相关材料，除遇紧急情况外，至少提前一天将会议议题和详细情况通知与会人员。

（五）充分讨论。会议开始时，先由分管领导或相关部门汇报议题内容，然后对议题进行充分讨论；班子成员都要发表意见，表明态度；因故未到会班子成员的意见，可用书面或其它形式表达并由办公室存档。

（六）逐项表决。对赞成与反对意见有较大分歧时，暂缓表决，待进一步调查研究、充分协商后讨论决定，必要时请示主管校领导。属重大问题范围内的突发事件和紧急情况而来不及召开领导班子会议的，信息技术部主任可临机处理，事后及时在领导班子会上通报。

（七）作出决定。信息技术部领导班子成员按照少数服从多数的原则，采取表决的方法作出决定，赞成数超过应到会班子成员半数的方为通过；领导班子会议由信息技术部主任在集中班子成员意见的基础上作出最后决定；对决策事项意见分歧较大的，可暂缓决定。

（八）会议必须作正式记录。“会议记录”应记录每个议题的内容、讨论过程、表决情况及最后决定，明确落实决定的责任。办公室主任负责记录和保管会议记录，并将电子版发中心领导班子成员。

# 信息技术部核心机房管理办法

第一章  总则

第一条 本办法适用于海南健康管理职业技术学院信息技术部教学楼五楼核心机房的日常运维管理。

第二章  出入管理

第二条 信息技术部核心机房存放有校园网各类主干网络设备及数据中心服务器，非机房工作人员未经批准不得进入机房。

第三条 外单位维护人员（指信息技术部以外的校内校外单位或部门）进出机房必须进行登记，并在机房工作人员陪同下进入机房。

第四条 参观人员需事先联系，并得到中心负责人批准，才能在工作人员陪同下进入机房。

第五条 严禁其他无关人员进入机房。

第六条 进入机房应遵守本办法并听从机房工作人员指导。

第七条 进入机房不得携带任何易燃、易爆、腐蚀性、强电磁、辐射性、流体物质等对设备正常运行构成威胁的物品。

第三章  操作管理

第八条 非机房工作人员不经允许，不得接触和操作机房内任何设备、设施。

第九条 网络机柜、网络设备的增减、更换，网络配置的增删修改以及网络结构的变更必须由中心网络运行维护部主管副主任负责授权和实施。

第十条 机房内关键网络设备的操作实行双人作业制度，严格按照预制操作流程进行。有关过程必须按规定进行详细登记和记录。

第十一条 操作人员注意保持机房整洁，操作结束后整理好有关工具和配件。

第四章  运行管理

第十二条 机房工作人员在工作日每天巡检机房一次，检查机房环境支撑设施运行状况，并进行记录。

第十三条 设备管理员随时监控机房设备运行状况，发现异常情况应立即按照预案规程进行操作，并及时上报和详细记录。

第十四条 机房工作人员应恪守保密制度，不得擅自泄露各种信息资料与数据。

第十五条 机房内严禁吸烟、喝水、吃食物、嬉戏和进行剧烈运动，保持机房安静。

第十六条 定期对机房进行清扫，对机器设备吸尘清洁。

第十七条 不定期对机房内设置的强电系统、消防器材、监控设备进行检查，以保证其有效性。

# 智慧教室、多媒体教室设备管理制度

为更好地服务于教学工作，特制订如下智慧教室、多媒体教室设备管理制度：

一、教室设备管理维护人员须提前到岗巡视所辖智慧教室、多媒体教室设备运行情况，即早上7:45，下午2:50（特殊情况除外）。

二、接到报修电话，应了解故障情况，如无法在电话中指导教师解决，须5分钟内赶到现场对问题进行处理。

三、保持良好的服务态度，应认真耐心地解决师生反馈问题。严禁与师生发生任何冲突或争吵。

四、做好经常性维护和巡查，减少多媒体设备故障率。

五、定期对多媒体教室教学用计算机进行统一的病毒库升级，并全盘扫描查杀病毒，要求一学期至少两次。

六、定期升级多媒体教室计算机教学常用软件，如：Office、视频播放器、WPS等。

七、每学期开学前两天，对所有教室多媒体设备进行全面检查和软件升级，确保新学期教学工作顺利进行。学期末，对教室多媒体设备进行全面检查，统计设备使用及损耗情况，损坏设备及时报修，并做好跟踪检测和验收。

# 网络与信息安全类突发公共事件应急预案

第一章 总则

### 1.1 编制目的

为建立健全校园网络与信息安全类突发公共事件应急工作机制，提高应对网络与信息安全类突发公共事件的能力，预防和减少网络与信息安全类突发公共事件造成的损失和危害，维护海南健康管职业技术学院信息系统安全和稳定。

### 1.2 编制依据

《教育系统社会安全类突发公共事件应急预案》和《教育系统网络与信息安全类突发公共事件应急预案》

### 1.3 适用范围

本预案适用于海南健康管职业技术学院网络与信息安全类突发公共事件。按照《国家网络与信息安全事件应急预案》规定，本预案所指的网络与信息安全事件分为有害程序事件、网络攻击事件、信息内容安全事件、设备设施故障和灾害性事件。

（1）有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

（2）网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

（3）信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

（4）信息内容安全事件是指通过网络传播法律法规禁止信息、组织非法串联、煽动集会游行或炒作敏感问题并危害校园安全、学校稳定和师生权益的事件。

（5）设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

（6）灾害性事件是指由自然灾害等其他突发事件导致的网络与信息安全事件。

### 1.4 工作原则

1.4.1 统一指挥，快速反应

建立健全处置学校全局性网络与信息安全类突发公共事件的快速反应机制，确保预警、发现、报告、指挥、处置等环节的紧密衔接，做到快速反应，正确应对，果断处置，防止事态升级和蔓延扩大。遇到重大紧急事件时应成立网络与信息安全应急处置专家组以及计算机网络应急协调小组。

1.4.2 预防为本，及时控制

应立足于防范，抓早抓小，认真开展日常情况下事件排查调处工作，强化信息的广泛收集和深层次研判，争取早发现、早报告、早控制、早解决，把网络与信息安全类突发公共事件风险控制在一定范围内。

1.4.3 系统联动，快速反应

发生突发公共事件后，各相关部门负责人要立即深入第一线，掌握情况，开展工作，控制局面。形成各级各部门系统联动、密切协同的处置工作格局。

1.4.4 依法办事，科学处置

在处置突发公共事件过程中，做到合情合理、依法办事，切实维护师生合法权益，处置工作要自觉维护法律法规的权威性和政策的严肃性，注意工作的方式方法，防止矛盾激化和事态扩大。根据事件发展情况，必要时采取果断措施，解决制止违反犯罪行为。

1.4.5 加强保障，重点建设

从制度上、组织上、物质上、技术上全面加强保障措施。在经费保障和力量部署等方面加强硬件和软件建设，增强工作实力，提高工作效率。

第二章 事件分级标准

参照《教育系统社会安全类突发公共事件应急预案》事件分级标准，根据事件的性质、突发紧迫程度、形成规模、行为方式、激烈程度、可能造成的危害、可能发展蔓延的趋势等，由高到低分成四个等级。

### 2.1 特别重大网络与信息安全事件（I级）

符合下列情形之一的，为特别重大网络与信息安全事件（I级）：

（1）校园网信息系统中的数据丢失或被窃取、假冒，对教育系统安全和稳定构成特别严重威胁。

（2）出现通过校园网传播反动信息、煽动性信息、涉密信息、谣言等情况，对校园网信息系统安全和稳定构成特别严重危害，引发学校大规模群体性事件，对学校教学、科研和生活秩序产生严重影响，教育教学活动无法正常进行，师生反应强烈并有过激行为的事件。

（3）其他校园网信息系统安全和稳定构成特别严重威胁，造成特别严重影响的网络与信息安全事件。

### 2.2 重大网络与信息安全事件（II级）

符合下列情形之一且未达到特别重大网络与信息安全事件的（I级）的，为重大网络与信息安全事件（II）。

（1）教育网内信息系统中的数据丢失或被窃取、假冒，对校园网信息系统安全和稳定构成重大威胁。

（2）出现通过教育网传播反动信息、煽动性信息、涉密信息、谣言等情况，对教育系统安全和稳定构成重大危害，引发学校突发群体性事件，对学校教学、科研和生活秩序产生较大影响，师生反应强烈的事件。

（3）其他校园网信息系统安全和稳定构成重大威胁，造成重大影响的网络与信息安全事件。

### 2.3 较大网络与信息安全事件（III级）

符合下列情形之一且未达到重大网络与信息安全事件的（II级）的，为较大网络与信息安全事件（III级）。

（1）校园网络信息系统中断运行造成较严重影响的。

（2）校园网信息系统中的数据丢失或被窃取、假冒，对校园网信息系统安全和稳定构成较大威胁。

（3）出现通过校园网传播反动信息、煽动性信息、涉密信息、谣言等情况，对校园网信息系统安全和稳定构成较大危害，对学校教学、科研和生活秩序产生一定影响，引起师生广泛关注的事件。

（4）其他校园网信息系统安全和稳定构成较大威胁，造成较大影响的网络与信息安全事件。

### 2.4 一般网络与信息安全事件（IV级）

除上述情形外，校园网内出现对信息系统安全和稳定构成一定威胁，对学校教学、科研和生活秩序产生一定影响的网络与信息安全事件，为一般网络与信息安全事件。

第三章 网络与信息安全类突发公共事件应急处置原则

（1）应统一指挥校园教育信息系统全局性网络与信息安全类突发公共事件的预防和处置。

（2）应研究确定事件性质、类型和级别，确定与其它类特定事件应急处置预案的联系，下达应急处置任务。

（3）重大事件应成立处理校园网教育信息系统重大网络与信息安全类突发公共事件专项工作组或调查组适时开展处置和善后恢复工作。

（4）重大事件应报送教育厅、海南省网络与信息安全事件应急指挥部和相关部门的标准、内容以及请求上级部门指示，联系相关单位协助。

（5）应督查事发部门和相关部门的处置工作。

（6）应组织评估重大网络与信息安全类突发公共事件所产生的损失与相关的处置情况。

（7）应督查汇总校园网络内安全工作，包括有害程序事件、网络攻击事件、设备设施故障和灾害性事件。协调、指挥调度校园网内各相关单位的网络与信息安全突发公共事件的应急处置工作。

第四章 预防预警

### 4.1 预防措施

应及时采取有效措施，避免和减少网络与信息安全事件的发生及其危害。具体措施包括：

（1）加强教育引导

全面加强师生思想政治工作，掌握师生动态。按照早发现、早报告、早控制、早解决的要求，把问题解决在萌芽状态，把风险控制在一定范围内。

（2）完善应急管理制度

建立严格的应急管理制度，负责制定本单位相关的应急预案、网络管理、机房管理、保密协议等规定，通过培训等手段不断提高管理人员的技术水平、责任意识和安全意识。

（3）加强技术防范措施

建立安全、稳定的网络运行环境，加强网络与信息安全的防护措施，在网络出入口安装必要的检测系统，定期进行网络漏洞扫描，实时监测局域网和关键信息系统。

重要信息系统采用高可靠设备，使用成熟稳定的系统和应用软件，进行定期系统和数据备份；采取有效的安全保护手段，及时进行系统更新并为系统打补丁；遵守安全操作规范，关闭所有不必要的服务和账号；严格限制内部用户的访问权限；对关键系统实施全时动态监测。

建立严格的信息上网审查制度，有效阻止不良信息传播，主要环节包括：网络边界的访问控制；反垃圾邮件措施；WEB和FTP服务器24小时实时监控；BBS内容过滤机制等。在学校督查不折不扣落实“用户实名注册”和“BBS校内信息交流平台”两项措施。

### 4.2 监测预警

建立严格的信息报送机制，完善快速应急处置的信息处理机制。

4.2.1 信息报送原则

（1）迅速：最先发现或接到发生网络与信息安全类突发公共事件的单位和个人，应按照“先口头、后书面”的原则，第一时间向学校党政、院长办公室报告，最迟不得超过3小时，在事件处置过程中再跟报、续报。

（2）准确：信息内容要客观翔实、不得主观臆测，不得漏报、瞒报、谎报。

（3）直报：网络与信息安全类突发公共事件一般采取分级报送原则。发生I、II级时间，应直接报省党委、政府、教育厅。

4.2.2 信息报送内容

（1）首报信息应包括事件的基本情况，含时间、地点、规模、涉及人员和单位、设备受损和人员受伤情况、对国家安全与社会安全的威胁程度以及事件发展趋势等。

（2）跟报信息应包括事件起因分析、性质判断和影响程度评估；事发单位或部门拟采取的措施。

（3）续报信息应包括校内外公众及媒体等方面的反应；事件发展状态跟踪、处置过程和结果；在事件处置完后报送事件的评估结果与处置总结。

（4）需要报送的其他事项。

4.2.3 信息处理机制

（1）网络与信息安全工作组办公室负责汇总、分析和研判网络与信息安全类突发事件发生后具体情况及各方面的反应，掌握发展态势；接到网络与信息安全类事件信息后，立即报告网络与信息安全工作组，通报有关处置；I、II级事件按教育部《教育系统网络与信息安全类突发公共事件应急预案》4.2.4条规定执行。

（2）根据工作需要，应与上级主管部门、公安部门建立通报信息沟通渠道，请其在宣传教育、加强互联网监控等方面给与协助和支持，阻止不良信息传播，正确引导社会舆论。

### 4.3 预警响应

根据预警信息，各部门和教学管理部门应配合信息技术部加强对本部门、本单位网络与信息系统安全的检测，做好应急处理准备工作。

第五章 应急处置

### 5.1应急响应

5.1.1 I级响应

（1）按教育部《教育系统网络与信息安全类突发公共事件应急预案》I级响应预案执行。学校各有关部门和单位边报告边做好应急响应相关工作。

（2）学校的响应

①应急响应。

在学校党委和行政的统一领导和指挥下，启动学校I级响应、通报相关单位，学校采取措施。

②应急状态。

相关单位指挥机构进入应急状态，在学校党委和行政的统一领导、指挥和协调下，负责学校应急处置工作或支援保障工作，24小时值班。

③跟踪事态发展。

学校及时将事态发展变化情况和处置进展报上级主管部门和教育部网络与信息安全工作组办公室。

④检查影响范围。

信息技术部网络与教育中心会同各信息系统主管部门立即全面了解本部门主管范围内的信息系统是否受到事件的波及或影响，并将有关情况及时上报上级主管部门和教育部网络与信息安全工作组办公室。

⑤及时通报情况。

负责汇总上述有关情况，并根据《教育系统网络与信息安全类突发公共事件应急预案》要求组织上报。

⑥处置实施。

控制事态，防止蔓延，协调小组要负责组织实施，安排组织应急小组采取技术措施，协调国家计算机网络应急处理中心、相关营运商以及公安部的相关技术部门给予支援，以尽快控制事态；组织、督促相关运行单位有针对性地加强防范，防止事件蔓延至其他信息系统。对于信息内容安全事件要督促有关单位及时采取必要的管控措施，有效阻止网上不良信息传播。

做好处置，消除隐患。有关部门和单位要根据事件发生原因，有针对性地采取措施，恢复受破坏信息系统正常运行。

及时开展调查取证。有关部门和单位要督促事发单位在应急恢复过程中尽量保留相关证据，对于人为破坏活动，应上报网络与信息安全工作组，协调有关部门按职责负责组织开展侦查和调查工作。

5.1.2 II级响应

（1）按教育部《教育系统网络与信息安全类突发公共事件应急预案》II级响应预案执行。

（2）学校的响应

①学校指挥机构进入应急状态，按照相关预案做好应急处置工作。

②事发部门在学校协调小组的统一部署下实施技术处置工作。

③学校及时将事态发展变化情况报上级主管部门。

④学校有关部门根据上级的通报，结合学校实际有针对性地加强防范，防止造成更大范围影响和损失。

5.1.3 III、IV级响应

① 在学校党委领导下，启动学校网络与信息安全事件应急预案，保持24小时联络畅通，相关人员24小时值班。

②密切掌握事件发展情况，及时向教育厅汇报。

③处置工作。组织专家组和应急技术支撑队伍到现场了解实际情况，研究解决方案。

检查事件影响范围，有针对性地加强防范，及时恢复受破坏信息系统正常运行，防止事件蔓延。对于信息内容安全事件要及时采取有效措施，防止不良信息传播。

及时开展调查取证。事发单位和部门在应急恢复过程中应尽量保留相关证据，对于人为破坏活动，应报教育厅，协调本地有关部门开展侦查和调查工作。

### 5.2应急处置措施

5.2.1 有害程序事件、网络攻击事件的应急处置

由信息技术部按分工和应急流程处置。对于大规模、影响较大的恶意移动代码、拒绝服务攻击、系统入侵和端口扫描处置：通知应急管理负责人和中心主管，决定上报或通报，按预案通知相关管理员采取措施，或直接实施控制，处置人员记录事件处理步骤和结果，总结报告。

5.2.2 设备实施故障、灾难性事件的应急处置

对火灾、盗窃、破坏等紧急事件按照国家消防有关法律法规、单位有关规定处理。对运行关键部位实施24\*7小时保卫。禁止任何非授权人员进入。

网络运行过程中设备故障，包括线路中断、路由故障、流量异常、域名系统故障等，由信息技术部负责，重大事件立即向中心管理人员报告。

遇供电相关紧急事件，由信息技术部指挥作紧急现场处置，根据停电时间、用电功耗、电池电能储备、供电管理部门信息、网络和信息运行情况等条件作调度，包括次要系统停电减轻负载等措施，密切跟踪参数变化并反馈调整控制，联系相关公司和人员作现场维护。总指挥及时与网络化和信息主管协商，协调处置事件。

### 5.3应急结束

I、II级响应结束按教育部《教育系统网络与信息安全类突发公共事件应急预案》5.3条规定执行。III、IV级应急响应结束。

第六章 后期处置

### 6.1 事件总结

I、II级网络与信息安全事件按教育部《教育系统网络与信息安全类突发公共事件应急预案》6.1条规定执行。III、IV级网络与信息安全事件由学校网络与信息安全工作组自行组织调查处理和总结评估。对事件的起因、性质、影响、责任等进行调查，提出处理意见和改进措施。

### 6.2 表彰和惩处

学校对在网络与信息安全应急工作中表现突出的单位和个人给予表彰；对保障不力、瞒报漏报网络与信息安全事件，给学校、国家和社会造成严重损失的单位和个人依照有关规定进行惩处。

第七章 保障措施

### 7.1 技术支撑队伍

加强学校应急小组建设，做好重大网络与信息安全事件的应急技术支援工作，提高应对突发网络与信息安全事件的能力。

### 7.2 专家队伍

学校要充分发挥网络与信息安全应急处置专家组的作用，为网络与信息安全事件的预防和处置提供技术咨询、技术指导和技术培训。学校加强专家队伍建设，充分发挥专家在科学决策中的作用。

### 7.3 基础平台

学校着力加强网络与信息安全硬件基础平台建设，做到早发现、早预警、早响应，提高应急处置能力。

### 7.4 技术研发

信息技术部应加强网络与信息安全防范技术研究领导工作，为应急响应工作提高技术支撑。

### 7.5 经费保障

信息技术部应支持网络与信息安全应急专业队伍建设、基础平台建设、情报力量建设、技术研发、预案演练等工作的开展。为网络与信息安全类突发公共事件的应急工作提高必要的经费保障。

第八章 宣传和演练

信息技术部应采取有效措施，加强突发网络与信息安全事件预防和处置的有关法律、法规和政策的宣传，开展网络与信息安全基本知识和技能的宣讲活动。

信息技术部应加强网络与信息安全特别是网络与信息安全应急预案的培训，提高防范意识和技能。

信息技术部应组织落实网络与信息安全事件的演练，模拟处置重大网络与信息安全事件，提高实战能力，检验和完成完善预案。

第九章 附则

### 9.1 预案修订

随着相关法律法规的制定、修改和完善，机构调整和应急资源发生变化，本预案将根据实际实施过程中发现的问题和出现的新情况，适时修订本预案。

### 9.2 预案实施

本预案自2018.3.1日起实施。