菏泽医学专科学校
信息系统管理应急预案

（2023 年修订）

目录

菏泽医学专科学校信息系统管理综合预案

一、总则

1.1 目的

完善信息安全应急响应机制，规范信息安全应急响应工作内容和流程，科学应对信息安全突发事件，有效预防、及时控制和最大限度地消除信息安全各类突发事件的危害和影响，保障信息系统的运行安全和数据安全。

1.2 应急响应需求

本单位是政府重要的职能部门，面向社会公众服务，信息具有安全保密的需要，存在发生入侵、篡改、增加、删除等突发事件的可能性，会对社会秩序、公共利益造成严重影响和损害。

1.3 基本原则

1、统一领导，分级负责。按照“谁主管谁负责”的原则，建立和完善责任制度、协调管理机制和联动工作机制。

2、快速反应，积极应对。一旦发生信息系统生产环境和业务系统突发事件，应迅速启动应急处置预案，明确职责，层层落实，采取有力措施积极应对，及时控制处理，防止产生连带风险。

3、加强沟通，有效传递。建立有效的信息传递机制，各部门之间加强共同协作，确保信息畅通；要加强与新闻媒体等外部单位的沟通协调，做好宣传解释工作，全面争取突发事件的内部处置和外部舆论

主动权。

4、保密数据，严格管理。在应急准备和应急预案正式启动期间，各级要做好数据资料的保密工作，明确数据资料保管责任人，资料接触人员要严格保密，决不随意向任何人泄漏，应急期间结束后，统一销毁备用数据资料。

5、严格自律，防范风险。突发事件应急处置期间，各级应急处置机构应加强宣传教育和检查监督，引导员工严格自律，遵守内控制度和业务操作要求，向社会作正面解释、宣传，不得散播影响单位形象和社会稳定的言论，严密防范内、外部潜在风险。

6、准确判断，及时响应。安全事件发生后，及时确定事件分类、级别，启动对应级别的响应措施。

1.4 适用范围

本预案适用于菏泽医学专科学校信息安全事件应急处理工作。

1.5 相关预案

《菏泽医学专科学校机房盗窃专项预案》

《菏泽医学专科学校机房火灾专项预案》

《菏泽医学专科学校机房漏水专项预案》

《菏泽医学专科学校电力故障专项预案》

《菏泽医学专科学校网络攻击应急预案》

《菏泽医学专科学校网络故障应急预案》

《菏泽医学专科学校网站攻击应急预案》

《菏泽医学专科学校网站内容安全事件应急预案》

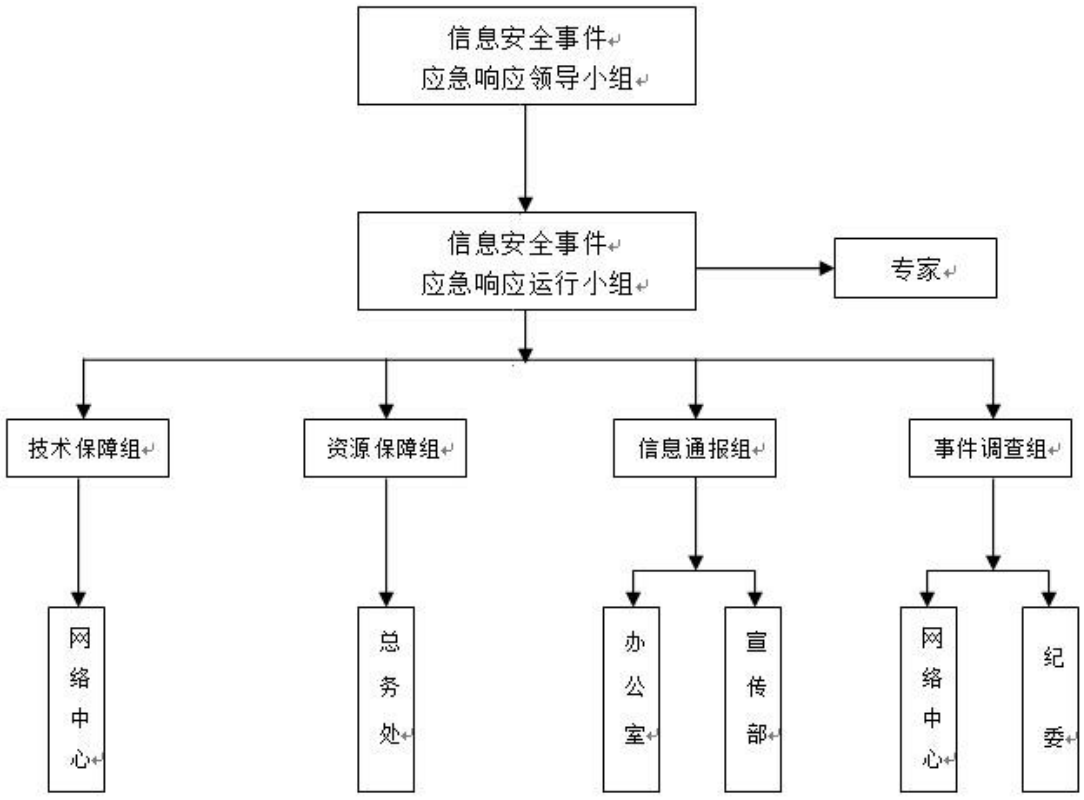
《菏泽医学专科学校关键应用故障应急预案》

《菏泽医学专科学校数据破坏应急预案》

《菏泽医学专科学校数据泄露应急预案》

二、应急处理组织结构与分工

信息安全事件应急救援组织体系由应急响应领导小组、应急响应日常运行小组、应急响应技术保障小组、应急响应资源保障小组、应急响应信息通报小组、应急响应事件调查处理小组，专家组组成。



菏泽医学专科学校信息安全应急救援体系框架图

2.1 信息安全事件应急响应领导小组

信息安全应急领导小组主要由菏泽医学专科学校单位领导、现代教育技术中心部门负责人及各主要成员部门负责人、专家组成员组成。

其主要职能包括:

1) 组织、指导和督促重大安全事件的应急响应工作。

2) 现场指挥重大安全事件应急响应。

3) 审定应急方案。

4) 批准应急方案的启用。

5) 组织协调各部门的应急合作、资源调配等工作。

6) 审定重大安全事件处理和分析报告。

2.2 信息安全事件应急响应日常运行小组

信息安全应急响应日常运行小组主要由信息化领导小组组成。

其主要职能包括:

1) 负责及时向应急领导小组、相关技术支持人员及其他关联系统运行和支持人员通知事件的发生时间、影响范围、应急响应等情况。

2) 组织、协调、督促相关的支持人员及时到场开展应急处理工作;

3) 现场参与和跟踪重大运行事件的应急处理全过程。

4) 通过电话会议等方式，牵头组织相关各部门对重大运行故障进行诊断和恢复，提出启用应急预案建议。

5) 负责对应急预案进行评审，检查应急预案的更新情况和内容有效性。

6) 现场或电话授权值班人员通过短信平台，定时向所有相关人员报告事件内容、目前事件进展和应急响应日常运行小组关于此事件跟踪联系人，以便各方与之联系。

7) 负责应急预案的培训组织。

8）负责制订应急演练方案，组织各相关小组进行应急演练。

2.3 信息安全事件应急响应技术保障小组

主要由技术人员（包括专家组成员、现代教育技术中心技术人员、相关软硬件提供商及集成商技术人员）、业务人员组成。

主要职能包括:

1）编写应急处理方案。

2）设计、实施应急技术方案。

3）组织应急处理方案的测试、更新。

4）应急响应过程中技术问题的解决。

5）组织应急处理方案的演练和培训组织应急处理方案的实施。

6）及时向应急响应日常运行小组报告进展情况。

7）及时资源请求。

2.4 信息安全事件应急响应资源保障小组

资源保障组主要由总务处人员组成。

主要职能包括:

1）对于安全事件发生后，需要的各种物资的准备，包括设备借用、采购，交通工具准备，通讯设备畅通等工作。

2）保障应急物资的正常使用。

2.5 信息安全事件应急响应信息通报组

信息通报组主要由办公室和宣传部组成。

主要职能包括:

1）应急领导小组信息的指令传达，各个应急小组进度汇总、资料整理，对内、外的信息的整理。

2）发布资料的整理及提交审核。

3）外部媒体的沟通及事件影响的控制及消除。

2.6 信息安全事件应急响应事件调查组

事件调查组主要由现代教育技术中心、纪委、专家组等成员组成。主要职能包括:

1）事件发生原因分析，是否存在失职、渎职情况，相关人员考核评价。

2）应急预案的改善、采取措施防止再次发生。

2.7 组织的外部协助

外部组织机构主要包括：公安局、信息系统服务提供商。

三、预防和预警机制

3.1 信息监测及报告

建立信息安全监测机制，单位内信息事件的发现者及发生信息安全事件的部门应立即向应急响应日常运行小组报告。

3.2 预防

积极推行信息安全等级保护制度，基础信息网络和重要信息系统建设要充分考虑抗毁性与灾难恢复。

定期进行信息安全等级保护评测，对于不符合项目制定改善计划；组织信息安全培训，能够使系统相关人员了解等级保护的规定和要求，确保信息系统符合安全等级防护要求。

定期进行相关预案的演练，保证各相关人员清晰掌握应急过程及个人职责。

3.3 预警

应急响应日常运行小组接到信息安全事件报告后，经初步核实后，将有关情况向应急响应领导小组汇报，并进一步进行情况综合，研究分析可能造成损害的程度，提出初步行动对策。应急响应领导小组根据情况召开协调会，决策行动方案，发布指示和命令。

四、应急响应流程

安全事件的应急响应一般包括事件通告、事件分类与定级、应急启动、应急处置、后期处置几个程序。

4.1 事件通告

4.1.1信息通报

信息事件发生后，应将相关信息及时通报给受到负面影响的外部机构、互联的单位系统及重要用户，同时根据应急响应的需要，通知服务提供商，以获得适当的响应支持。

4.1.2信息上报

信息事件发生后，应按照各个级别的应急响应策略，及时上报上级主管部门或监管单位。

4.1.3信息披露

根据事件的严重程度，由信息通报组根据应急领导小组的指示准备相关的信息，确定发布的方式、范围、时间、内容等，并经应急领导小组审批后进行信息的批露。单位其他成员、各应急小组未经允许，不得擅自发布任何消息，共同做好维护稳定工作。

4.2 事件分类与定级

4.2.1概述

信息事件发生后，应急响应日常运行小组应事件进行评估，确定事件的类别和级别。

4.2.2事件的分类

菏泽医学专科学校信息安全事件主要分为以下几类:

1）物理环境事件

主要包括机房设备盗窃事件、机房火灾事件、机房漏水事件、机房电力事件等。

2）网络事件

主要包括网络攻击和网络故障等。

3）应用事件

主要包括网站攻击事件、网站内容安全事件、关键应用故障事件等。

4）数据事件

主要包括数据损害、数据泄露事件。

4.2.3事件的定级

实施预警信息等级制度，按照系统重要程度、系统损失和社会影响，分为四个级别：特别重大事件、重大事件、较大事件和一般事件:

特别重大事件（I级）：本级信息安全事件对信息系统、单位利益以及社会公共利益有灾难性的影响或破坏，在全国范围内产生特别严重的危害或影响。

重大事件（II级）：本级信息安全事件对信息系统、单位利益以

及社会公共利益有巨大的影响或破坏，在全省范围内产生一定的危害或影响。

较大事件（III级）：本级信息安全事件对信息系统、单位利益以及社会公共利益有较大的影响或破坏，在行业内部产生一定的危害或影响。

一般事件（IV级）：本级信息安全事件对信息系统、单位利益以及社会公共利益没有的影响，在省厅范围内产生一定影响。

4.3 应急启动

按照安全事件的可控性、严重程度和影响范围，应急响应级别原则上分为I级响应、II级响应、III级响应和IV级响应。

Ⅰ级响应时，由应急响应领导小组指挥协调，并及时向上级主管/监管单位报告；超出单位处置能力时，应及时向上级信息安全应急组织请求协助；要求各应急小组成员10分钟内赶赴单位。

Ⅱ级响应时，由应急响应领导小组指挥协调；超出单位处置能力时，应及时向上级信息安全应急领导小组报告，请求协助；要求各应急小组成员30分钟内赶赴单位。

III级响应时，由日常运行小组协调组织解决事件，并通知应急响应领导小组，要求相关应急小组成员60分钟内赶赴单位。

IV级响应时，不需要启动应急预案，由现代教育技术中心直接协调解决事件。

4.4 应急处置

4.4.1 概述

由日常运行小组初步确定应急处理方式，确定是否存在针对该事

件的特定系统预案。如有，则启动相关预案；如果事件涉及多个专项预案，应同时启动所有涉及的专项预案。

如果没有针对该事件的专项预案，应根据事件具体情况由应急响应领导小组指挥采取抑制措施，抑制事件进一步扩散，并根除事件影响，恢复系统运行。

如果以自身力量无法处理的事件，应提出应急支援请求，由日常运行小组邀请专家、外部协助组织、上级主管单位派出应急支援技术人员进行信息安全应急支援。

及时采取行动遏制事件发展的同时，限制潜在的损失与破坏，同时要确保对涉及相关业务影响最小。

在应急过程中，资源保障小组要确保应急过程中的物资、通讯、资金、交通工具等及时到位。

4.4.2恢复顺序

系统恢复时首先确保数据的完整性和安全性。

当恢复复杂系统是，恢复进程应按照《业务系统重要度排序表》的优先顺序进行恢复。以避免对相关系统及业务产生重大影响。

4.4.3恢复规程

为了进行恢复操作，针对关键系统应制定详细的业务恢复规程。应急响应技术小组应熟练掌握恢复规程，恢复规程应包括以下行动：

1）获得访问受损设施或区域的授权。

2）通知相关系统的内部和外部业务伙伴。

3）获取所需的硬件环境和网络环境。

4）获得装载备份的介质。

5）恢复关键操作系统和应用软件。

6）恢复系统数据。

7）进行系统测试。

8）测试通过后，通知相关人员开展工作。

4.5 后期处置

4.5.1系统重建

1）在应急处置工作结束后，应由信息办制定重建方案，尽快抢修受损的基础设施、减少损失，尽快恢复正常工作。

2）应急过程如果涉及到涉密数据的使用，在重建过程需遵照涉密要求进行数据的删除。

4.5.2应急响应总结

响应总结是应急处置之后应进行的工作，由事件调查小组负责，具体包括:

1）分析和总结事件发生的原因。

2）分析和总结事件发生的现象。

3）评估系统的损害程度。

4）评估事件导致的损失。

5）分析和总结应急处置过程。

6）评审应急响应措施的效果和效率；并提出改进意见。

7）评审应急响应方案的效果和效率；并提出改进意见。

8）评审应急过程中是否存在失职情况，并给出处理意见。

五、应急保障措施

5.1 概述

应急响应保障措施是应急响应工作的重要组成部分，是保障信息安全事件发生后能够快速有序的实施响应计划的关键因素，需要从人力、资源、技术这三大方面进行保障。

5.2 人力保障

5.2.1 管理人力保障

应急响应领导小组组长应由省厅领导担任，确保应急响应组织机构人员到位，职责清晰，能够完成日常管理工作。

5.2.2 技术人力保障

由日常运行小组应根据应急响应技术需要，定期组织进行技术培训；如本单位特殊情况，无法实现技术的全面掌握，可聘请外部专家或技术供应商，作为技术保障小组成员，定期进行交流、演练。确保各应急技术岗位人员分工清晰，职责明确。

5.3 物质保障

5.3.1 基础物质保障

建立应急响应设备库，包括信息系统的备用设备、应急响应过程所需要的工具。由保障小组进行保管，并确保能够正常使用，由日常运行小组每季度进行定期检查。

5.3.2 应急响应物质保障

1）财力保障

物资保障小组要保证发生应急事件后，资金能及时到位。

2）交通运输保障

在发生安全事件后，单位内所有交通工具应原地待命，全部使用于应急工作，应急响应宣布结束后，方可调配其他工作。

3）通信保障

物资保障小组应保障应急过程中通讯工具及时到位，人员联系畅通。

5.4 技术保障

5.4.1 应急响应技术服务

技术保障由应急响应技术小组负责，技术小组应制定信息安全事件技术应对表，全面考察和管理技术基础，选择合适的技术服务人员，明确职责和沟通方式。

5.4.2 日常技术保障

日常技术保障包括事件监控与预警的技术保障，应急技术储备两部分。

1）事件监控与预警的技术保障

由应急响应技术小组采取监控技术对整个系统进行安全监控，通过及时预警，尽早发现安全事件。

2）应急技术储备

由应急响应技术小组分析应急过程所需有的各项技术，针对各项技术形成培训方案或操作手册。

六、应急演练及维护

6.1 建立定期演练制度

每年应当至少组织一次应急演练，模拟处置影响较大的信息安全事件,发现并解决应急工作体系和工作机制存在的问题，检验物资器材的完好情况，提高应急处理能力。

6.2 预案的修订完善

信息安全应急响应日常运行小组负责应急预案的修订完善。应急响应技术小组和专家组成员应针对应急响应工作中遇到的问题，分析预案的科学性和合理性，及时向信息安全应急响应日常运行小组提出修改建议。在上级预案或相关的法律法规修改后，本预案应进行调整与其保持一致。

2023 年 6 月 26 日

菏泽医学专科学校

菏泽医学专科学校机房盗窃事件应急预案

一、总则

1.1 目的

为加强机房设备安全工作，确保单位迅速有效地处理盗窃事件，将事故对数据、设备和环境造成的损失降到最小程度，最大限度的保障信息系统的安全。

1.2 适用范围

本规范适用于菏泽医学专科学校数据中心机房盗窃事件应急处理工作。

1.3 相关预案

《菏泽医学专科学校信息系统管理综合预案》

二、应急处理组织结构与分工

2.1 常设组织机构

具体组织架构及职责参照《菏泽医学专科学校信息系统管理综合预案》的应急处理组织结构与分工部分。

2.2 应急响应防盗小组

1) 负责现场环境的保护。

2) 负责协调公安机关进行取证。

3) 负责取证后的机房保护，避免二次被盗。

4) 负责跟进公安机关的调查进度跟进。

2.3 组织的外部协助

外部组织机构主要为公安机关。

三、预防和预警机制

3.1 信息监测及报告

使用机房安全防盗报警监控系统进行实时监控。发生报警后，收到报警信息的人员应立即向应急响应日常运行小组报告。

3.2 预防

建设机房防盗报警系统，并定期检查报警系统的可用性。加强单位人员、车辆进出管理，降低被盗风险。

3.3 预警

应急响应日常运行小组接到防盗报警后，应通知防盗应急响应小组赶赴现场，查看现场情况。初步核实是否发生人员入侵情况；如果为误报，则通知应急响应日常运行小组，解除警报。如发生了入侵事件，则应将有关情况向应急响应日常运行小组汇报。应急响应日常运行小组根据事情的情况，汇总后上报应急响应领导小组。

四、应急响应流程

4.1 事件通告

4.1.1 信息通报

被盗事件发生后，由信息通报小组通知受影响的业务部门，并制定统一的解释原因，向咨询方进行解释。

4.1.2信息上报

被盗事件发生后，根据事件等级，由应急响应领导小组决策是否

向上级主管或监管单位上报。

4.1.3信息披露

根据事件的严重程度，由信息通报组根据应急领导小组的指示准备相关的信息，确定发布的方式、范围、时间、内容等，并经应急领导小组审批后进行信息的批露。单位其他成员、各应急小组未经允许，不得擅自发布任何消息，共同做好维护稳定工作。

4.2 事件定级

实施预警信息等级制度，按照系统重要程度、系统损失和社会影响，分为三个级别：特别重大事件、重大事件和一般事件:

特别重大事件（I级）：机房设备被盗数量超过5台，或存储设备被盗，综合损失超过10万。

重大事件(II级):机房设备被盗数量小于5台,综合损失介于2-10万。

一般事件（IV级）：机房设备被盗1台，未对系统产生不良影响，综合损失小于2万。

4.3 应急启动

按照安全事件的可控性、严重程度和影响范围，应急响应级别原则上分为I级响应、II级响应、和III级响应。

I 级响应时，由单位应急响应领导小组指挥协调，并及时向上级主管/监管单位报告；超出单位处置能力时，应及时向上级信息安全应急组织请求协助位；必要时由上级应急组织指挥应急响应；要求各应急小组成员20分钟内赶赴单位。

II 级响应时，由单位应急响应领导小组指挥协调；超出24小时系

统未恢复正常运行，应及时向上级信息安全应急领导小组报告，请求协助；要求各应急小组成员40分钟内赶赴单位。

III级响应时，由现代教育技术中心协调组织解决事件，并通知应急响应日常运行小组；要求现代教育技术中心成员90分钟内赶赴单位。

4.4 应急处置

4.4.1 应急处置

4.4.1.1 一级响应

1）应急响应领导小组指挥，及时向上级主管/监管单位报告。

2）应急响应防盗小组及时联系公安机关。

3）应急响应防盗小组维持现场状况，禁止无关人员进出，减少对现场的破坏。

4）应急响应防盗小组协助公安机关取证。

5）技术小组尽快设计恢复方案，并邀请专家进行审核。

6）技术小组根据库存情况，列清应急所需物资清单。

7）由领导小组审批同意后，物资保障小组进行采购，技术小组进行实施。

8）宣传小组组织对外发布材料，经领导小组审批后，根据情况适时发布。

9）机房安全加固未完成前，由应急响应防盗小组进行不间断保护。

10）超出单位处置能力时，应及时向上级信息安全应急组织请求协助；

4.4.1.2 二级响应

1）应急响应领导小组指挥。

2）应急响应防盗小组及时联系公安机关。

3）应急响应防盗小组维持现场状况，禁止无关人员进出，减少对现场的破坏。

4）应急响应防盗小组协助公安机关取证。

5）技术小组尽快设计恢复方案。

6）技术小组根据库存情况，列清应急所需物资清单。

7）由领导小组审批同意后，物资保障小组进行采购，技术小组进行实施。

8）宣传小组组织对外发布材料，经领导小组审批后，根据情况适时发布。

9）机房安全加固未完成前，由应急响应防盗小组进行不间断保护。

4.4.1.3 三级响应

1）现代教育技术中心及时联系公安机关。

2）现代教育技术中心维持现场状况，禁止无关人员进出，减少对现场的破坏；协助公安机关取证。

3）机房安全加固未完成前，由现代教育技术中心进行不间断保护。

4.4.2恢复顺序

系统恢复时首先确保数据的完整性和安全性。

当恢复复杂系统时，恢复进程应按照《业务系统重要度排序表》的优先顺序进行恢复。以避免对相关系统及业务产生重大影响。

4.5 后期处置

具体处置措施按照综合预案的后期处置进行。

2023 年 6 月 26 日

菏泽医学专科学校

菏泽医学专科学校机房火灾事件应急预案

一、总则

1.1 目的

为加强机房重点防火部位重要危险源的消防安全工作，确保单位迅速有效地处理火灾事故，将事故对数据、设备和环境造成的损失降到最小程度，最大限度的保障信息系统的安全。

1.2 适用范围

本规范适用于菏泽医学专科学校数据中心机房火灾事件的应急处理。

1.3 相关预案

《菏泽医学专科学校信息系统管理综合预案》

二、应急处理组织结构与分工

2.1 常设组织机构

具体组织架构及职责参照《菏泽医学专科学校信息系统管理综合预案》的应急处理组织结构与分工部分。

2.2 应急响应消防小组

1) 负责机房火灾的应急响应处置。

2) 事件发生后，机房内消防设备的开启。

3) 负责消防通道的日常检查及事件发生后消防车到达现场通道的畅通。

4）负责维护事故现场秩序，防止无关人员接近事故现场。

5）事故发生后，采取抑制措施，避免火灾进一步扩大。

6）负责日常消防安全检查；负责组织日常消防演练。

7）负责安全消防知识宣传。

2.3 组织的外部协助

外部组织机构主要包括：菏泽市消防支队、菏泽市急救中心

三、预防和预警机制

3.1 信息监测及报告

使用机房消防报警监控系统进行实时监控。发生报警后，收到报警信息的人员应立即向应急响应日常运行小组报告。

3.2 预防

1）定期对气体灭火系统、消防栓、灭火器等进行检查、更换，避免消防器材过期；保障消防通道畅通，保障应急照明灯可用。

2）定期对机房电路进行检查，及时更换，防止线路老化引起火灾。

3）机房严禁放置易燃易爆物品。

4）保持机房内适当的湿度。

5）严禁携带易燃品进入机房。

6）组织相关人员进行消防安全培训，学习消防知识，学会正确使用灭火器材，有计划的进行相关应急演练。

3.3 预警

应急响应日常运行小组接到火灾报警后，应通知应急响应消防小

组赶赴现场，查看现场情况。初步核实是否发火灾情况；如果为误报，则通知应急响应日常运行小组，解除警报。如发生了火灾，则应将有关情况向应急响应日常运行小组汇报，最大限度实施遏制措施。应急响应日常运行小组根据事情的情况，汇总后上报应急响应领导小组。

四、应急响应流程

4.1 事件通告

4.1.1 信息通报

机房火灾发生后，由信息通报小组通知受影响的业务部门，并制定统一的解释原因，向咨询方进行解释。

4.1.2 信息上报

机房火灾事件发生后，根据事件等级，由应急响应领导小组决策是否向上级主管或监管单上报。

4.1.3 信息披露

根据事件的严重程度，由信息通报组根据应急领导小组的指示准备相关的信息，确定发布的方式、范围、时间、内容等，并经应急领导小组审批后进行信息的批露。单位其他成员、各应急小组未经允许，不得擅自发布任何消息，共同做好维护稳定工作。

4.2 事件定级

实施预警信息等级制度，按照系统重要程度、系统损失和社会影响，分为两个级别:重大事件和一般事件。

重大事件（I 级）：机房内部出现大面积燃烧，机房内消防设施无

法开启或开启后火势不能得到有效控制；发生人员严重烧伤或死亡情况。

一般事件（II 级）：机房有出现冒烟或零星火苗，机房内消防设施开启后火势得到有效控制；机房边缘区域纸质易燃物燃烧，使用消防器材可以进行控制。

4.3 应急启动

按照安全事件的可控性、严重程度和影响范围，应急响应级别原则上分为 I 级响应、II 级响应。

I 级响应时，由单位应急响应领导小组亲自组织救援，各部门全力做好救援工作，要求各小组在 10 分钟内到达现场开展救援。超出单位处置能力时，立即拨打 119，事态无法控制必要时单位应及时请求地方政府协调。

II 级响应时，由日常运行小组协调；应急响应消防小组组织灭火，降低火灾损失；若 5 分钟内扑灭火源，10 分钟内确认不会再次出现复燃情况，可考虑终止应急影响；超出 10 分钟未解决时或火势有恶化趋势，应及时向应急响应领导小组报告，请求协助。

4.4 应急处置

应急处置　机房火灾处置应遵循以下原则:首先保证人员安全，其次保证关键设备安全，再保证一般设备安全。

4.4.1.1 一级响应

1）应急响应领导小组指挥，确定是否向上级主管/监管单位报告。

2）应急响应消防小组及时拨打 119，汇报火势情况，请求消防队尽

快支援。

3）技术保障小组负责尽快按照合理顺序远程关闭设备。

4）应急响应消防小组确定若是由电器原因导致的火灾，应第一时间切断区域供电。

5）应急响应消防小组负责保证消防车辆进入通道畅通，引导消防员到达消防栓所在位置;

4.4.1.2 二级响应

1）现代教育技术中心及时开启机房内消防设备;

2）若由电路原因发生火灾，则现代教育技术中心应及时切断区域供电电源。

3）现代教育技术中心联系应急响应消防小组，携带消防器材到达现场，在火势不受控情况下，准备进一步扑救；电源未切断前，严禁用水扑救。

4）5 分钟内火势仍然扩大趋势，则升级为一级响应，并拨打 119，联系消防队支援。

4.4.2 恢复顺序

系统恢复时首先确保数据的完整性和安全性。

当恢复复杂系统是，恢复进程应按照《业务系统重要度排序表》的优先顺序进行恢复，以避免对相关系统及业务产生重大影响。

4.5 后期处置

具体处置措施按照综合预案的后期处置进行。

2023 年 6 月 26 日

菏泽医学专科学校

菏泽医学专科学校机房漏水应急预案

一、总则

1.1 目的

为加强机房机房漏水应急管理，确保单位迅速有效地处理漏水事件，将事件对数据、设备和环境造成的损失降到最小程度，最大限度的保障信息系统的安全。

1.2 适用范围

本规范适用于菏泽医学专科学校数据中心机房漏水事件应急处理工作。

1.3 相关预案

《菏泽医学专科学校信息系统管理综合预案》

二、应急处理组织结构与分工

2.1 常设组织结构

具体组织架构及职责参照《菏泽医学专科学校信息系统管理综合预案》的应急处理组织结构与分工部分。

2.2 应急响应防水小组

1) 定期检查机房空调设备专用水源的密封性能,发现有泄露处应及时修理。
2) 定期检查机房屋面有无渗水漏水的情况。
3) 定期检查防水雨水从窗子、门缝渗入。

4）防止空调设备冷凝水漏在机房里。

5）采用现代化漏水检测系统,一旦发生漏水,及时报警,及时处理避免酿成水害。

2.3 组织的外部协调

外部组织机构主要包括：空调维保单位。

三、预防和预警机制

3.1 信息监测及报告

使用机房安全防漏水报警监控系统进行实时监控。发生报警后，收到报警信息的人员应立即向应急响应日常运行小组报告。

3.2 预防

1）针对空调可能发生的漏水:

安装动力环境监控设备、砌防水墙、制作防水盘，采用双层水管保护、一台空调一路供水管道等方法，同时注意降低进入机房供水管道的压强和有效控制水源。

2）针对屋顶、墙壁、门窗等可能发生的凝露、渗漏:

所有进入机房的水管做保温处理，防止由于温差形成的凝露；屋顶、墙壁进行防水处理，增加过渡区域。

3）上层建筑、附近办公室的暖气、水管等进行定期检查，定期更换。

4）上层建筑、附件办公室的暖气、水管的总开关应有明确标识。

3.3 预警

应急响应日常运行小组接到防水报警后，应通知防水应急响应小组赶赴现场，查看现场情况。初步核实是否发生漏水、积水情况；如果为误报，则通知应急响应日常运行小组，解除警报。如发生了漏水、积水事件，则应将有关情况向应急响应日常运行小组汇报。应急响应日常运行小组根据事情的情况，汇总后上报应急响应领导小组。

四、应急响应流程

4.1 事件的通告

4.1.1 信息通报

机房漏水、积水事件发生后，由信息通报小组通知受影响的业务部门，并制定统一的解释原因，向咨询方进行解释。

4.1.2 信息上报

机房漏水、积水事件发生后，根据事件等级，由应急响应领导小组决策是否向上级主管或监管单位上报。

4.1.3 信息披露

根据事件的严重程度，由信息通报组根据应急领导小组的指示准备相关的信息，确定发布的方式、范围、时间、内容等，并经应急领导小组审批后进行信息的批露。单位其他成员、各应急小组未经允许，不得擅自发布任何消息，共同做好维护稳定工作。

4.2 事件定级

实施预警信息等级制度，按照系统重要程度、系统损失和社会影响，分为二个级别：重大事件和一般事件。

重大事件（I 级）：机房产生积水或预计 10 分钟内积水;

一般事件（II 级）：空调排水管（槽）轻微渗漏，机柜、墙壁水珠凝结等情况，机房发生漏水或预计 30 分钟内不会产生积水。

4.3 应急启动

按照漏水事件的可控性、严重程度和影响范围，应急响应级别原则上分为 I 级响应、II 级响应。

I 级响应时，由单位应急响应日常运行小组协调，防水小组实施救援，要求防水小组成员 20 分钟内到达现场。

II 级响应时，由现代教育技术中心协调组织解决事件，并通知应急响应日常运行小组；要求现代教育技术中心成员 90 分钟内赶赴单位。

4.4 应急处置

4.4.1应急处置

4.4.1.1 一级响应

1）日常运行小组协调防水小组查找漏水原因，若为空调漏水，则关闭空调；若为管道漏水，则关闭漏水点阀门。

2）现代教育技术中心人员应尽快关闭关键设备的电源，然后关闭机房电闸，包括 UPS 电源。

3）确保机房内电源全部切断后，防水小组进入机房使用抽水设备进行排水。

4）确保不再漏水后，现代教育技术中心人员进行系统的恢复。

5）若为管道漏水，防水小组则进行维修；若为空调故障，由现代教育技术中心联系空调维保厂商进行维修，确保不再漏水。

4.4.1.2 二级响应

1）日常运行小组协调防水小组查找漏水原因，若为空调漏水，则关闭空调；若为管道漏水，则关闭漏水点阀门。

2）开启空调除湿功能，使用干布擦出水珠。

3）若为管道漏水，防水小组则进行维修；若为空调故障，由现代教育技术中心联系空调维保厂商进行维修，确保不再漏水。

4.4.2恢复顺序

系统恢复时首先确保数据的完整性和安全性。

当恢复复杂系统时，恢复进程应按照《业务系统重要度排序表》的优先顺序进行恢复。以避免对相关系统及业务产生重大影响。

4.5 后期处置

具体处置措施按照综合预案的后期处置进行。

2023 年 6 月 26 日

菏泽医学专科学校

菏泽医学专科学校机房电力故障应急预案

一、总则

1.1 目的

为保障信息系统稳定运行，切实做好机房供电系统的保障工作，科学、有效、快速的处理机房内的应急供电设备、消防电气设备、应急照明等设备所遇到的突发事件，最大限度的减少停电造成的影响和损失，根据我单位的有关要求，结合本部门的职责范围制定本预案。

1.2 适用范围

本规范适用于菏泽医学专科学校数据中心机房电力故障事件应急处理工作。

1.3 相关预案

《菏泽医学专科学校信息系统管理综合预案》

二、应急处理组织结构与分工

2.1 常设组织结构

具体组织架构及职责参照《菏泽医学专科学校信息系统管理综合预案》的应急处理组织结构与分工部分。

2.2 应急响应电力小组

1）机房电路及供电的设计优化。

2）电力故障的原因查找及解决。

3）应急方案的设计、审核及修订。

2.3 组织的外部协调

外部组织机构主要包括：菏泽供电公司。

三、预防和预警机制

3.1 信息监测及报告

使用机房断电报警监控系统，日常运行维护人员实时监控。发生报警后，收到报警信息的人员应立即向应急响应日常运行小组报告。

3.2 预防

1）定期检查电路线缆、插排、开关等，发生老化情况后及时更换，避免线路故障。

2）定期进行 UPS 检查，确保 UPS 主机正常运行，电池续航能力持续。

3.3 预警

应急响应日常运行小组接到电力故障报警后，应通知电力应急响应小组赶赴现场，查看现场情况。初步核实是否发生断电、短路等电力故障；如果为误报，则通知应急响应日常运行小组，解除警报。如发生了断电、短路等事件，则应将有关情况向应急响应日常运行小组汇报。应急响应日常运行小组根据事情的情况，汇总后上报应急响应领导小组。

四、应急响应流程

4.1 事件通告

4.1.1 信息通报

机房断电、短路等电力故障事件发生后，由信息通报小组通知受影响的业务部门，并制定统一的解释原因，向咨询方进行解释。

4.1.2 信息上报

机房断电、短路等电力故障事件发生后，根据事件等级，由应急响应领导小组决策是否向上级主管或监管单位上报。

4.1.3 信息披露

根据事件的严重程度，由信息通报组根据应急领导小组的指示准备相关的信息，确定发布的方式、范围、时间、内容等，并经应急领导小组审批后进行信息的批露。单位其他成员、各应急小组未经允许，不得擅自发布任何消息，共同做好维护稳定工作。

4.2 事件定级

实施预警信息等级制度，按照系统重要程度、系统损失和社会影响，分为三个级别：特别重大事件、重大事件和一般事件:

特别重大事件（I 级）：机房核心、关键业务系统包含的主要设备所在机柜出现断电、短路情况，造成工作日上班时间关键业务无法开展且预计 8 小时内无法恢复运转；因电力故障造成人员重伤或死亡；因电力故障发生严重火灾。

重大事件（II级）：机房核心、关键业务系统包含的一般设备所在机柜出现断电、短路情况，造成核心、关键业务的部分流程、功能造成影响且预计24小时内无法恢复运转，但不影响整体业务开展；因电力故障造成人员受轻微伤；因电力故障发生小型火灾。

一般事件（IV级）：机房出现断电情况但时间较短，关键业务系统未受到影响，或预计电力恢复供应时间不超过1小时。

4.3 应急启动

按照安全事件的可控性、严重程度和影响范围，应急响应级别原则上分为I级响应、II级响应、和III级响应。

Ⅰ级响应时，由单位应急响应领导小组亲自组织救援，各部门全力做好救援工作，要求各小组在30分钟内到达现场展开救援。若发生火灾，则同时启动机房火灾应急响应。

Ⅱ级响应时，由日常运行小组协调应急响应电力小组实施救援。根据事态的发展，当故障超出本单位处理能力的应及时寻求外部支持。事件破坏性进一步升级时，应考虑升级为Ⅰ级响应。

III级响应时，由现代教育技术中心协调组织解决事件，并通知应急响应日常运行小组、业务电工；要求现代教育技术中心成员90分钟内赶赴单位。

4.4 应急处置

4.4.1应急处置

4.4.1.1 一级响应

1）应急响应领导小组指挥，及时向上级主管/监管单位报告。

2）若有人员伤亡，则及时拨打120进行人员抢救。

3）若发生火灾，则必须在保障人员生命安全的情况下优先保护存储数据的设备，其次是关键应用的设备，然后是其他设备，尽量减少财产损失。

3）应急响应电力小组进行故障的排查。UPS故障，则联系维保厂家，

并切换到旁路供电状态；单位线路线缆故障，则现场进行更换维修。外部供电故障，则联系供电公司进行故障解决。

4）外部供电故障，且2小时内无法修复，则应联系相关单位、公司，借用或租用柴油发电机进行内部供电。

5）宣传小组组织对外发布材料，经领导小组审批后，是否进行发布或适时发布。

4.4.1.2 二级响应

1）日常运行小组指挥，协调应急响应电力小组进行故障的排查；UPS故障，则联系维保厂家，并切换到旁路供电状态；单位线路线缆故障，则现场进行更换维修；外部供电故障，则联系供电公司进行故障解决。

2)若有人员受轻微伤,则由物资保障小组安排车辆送往就近医院。

4.4.1.3 三级响应

现代教育技术中心协调指挥。UPS故障，则联系维保厂家，并切换到旁路供电状态；单位线路线缆故障，联系应急响应电力小组则现场进行更换维修；外部供电故障，则联系供电公司进行故障解决。

4.4.2恢复顺序

系统恢复时首先确保数据的完整性和安全性。

当恢复复杂系统时，恢复进程应按照《业务系统重要度排序表》的优先顺序进行恢复，以避免对相关系统及业务产生重大影响。

4.5 后期处置

具体处置措施按照综合预案的后期处置进行。

2023 年 6 月 26 日

菏泽医学专科学校网络攻击应急预案

一、总则

1.1 目的

为提高应对网络安全能力，维护网络安全和社会稳定，保障本单位各项工作的顺利开展，避免和减少网络问题带来办公效率低下，信息泄露，经济、财产受损等情况的特制定本预案。

1.2 适用范围

本规范适用于菏泽医学专科学校现代教育技术中心内部网络及外部网络受到攻击后应急处理工作。

1.3 相关预案

《菏泽医学专科学校信息系统管理综合预案》

二、应急处理组织结构与分工

2.1 常设组织机构

具体组织架构及职责参照《菏泽医学专科学校信息系统管理综合预案》的应急处理组织结构与分工部分。

2.2 组织的外部协助

外部组织机构主要包括：菏泽联通公司、菏泽市公安局（公共信息网络监察处）、网络安全服务机构

三、预防和预警机制

3.1 信息监测及报告

使用机房网络在线监控系统进行实时监控。发生报警后，收到报警信息的人员应立即向应急响应日常运行小组报告。

3.2 预防

建设网络状态监控平台，设置网络攻击声音、邮件报警，日常运行小组每日对关键业务系统包含的网络设备、安全设备巡检，定期分析设备运行日志，及早发现设备可能出现的隐患。

3.3 预警

应急响应日常运行小组接到网络攻击报警后，应通知网络攻击应急响应小组赶赴现场，查看现场情况。初步核实是否发生网络攻击；如果为误报，则通知应急响应日常运行小组，解除警报。如发生了网络攻击事件，则应将有关情况向应急响应日常运行小组汇报。应急响应日常运行小组根据事情的情况，汇总后上报应急响应领导小组。

四、应急响应流程

4.1 事件通告

4.1.1 信息通报

网络攻击发生后，由信息通报小组通知受影响的业务部门，并制定统一的解释原因，向咨询方进行解释。

4.1.2信息上报

网络攻击事件发生后，根据事件等级，由应急响应领导小组决策

是否向上级主管或监管单位上报。

4.1.3信息披露

根据事件的严重程度，由信息通报组根据应急领导小组的指示准备相关的信息，确定发布的方式、范围、时间、内容等，并经应急领导小组审批后进行信息的批露。单位其他成员、各应急小组未经允许，不得擅自发布任何消息，共同做好维护稳定工作。

4.2 事件定级

实施预警信息等级制度，按照系统重要程度、系统损失和社会影响，分为三个级别：特别重大事件、重大事件和一般事件:

特别重大事件（I级）：核心、关键业务系统使用的主干网络、设备因遭受网络攻击出现宕机、异常，导致业务中断且2小时内无法恢运转；关键业务系统包含的主要设备遭受入侵。

重大事件（II级）：核心、关键业务系统使用的主干网络、关键设备运转异常，业务系统整体运行缓慢，但因遭受攻击造成的设备负荷、网络带宽使用率低于理论极限的60%；关键业务系统包含的一般设备或非关键业务系统包含的主要设备存在被入侵迹象。

一般事件（IV级）：网络攻击对一般业务系统造成轻微影响或无影响，安全设备成功拦截攻击行为。

4.3 应急启动

按照安全事件的可控性、严重程度和影响范围，应急响应级别原则上分为I级响应、II级响应、和III级响应。

I 级响应时，由单位应急响应领导小组指挥协调，并及时向上级主管/监管单位报告；超出单位处置能力时，应及时向上级信息安全应

急组织请求协助位；必要时由上级应急组织指挥应急响应；要求各应急小组成员20分钟内赶赴单位。

II级响应时，由单位应急响应领导小组指挥协调；超出8小时未解决时，应及时向上级信息安全应急领导小组报告，请求协助；要求各应急小组成员40分钟内赶赴单位。

III级响应时，由现代教育技术中心协调组织解决事件，并通知应急响应日常运行小组;要求现代教育技术中心成员90分钟内赶赴单位。

4.4 应急处置

4.4.1 应急处置

4.4.1.1 一级响应

1）应急响应领导小组指挥，及时向上级主管/监管单位报告。

2）技术小组搜集、分析相关日志、数据，进行分析进一步定位确认网络攻击类型、起源；联系公安部门进行报警。

3）技术小组，联系安全厂商应急支援，同时做好配合工作。必要时请求公安机关网络监察部门支援。

4）技术小组尽快设计恢复、安全加固方案，邀请专家进行审核。

5）技术小组根据库存情况，列清应急所需物资清单。

6）由领导小组审批同意后，物资保障小组进行采购，技术小组进行实施。

7）宣传小组组织对外发布材料，经领导小组审批后，根据情况适时发布。

8）网络攻击解决前，由技术小组提供临时代替措施。

9）超出单位处置能力时，应及时向上级信息安全应急组织请求协助。

4.4.1.2 二级响应

1）应急响应日常运行小组指挥。

2）应急响应技术小组搜集、分析相关日志、数据，进行分析进一步定位确认网络攻击类型、起源；联系公安机关报警。

4）技术小组尽快设计恢复、安全加固方案。

5）技术小组根据库存情况，列清应急所需物资清单。

6）由领导小组审批同意后，物资保障小组进行采购，技术小组进行实施。

7）宣传小组组织对外发布材料，经领导小组审批后，根据情况适时发布。

8）机房网络攻击解决前，由应急响应技术小组提供临时代替措施。

4.4.1.3 三级响应

1）现代教育技术中心进行网络攻击类型分析。

2）检查相关设备是否存在安全漏洞。

3）及时升级软、硬件、带宽资源以防范更高级别的攻击行为。

4.4.2恢复顺序

系统恢复时首先确保数据的完整性和安全性。

当恢复复杂系统时，恢复进程应按照《业务系统重要度排序表》

的优先顺序进行恢复。以避免对相关系统及业务产生重大影响。

4.5 后期处置

具体处置措施按照综合预案的后期处置进行。

2023 年 6 月 26 日

菏泽医学专科学校

菏泽医学专科学校网络故障应急预案

一、总则

1.1 目的

为提高应对网络故障应对能力，维护单位网络稳定运行，保障本单位各项工作的顺利开展，避免和减少网络故障对业务开展、正常工作秩序的影响，特制定本预案。

1.2 适用范围

本规范适用于菏泽医学专科学校数据中心机房网络故障应急处理工作。

1.3 相关预案

《菏泽医学专科学校信息系统管理综合预案》

二、应急处理组织结构与分工

2.1 常设组织机构

具体组织架构及职责参照《菏泽医学专科学校信息系统管理综合预案》的应急处理组织结构与分工部分。

2.2 组织的外部协助

外部组织机构主要包括：菏泽联通、网络设备提供商。

三、预防和预警机制

3.1 信息监测及报告

使用机房网络在线监控系统进行实时监控。发生报警后，收到报警信息的人员应立即向应急响应日常运行小组报告。

3.2 预防

建设网络状态监控平台，设置网络故障声音、邮件报警，日常运行小组每日对关键业务系统包含的网络设备、安全设备巡检，定期分析设备运行日志，及早发现设备可能出现的隐患。

3.3 预警

应急响应日常运行小组接到网络故障报警后，应通知技术小组赶赴现场，查看现场情况。初步核实是否发生网络故障情况；如果为误报，则通知应急响应日常运行小组，解除警报。如发生了网络故障事件，则应将有关情况向应急响应日常运行小组汇报。应急响应日常运行小组根据事情的情况，汇总后上报应急响应领导小组。

四、应急响应流程

4.1 事件通告

4.1.1 信息通报

网络故障发生后，由信息通报小组通知受影响的业务部门，并制定统一的解释原因，向咨询方进行解释。

4.1.2信息上报

网络故障事件发生后，根据事件等级，由应急响应领导小组决策

是否向上级主管或监管单位上报。

4.1.3信息披露

根据事件的严重程度，由信息通报组根据应急领导小组的指示准备相关的信息，确定发布的方式、范围、时间、内容等，并经应急领导小组审批后进行信息的批露。单位其他成员、各应急小组未经允许，不得擅自发布任何消息，共同做好维护稳定工作。

4.2 事件定级

实施预警信息等级制度，按照系统重要程度、系统损失和社会影响，分为两个级别：重大事件和一般事件:

重大事件（I级）：核心、关键业务系统使用的主干网络故障但故障原因明确30分钟内网络通信可恢复正常。

一般事件（II级）：核心、关键业务系统中非关键设备中断，断网影响人群不超过正常比例的10%；非核心、非关键业务系统的主要设备、线路故障导致网络正常运行受到影响。

4.3 应急启动

按照安全事件的可控性、严重程度和影响范围，应急响应级别原则上分为I级响应和II级响应。

I 级响应时，由日常运行小组指挥协调；由技术小组要求20分钟内到达现场。

II 级响应时，由现代教育技术中心协调组织解决事件，要求现代教育技术中心成员40分钟内赶赴单位。

4.4 应急处置

4.4.1 应急处置

4.4.1.1 一级响应

1）由日常运行小组指挥。

2）技术小组确定为单位外部线路故障及时通知相应的ISP服务人员进行抢修，同时做好配合工作；若为内部故障，则及时采取措施，尽快恢复。

3）技术小组根据库存情况，列清应急所需物资清单。

4）由领导小组审批同意后，物资保障小组进行采购，技术小组进行实施。

4.4.1.2 二级响应

1）现代教育技术中心进行故障分析和排除。

2）现代教育技术中心设计恢复办法。

3）现代教育技术中心提供临时解决办法。

4.4.2恢复顺序

系统恢复时首先确保数据的完整性和安全性。

当恢复复杂系统时，恢复进程应按照《业务系统重要度排序表》的优先顺序进行恢复。以避免对相关系统及业务产生重大影响。

4.5 后期处置

具体处置措施按照综合预案的后期处置进行。

2023 年 6 月 26 日

菏泽医学专科学校

菏泽医学专科学校网站攻击应急预案

一、总则

1.1 目的

为完善网站安全应急响应机制，规范网站安全应急响应工作内容和流程，科学应对网站安全突发事件，保障重要网站系统的实体安全、运行安全和数据安全，减少网站攻击对我单位正常工作和业务开展带来的破坏，避免对单位形象和社会秩序造成不良影响，特制定本预案。

1.2 适用范围

本规范适用于菏泽医学专科学校网站攻击，或页面内容未被恶意篡改的应急处理工作。

1.3 相关预案

《菏泽医学专科学校信息系统管理综合预案》

二、应急处理组织结构与分工

2.1 常设组织机构

具体组织架构及职责参照《菏泽医学专科学校信息系统管理综合预案》的应急处理组织结构与分工部分。

2.2 组织的外部协助

外部组织机构主要包括：菏泽市公安局（公共信息网络监察处）、网络安全服务机构。

三、预防和预警机制

3.1 信息监测及报告

使用网站安全监控平台进行实时监控。发生报警后，收到报警信息的人员应立即向应急响应日常运行小组报告。

3.2 预防

1) 定期进行渗透测试，根据测试结果进行安全加固。

2) 定期进行风险评估，针对风险因素进行风险降低。

3) 定期进行漏洞扫描，根据扫描结果进行漏洞防护。

4) 定期进行系统升级及补丁更新。

3.3 预警

应急响应日常运行小组接到网络攻击报警后，应通知技术小组查看安全监测平台报警情况。初步核实是否发生网站攻击；如果为误报，则通知应急响应日常运行小组，解除警报。如发生了网站攻击事件，则应将有关情况向应急响应日常运行小组汇报。应急响应日常运行小组根据事情的情况，汇总后上报应急响应领导小组。

四、应急响应流程

4.1 事件通告

4.1.1 信息通报

网站攻击发生后，由信息通报小组通知受影响的业务部门，并制定统一的解释原因，向咨询方进行解释。

4.1.2信息上报

网络攻击事件发生后，根据事件等级，由应急响应领导小组决策是否向上级主管或监管单位上报。

4.1.3信息披露

根据事件的严重程度，由信息通报组根据应急领导小组的指示准备相关的信息，确定发布的方式、范围、时间、内容等，并经应急领导小组审批后进行信息的批露。单位其他成员、各应急小组未经允许，不得擅自发布任何消息，共同做好维护稳定工作。

4.2 事件定级

实施预警信息等级制度，按照系统重要程度、系统损失和社会影响，分为两个级别：重大事件和一般事件。

重大事件（I 级）：重业务系统网站、门户网站等核心网站，遭受流量攻击，超出防火墙防御范围，网站无法访问或访问较慢；网站被挂马、操作系统出现提权事件;网站遭受篡改，但未出现法律禁止的黄、赌、毒、反动信息等；网站数据库泄露导致相关数据被非法利用；网站服务器被发现存在木马、病毒、后门程序。

一般事件（II 级）：网络攻击对一般业务系统造成轻微影响或无影响，安全设备成功拦截攻击行为；网站服务器存在大量异常访问，如密码试探、弱端口扫描、未成功的 SQL 注入行为等。

4.3 应急启动

按照安全事件的可控性、严重程度和影响范围，应急响应级别原则上分为 I 级响应和 II 级响应。

I 级响应时，由单位应急响应领导小组指挥协调，并及时向上级

主管/监管单位报告；超出单位处置能力时，应及时向上级信息安全应急组织请求协助位；必要时由上级应急组织指挥应急响应；要求各应急小组成员 20 分钟内赶赴单位。

II 级响应时，由现代教育技术中心协调组织解决事件，并通知应急响应日常运行小组;要求现代教育技术中心成员 90 分钟内赶赴单位。

4.4 应急处置

4.4.1 应急处置

4.4.1.1 一级响应

1）应急响应领导小组指挥，及时向上级主管/监管单位报告。

2）技术小组搜集、分析相关日志、数据，进行分析进一步定位、确认攻击类型、起源；设置防火墙策略、流量清洗、使用 cdn 节点分流等措施降低流量攻击影响;删除恶意代码，还原数据保障网站快速恢复。

3)技术小组及时报警，配合公安机关进行攻击源的定位。

4）技术小组联系安全厂商应急支援，同时做好配合工作。

5）技术小组尽快设计恢复、安全加固方案，邀请专家进行审核。

6）技术小组根据库存情况，列清应急所需物资清单。

7）由领导小组审批同意后，物资保障小组进行采购，技术小组进行实施。

8）宣传小组组织对外发布材料，经领导小组审批后，根据情况适时发布。

9）机房网络攻击解决前，由应急响应网络攻击小组提供临时代替

措施。

4.4.1.2 二级响应

1）应急响应领导小组指挥。

2）应急响应网站攻击小组搜集、分析相关日志、数据，进行分析进一步定位、确认攻击类型、起源；设置防火墙策略、流量清洗、使用 cdn 节点分流等措施降低流量攻击影响;删除恶意代码，还原数据保障网站快速恢复。

3）网站攻击应急小组尽快设计恢复、安全加固方案。

4）网站攻击应急小组根据库存情况，列清应急所需物资清单。

5）由领导小组审批同意后，物资保障小组进行采购，技术小组进行实施。

6）宣传小组组织对外发布材料，经领导小组审批后，根据情况适时发布。

8）网站攻击解决前，由应急响应网站攻击小组提供临时应对办法。

4.4.1.3 三级响应

1)现代教育技术中心安排日常运行小组进行网络攻击类型分析。

2）检查相关设备是否存在安全漏洞。

3）及时升级操作系统、网站程序，修复漏洞；更换安全级别更高的登录口令。

4.4.2恢复顺序

系统恢复时首先确保数据的完整性和安全性。

当恢复复杂系统时，恢复进程应按照《业务系统重要度排序表》的优先顺序进行恢复。以避免对相关系统及业务产生重大影响。

4.5 后期处置

具体处置措施按照综合预案的后期处置进行。

2023 年 6 月 26 日

菏泽医学专科学校

菏泽医学专科学校网站内容安全应急预案

一、总则

1.1 目的

为保障网站发布内容真实、有效，符合国家法律、法规的要求，明确突发网站内容安全事件时处理顺序，特制订本预案。

1.2 适用范围

本规范适用于菏泽医学专科学校网站内容发生恶意篡改事件应急处理工作。

1.3 相关预案

《菏泽医学专科学校信息系统管理综合预案》

二、应急处理组织结构与分工

2.1 常设组织机构

具体组织架构及职责参照《菏泽医学专科学校信息系统管理综合预案》的应急处理组织结构与分工部分。

2.2 组织的外部协助

外部组织机构主要包括：省公安厅

三、预防和预警机制

3.1 信息监测及报告

建立网站安全监测系统，对于敏感字、网页篡改进行实时监控。发

生报警后，收到报警信息的人员应立即向应急响应日常运行小组报告。

3.2 预防

1）定期进行渗透测试，根据测试结果进行安全加固。

2）定期进行风险评估，针对风险因素进行风险降低。

3）定期进行漏洞扫描，根据扫描结果进行漏洞防护。

4）定期进行系统升级及补丁更新。

5）使用网站防篡改技术，对于防止网页被恶意篡改。

6）建立实时监控系统，对于敏感字、网页篡改进行实时监控。

3.3 预警

应急响应日常运行小组接到应用故障报警后，应通知应用故障应急响应小组登录网站及网站程序管理平台，查看情况。初步核实是否发生恶意篡改事件；如果为误报，则通知应急响应日常运行小组，解除警报。如发现了恶意内容，则应将有关情况向应急响应日常运行小组汇报。应急响应日常运行小组根据事情的情况，汇总后上报应急响应领导小组。

四、应急响应流程

4.1 事件通告

4.1.1 信息通报

网站内容安全事件发生后，由信息通报小组通知受影响的业务部门，并制定统一的解释原因，向咨询方进行解释。

4.1.2信息上报

网站内容安全事件发生后，根据事件等级，由应急响应领导小组决策是否向上级主管或监管单位上报。

4.1.3信息披露

根据事件的严重程度，由信息通报组根据应急领导小组的指示准备相关的信息，确定发布的方式、范围、时间、内容等，并经应急领导小组审批后进行信息的批露。单位其他成员、各应急小组未经允许，不得擅自发布任何消息，共同做好维护稳定工作。

4.2 事件定级

实施预警信息等级制度，按照系统重要程度、系统损失和社会影响，分为两个级别：特别重大事件、重大事件。

特别重大事件（I 级）：网站出现国家法律明令禁止的违法信息，如涉及黄、赌、毒信息，反政府信息等；涉及国家秘密的信息；当地政府要求不能对外发布的信息；单位机密信息泄露；对单位、社会造成恶劣形象的信息；内容安全事件发生超过 1 小时，已经在社会产生了不良影响。

重大事件（II 级）：网站出现国家法律明令禁止的违法信息，如涉及黄、赌、毒信息，反政府信息等；当地政府要求不能对外发布的信息；单位机密信息泄露；对单位、社会造成恶劣形象的信息；内容安全事件发生未超过 1 小时，未在社会上产生不良影响。

4.3 应急启动

按照安全事件的可控性、严重程度和影响范围，应急响应级别原则上分为 I 级响应和 II 级响应。

Ⅰ级响应时，由单位应急响应领导小组指挥协调，及时向上级主管/监管单位报告，同时要求应急响应网站内容发布小组立即处理相关信息；超出单位处置能力时，应及时向上级信息安全应急组织请求协助位；必要时由上级应急组织指挥应急响应；要求技术小组成员 5 分钟内登录网站平台处理。

Ⅱ级响应时，由单位应急响应领导小组指挥协调；超出 2 小时未解决时，应及时向上级信息安全应急领导小组报告，请求协助；要求技术小组成员 10 分钟内登录网站平台处理。

4.4 应急处置

4.4.1 应急处置

4.4.1.1 一级响应

1）应急响应领导小组指挥，及时向上级主管/监管单位报告。

2）应急响应技术小组立即停止原服务器网站服务，使用备用服务器提供网站服务或停止服务。

3）应急响技术小组使用物理隔离方法保护被入侵服务器不受再次破坏，搜集、分析相关日志、数据，确定内容发布来源，锁定发布人；并通知公安机构协助追查。

4）技术小组尽快设计加固方案，并邀请专家进行审核。

5）技术小组根据库存情况，列清应急所需物资清单。

6）由领导小组审批同意后，物资保障小组进行采购，技术小组进行实施。

7）宣传小组组织对外发布材料，经领导小组审批后，根据情况

适时发布。

8）备用网站服务期间，由技术时刻进行监控，避免二次攻击。

9）超出单位处置能力时，应及时向上级或外界信息安全应急组织请求协助。

4.4.1.2 二级响应

1）应急响应日常运行指挥，将事件通知领导小组。

2）应急响应技术小组立即停止原服务器网站服务，使用备用服务器提供网站服务或停止服务。

3）应急响技术小组使用物理隔离方法保护被入侵服务器不受再次破坏，搜集、分析相关日志、数据，确定内容发布来源，锁定发布人；并通知公安机构协助追查。

4）技术小组尽快设计加固方案，并邀请专家进行审核。

5）技术小组根据库存情况，列清应急所需物资清单。

6）由领导小组审批同意后，物资保障小组进行采购，技术小组进行实施;

7）宣传小组组织对外发布材料，经领导小组审批后，根据情况选择不发布或适时发布;

8）备用网站服务期间，由技术时刻进行监控，避免二次攻击。

9）超出单位处置能力时，应及时向上级或外界信息安全应急组织请求协助。

4.4.2恢复顺序

网站内容恢复时首先确保数据的完整性和安全性。

当恢复复杂网站系统时，恢复进程应按照《业务系统重要度排序表》的优先顺序进行恢复。以避免对相关系统及业务产生重大影响。

4.5 后期处置

具体处置措施按照综合预案的后期处置进行。

2023 年 6 月 26 日

菏泽医学专科学校

菏泽医学专科学校关键应用故障应急预案

一、总则

1.1 目的

为科学分析本单位业务系统可能存在的风险隐患，制定相应的应急措施，避免突发事件时出现职责不明、反应不快、应急准备不足情况，及时有效的应对关键应用故障，特制定本预案。

1.2 适用范围

本规范适用于菏泽医学专科学校数据中心机房关键应用故障应急处理工作。

1.3 相关预案

《菏泽医学专科学校信息系统管理综合预案》

二、应急处理组织结构与分工

2.1 常设组织机构

具体组织架构及职责参照《菏泽医学专科学校信息系统管理综合预案》的应急处理组织结构与分工部分。

2.2 组织的外部协助

外部组织机构主要包括：应用服务开发单位。

三、预防和预警机制

3.1 信息监测及报告

故障信息获取主要通过应用监控系统进行实时监控、日常运行小组人工报告等。发生报警后，收到报警信息的人员应立即向应急响应日常运行小组报告。

3.2 预防

建立应用监控平台，现代教育技术中心对关键业务系统包含的设备进行巡检，定期分析设备运行日志，及早发现设备、程序、数据库可能出现的隐患。

3.3 预警

应急响应日常运行小组接到应用故障报警后，应通知应用技术保障小组登陆程序管理平台，查看情况。初步核实是否发生应用故障情况；如果为误报，则通知应急响应日常运行小组，解除警报。如发生了应用故障事件，则应将有关情况向应急响应日常运行小组汇报。应急响应日常运行小组根据事情的情况，汇总后上报应急响应领导小组。

四、应急响应流程

4.1 事件通告

4.1.1 信息通报

关键应用故障发生后，由信息通报小组通知受影响的业务部门，并制定统一的解释原因，向咨询方进行解释。

4.1.2信息上报

关键应用故障事件发生后，根据事件等级，由应急响应领导小组决策是否向上级主管或监管单位上报。

4.1.3信息披露

根据事件的严重程度，由信息通报组根据应急领导小组的指示准备相关的信息，确定发布的方式、范围、时间、内容等，并经应急领导小组审批后进行信息的批露。单位其他成员、各应急小组未经允许，不得擅自发布任何消息，共同做好维护稳定工作。

4.2 事件定级

实施预警信息等级制度，按照系统重要程度、系统损失和社会影响，分为三个级别：特别重大事件、重大事件和一般事件:

特别重大事件（I级）：承载关键应用的设备、连接数据库出现异常情况（如设备损坏、程序逻辑错误、数据库丢失或损坏等），导致应用无法使用且2小时内无法恢复；影响范围为所有使用者。

重大事件（II级）：承载关键应用的设备、连接数据库出现短暂异常、不稳定情况（如设备资源短时间内使用率较高导致应用系统响应速度较慢）。

一般事件（IV级）：一般性的程序错误、报警信息。

4.3 应急启动

按照安全事件的可控性、严重程度和影响范围，应急响应级别原则上分为I级响应、II级响应、和III级响应。

Ⅰ级响应时，由单位应急响应领导小组指挥协调，及时向上级主管/监管单位报告，同时联系程序研发单位进行故障恢复；超出单位处置能力时，应及时向上级信息安全应急组织请求协助位；必要时由上级应急组织指挥应急响应；要求各应急小组成员20分钟内赶赴单位。

Ⅱ级响应时，由单位应急响应领导小组指挥协调；超出8小时未解

决时，应及时向上级信息安全应急领导小组报告，请求协助；要求各应急小组成员40分钟内赶赴单位。

III级响应时，由现代教育技术中心协调组织解决事件，并通知应急响应日常运行小组；要求现代教育技术中心成员90分钟内赶赴单位。

4.4 应急处置

4.4.1 应急处置

4.4.1.1 一级响应

1）应急响应领导小组指挥，及时向上级主管/监管单位报告。

2）应急响应应用故障小组确定为程序本身故障或程序所处设备故障，应立即联系产品研发单位，同时做好配合工作。

3）应急响应应用故障小组搜集、分析相关日志、数据，进行分析进一步定位确认故障原因。

4）技术小组尽快设计恢复方案，并邀请专家进行审核。

5）技术小组根据库存情况，列清应急所需物资清单。

6）由领导小组审批同意后，物资保障小组进行采购，技术小组进行实施。

7）宣传小组组织对外发布材料，经领导小组审批后，根据情况适时发布。

8）应用程序故障解决前，由应急响应应用故障小组提供临时代替措施。

9）超出单位处置能力时，应及时向上级信息安全应急组织请求协助。

4.4.1.2 二级响应

1）应急响应领导小组指挥。

2）应急响应应用故障小组确定为程序本身故障或程序所处设备故障，应立即联系产品研发单位，同时做好配合工作。

3）应急响应应用故障小组搜集、分析相关日志、数据，进行分析进一步定位确认故障原因。

4）技术小组尽快设计恢复方案。

5）技术小组根据库存情况，列清应急所需物资清单。

6）由领导小组审批同意后，物资保障小组进行采购，技术小组进行实施。

7）宣传小组组织对外发布材料，经领导小组审批后，根据情况适时发布。

8）机房网络故障解决前，由应急响应网络故障小组提供临时代替措施。

4.4.1.3 三级响应

1）现代教育技术中心安排日常运行小组进行故障分析和排除。

2）现代教育技术中心搜集相关错误信息提交研发单位分析，确定是否需要对程序进行升级。

3）现代教育技术中心提供临时解决办法。

4.4.2恢复顺序

系统恢复时首先确保数据的完整性和安全性。

当恢复复杂系统时，恢复进程应按照《业务系统重要度排序表》的优先顺序进行恢复。以避免对相关系统及业务产生重大影响。

4.5 后期处置

具体处置措施按照综合预案的后期处置进行。

2023 年 6 月 26 日

菏泽医学专科学校

菏泽医学专科学校数据破坏事件应急预案

一、总则

1.1 目的

为加强机房数据安全工作，确保单位迅速有效地处理数据破坏事件，将事故对数据、设备造成的损失降到最小程度，最大限度的保障信息系统的稳定运行。

1.2 适用范围

本规范适用于菏泽医学专科学校信数据破坏事件应急处理工作。

1.3 相关预案

《菏泽医学专科学校信息系统管理综合预案》

二、应急处理组织结构与分工

2.1 常设组织机构

具体组织架构及职责参照《菏泽医学专科学校信息系统管理综合预案》的应急处理组织结构与分工部分。

2.2 组织的外部协助

外部组织机构主要包括：数据恢复单位（需要签订保密协议）

三、预防和预警机制

3.1 信息监测及报告

使用数据监控平台进行实时信息监控。发生报警后，收到报警信息

的人员应立即向应急响应日常运行小组报告。

3.2 预防

依据数据重要程度采取多样性备份措施，如实时备份、每日备份，异地备份等。

定期对备份的数据进行有效性验证。

3.3 预警

应急响应日常运行小组接到数据破坏报警后，应通知技术小组赶赴现场，查看数据受损情况。初步核实是否发生数据破坏情况；如果为误报，则通知应急响应日常运行小组，解除警报。如发生了数据破坏事件，则应将有关情况向应急响应日常运行小组汇报。应急响应日常运行小组根据事情的情况，汇总后上报应急响应领导小组。

四、应急响应流程

4.1 事件通告

4.1.1 信息通报

数据破坏事件发生后，由信息通报小组通知受影响的业务部门，并制定统一的解释原因，向咨询方进行解释。

4.1.2信息上报

数据破坏事件发生后，根据事件等级，由应急响应领导小组决策是否向上级主管或监管单位上报。

4.1.3信息披露

根据事件的严重程度，由信息通报组根据应急领导小组的指示准

备相关的信息，确定发布的方式、范围、时间、内容等，并经应急领导小组审批后进行信息的批露。单位其他成员、各应急小组未经允许，不得擅自发布任何消息，共同做好维护稳定工作。

4.2 事件定级

实施预警信息等级制度，按照系统重要程度、系统损失和社会影响，分为两个级别：特别重大事件和一般事件。

特别重大事件（I级）：关键数据丢失，且备份数据无法恢复。

一般事件（II级）：数据遭受破坏，通过备份数据恢复，使系统可以正常运行。

4.3 应急启动

按照安全事件的可控性、严重程度和影响范围，应急响应级别原则上分为I级响应、II级响应。

I 级响应时，由单位应急响应领导小组指挥协调，并及时向上级主管/监管单位报告；超出单位处置能力时，应及时向上级信息安全应急组织请求协助位；必要时由上级应急组织指挥应急响应；要求技术保障小组成员20分钟内赶赴单位。

II 级响应时，由现代教育技术中心协调组织解决事件，并通知应急响应日常运行小组；要求现代教育技术中心成员60分钟内赶赴单位。

4.4 应急处置

4.4.1 应急处置

4.4.1.1 一级响应

1）应急响应领导小组指挥，及时向上级主管/监管单位报告。

2）应急响应技术小组立刻停止业务系统，避免数据继续写入。

3）应急响应技术小组使用数据恢复软件对数据进行恢复。

4）技术小组自身无法恢复数据，则联系外部组织进行技术支持。

5）数据恢复后，应记录数据经手人，避免以后产生数据外泄情况发生。

4.4.1.2 二级响应

1）现代教育技术中心负责协调指挥。

2）应急响应技术小组立刻停止业务系统，避免数据继续写入。

3）应急响应技术小组使用备份数据进行数据的恢复，启动业务系统，进行有效性测试。

4）测试正常后，通知业务部门开始使用系统。

4.4.2恢复顺序

系统恢复时首先确保数据的完整性和安全性。

当恢复复杂系统时，恢复进程应按照《业务系统重要度排序表》的优先顺序进行恢复。以避免对相关系统及业务产生重大影响。

4.5 后期处置

具体处置措施按照综合预案的后期处置进行。

2023 年 6 月 26 日

菏泽医学专科学校

菏泽医学专科学校数据泄露事件应急预案

一、总则

1.1 目的

为加强数据安全，提高单位相关人员应对突发数据泄露能力，降低数据在存储、传输、处理过程中泄露的风险，加强相关人员安全意识，明确汇报对象和处置流程，特制订本预案。

1.2 适用范围

本规范适用于菏泽医学专科学校信数据泄露事件应急处理工作。

1.3 相关预案

《菏泽医学专科学校信息系统管理综合预案》

二、应急处理组织结构与分工

2.1 常设组织机构

具体组织架构及职责参照《菏泽医学专科学校信息系统管理综合预案》的应急处理组织结构与分工部分。

2.2 组织的外部协助

外部组织机构主要包括：省公安厅、信息安全服务机构

三、预防和预警机制

3.1 信息监测及报告

应急响应技术小组通过在线监控系统检测网络中是否存在敏感信

息关键字，配合审计系统用户行为分析确定是否存在泄密事件。若存在泄密事件，应及时汇报给应急领导小组。

3.2 预防

建设数据防泄密系统，在关键区域部署审计系统，涉密信息按照涉密网要求建立独立专网，重要数据进行数据加密和访问身份鉴别，涉密设备控制信息输出，加强敏感介质废弃销毁管理，同时加强人员安全意识教育。

3.3 预警

数据泄露应急小组接到泄密报警信息后，应对泄密发生部门、个人做初步调查。初步核实是否发泄密情况；如果为误报，则解除警报。如泄密事件，则应将有关情况上报应急响应领导小组。

四、应急响应流程

4.1 事件通告

4.1.1 信息通报

数据泄露事件发生后，由信息通报小组通知受影响的业务部门，并制定统一的解释原因，向咨询方进行解释。

4.1.2信息上报

数据泄露事件发生后，根据事件等级，由应急响应领导小组决策是否向上级主管或监管单位上报。

4.1.3信息披露

根据数据泄露的严重程度，由信息通报组根据应急领导小组的指

示准备相关的信息，确定发布的方式、范围、时间、内容等，并经应急领导小组审批后进行信息的批露。单位其他成员、各应急小组未经允许，不得擅自发布任何消息，共同做好维护稳定工作。

4.2 事件定级

实施预警信息等级制度，按照系统重要程度、系统损失和社会影响，分为三个级别：特别重大事件、重大事件和一般事件:

特别重大事件（I级）：泄露数据属于国家绝密、机密、秘密内容;泄露数据属于单位关键、核心内容，对单位关键业务造成重大影响;产生连锁反应，将对上、下级单位造成重大影响。

重大事件（II级）：泄露数据属于单位重要内容，对单位一般业务造成重大影响，不会对外部单位造成影响。

一般事件（IV级）：单位一般性内部数据泄露，不会对正常业务开展造成影响。

4.3 应急启动

按照安全事件的可控性、严重程度和影响范围，应急响应级别原则上分为I级响应、II级响应、和III级响应。

Ⅰ级响应时，由单位应急响应领导小组指挥协调，并及时向上级主管/监管单位报告；超出单位处置能力时，应及时向上级信息安全应急组织请求协助位；必要时由上级应急组织指挥应急响应；要求各应急小组成员30分钟内进行到达现场。

Ⅱ级响应时，由单位应急响应领导小组指挥协调；超出24小时未解决时，应及时向上级信息安全应急领导小组报告，请求协助；要求各应急小组成员60分钟内进行响应。

III级响应时，由现代教育技术中心协调组织解决事件，并通知应急响应日常运行小组；要求现代教育技术中心成员90分内赶赴现场，开展调查。

4.4 应急处置

4.4.1 应急处置

4.4.1.1 一级响应

1）应急响应领导小组指挥，及时向上级主管/监管单位报告。

2）日常运行小组经应急领导小组对事态进行评估授权后，及时联系公安局报警。

3）技术小组防收集审计记录、维持现场状况，禁止无关人员进出，减少对现场的破坏。

4）技术小组协助公安机关取证。

5）技术小组尽快设方案，减少数据泄露带来的影响，并邀请专家进行审核。

6）泄露信息调查取证完成前，由技术小组对现场进行不间断保护。

4.4.1.2 二级响应

1）日常运行小组指挥。

2）日常运行小组对事态进行评估授权后，上报应急领导小组审批是否联系公安局报警。

3）技术小组防收集审计记录、维持现场状况，禁止无关人员进出，减少对现场的破坏。

4）数据泄露应急小组协助公安机关取证。

5）技术小组尽快设方案，减少数据泄露带来的影响。

6）泄露信息调查取证完成前，由技术小组对现场进行不间断保护。

4.4.1.3 三级响应

1）现代教育技术中心对整体泄露事件进行评估。

2）现代教育技术中心收集审计记录、维持现场状况，禁止无关人员进出，减少对现场的破坏。

3）现代教育技术中心查找泄密途径和人员。

4）泄露信息调查取证完成前，由现代教育技术中心对现场进行不间断保护。

4.4.2恢复顺序

系统恢复时首先确保数据的完整性和安全性。

当恢复复杂系统时，恢复进程应按照《业务系统重要度排序表》的优先顺序进行恢复。以避免对相关系统及业务产生重大影响。

4.5 后期处置

具体处置措施按照综合预案的后期处置进行。

2023 年 6 月 26 日

菏泽医学专科学校

附件

附件一 各小组联系人清单

应急处理组织联系人清单								
小组名称	组成部门	姓名	所在部门	职位	工作职责	联络方式		
						手机	办公电话	紧急联系人及电话
领导小组		顾润国	校领导	组长	负责应急预案的审批及应急过程中重大事件的决策。	18905302219	0530-5633111	18905302219
		蒋继国	校领导	副组长	组长不在岗情况下，负责组长职责，协助组长开展应急工作。	15552088932	0530-5925769	15552088932
		齐云飞	校领导	成员	负责应急协调工作。	15552088660	0530-5260876	15552088660
		高军	校领导	成员	负责应急协调工作。	13869912698	0530-5260877	13869912698
		李铮	校领导	成员	负责应急协调工作。	18963052777	0530-5630881	18963052777
		代爱英	校领导	成员	负责应急协调工作。	15552088932	0530-5925931	15552088932
日常运		蒋方剑	现代教育技	组长	负责应急响应的日常管理工	13869712505	0530-5630160	13869712505

行小组			术中心		作；负责组织预案的修订；负责组织应急演练。			
		周岩	现代教育技术中心	副组长	组长不在岗情况下，负责组长职责，协助组长开展应急工作，组织应急培训。	13605309306	0530-5925709	13605309306
		董鹏	现代教育技术中心	成员	负责接收应急事件，负责检查应急设备。	13563851666	0530-5925820	13563851666
		杜健持	现代教育技术中心	成员	负责接收应急事件，负责检查应急设备。	15666662013	0530-5925709	15666662013
技术保障小组		蒋方剑	现代教育技术中心	组长	负责应急响应的技术问题解决；负责应急预案的技术流程制定。	13869712505	0530-5630160	13869712505
		周岩	现代教育技术中心	副组长	组长不在岗情况下，负责组长职责，协助组长开展应急工作。	13605309306	0530-5925709	13605309306
		董鹏	现代教育技术中心	成员	负责数据库技术问题解决，负责服务器虚拟化技术问题解决。	13563851666	0530-5925709	13563851666
		杜健持	现代教育技术中心	成员	负责网络技术问题解决，包含网络技术问题与安全设备技术问题。	15666662013	0530-5925709	15666662013
火灾事件应急小组		马振山	综治办	组长	负责机房火灾事件应急预案的流程设计；负责机房日常消防检查；负责机房火灾事件的协调处理；负责组织消防培训和日常演练。	15990950111	0530-5632110	15990950111

		周登杰	综治办	副组长	组长不在岗情况下，负责组长职责，协助组长开展应急工作。	13518600070	0530-5632110	13518600070
		周岩	现代教育技术中心	成员	负责机房火灾事件的初步扑灭、抑制。	13605309306	0530-5925709	13605309306
漏水事件应急小组		张风刚	水电暖保障管理中心	组长	负责机房漏水事件应急预案的流程设计；负责机房日常漏水点检查；负责机房漏水事件的协调处理；负责组织日常漏水事件演练。	13561327966	0530-5631061	13561327966
		王 龙		副组长	组长不在岗情况下，负责组长职责，协助组长开展应急工作。	17805300877	0530-5631061	17805300877
盗窃事件应急小组		马振山	综治办	组长	负责机房盗窃事件应急预案的流程设计；负责机房日常安全防盗检查；负责机房盗窃事件的协调处理。	15990950111	0530-5632110	15990950111
		周登杰		副组长	组长不在岗情况下，负责组长职责，协助组长开展应急工作。	13518600070	0530-5632110	13518600070
		周岩	现代教育技术中心	成员	负责盗窃事件的现场维护。	13605309306	0530-5925709	13605309306
电力故障事件小组		张风刚	水电暖保障管理中心	组长	负责机房电力故障事件应急预案的流程设计；负责机房日常安全用电检查；负责机房电力故障事件的协调处理；负责组织电力故障事件演练。	13561327966	0530-5631061	13561327966
		王 龙		副组长	组长不在岗情况下，负责组长职责，协助组长开展应急工作。	17805300877	0530-5631061	17805300877

附件二 应急物资清单

应急物资清单				
序号	物品名称	存放位置	负责人	备注
1	灭火器	现代教育技术中心机房	周岩	
2	消防栓	走廊	周登杰	
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

附件三 应急事件处理报告单

应急事件处理报告单	
应急事件类型：	
发生事件的时间： 年 月 日 时 分	
发现事件的时间： 年 月 日 时 分	
事件发现人：	事件发现地点：
报告编制人：	联系电话：
事件发现过程描述： 事件处理过程描述：	
启动的应急响应级别： □一级 □二级 □三级 □四级	
事件原因：	
受影响的资产： □信息/数据 □硬件 □软件 □通信设施 □文档	
影响范围和严重程度：	

已经采取的措施：
计划采取的措施：
日常运行小组意见：
专家意见：
应急响应领导小组意见：