杨凌职业技术学院文件

杨职院发〔2023〕243号

杨凌职业技术学院关于
印发《网络信息安全事件应急预案》的通知

各学院（部）、处室：

《杨凌职业技术学院网络信息安全事件应急预案》已经2023年12月15日院务会审定通过，现予以印发，请遵照执行。

杨凌职业技术学院

2023年12月26日

杨凌职业技术学院
网络信息安全事件应急预案

为规范学校网络信息安全事件应急响应工作机制，有效预防并科学应对网络信息安全突发事件，确保校园网络与信息系统正常运行，根据《中华人民共和国计算机信息系统安全保护条例》《教育系统网络与信息安全类突发公共事件应急预案》《信息技术安全事件报告与处理流程》《信息安全事件分类分级指南》（GB/T20986-2023）和中省有关法律法规，结合学校实际，特制定本预案。

第一章 总则

第一条 校园网络信息安全事件是指校园信息化基础设施、应用系统、网站、信息化数据等因各种因素遭到破坏，对学校工作、学习、生活秩序造成负面影响的事件。

第二条 应急处置遵循“统一领导、归口负责、预防为本、快速反应、科学处置”的原则，最大可能的降低危害和影响。

第三条 加强网络与信息系安全管理，健全工作制度和建立预报预警监测体系，避免和减少网络信息安全事件发生。

第二章 组织机构及职责

第四条 学校成立网络安全和信息化领导小组，在网络信息安全事件应急方面，其主要职责是:

（一）统筹全校网络与信息安全工作，组织协调处置网络与信息安全工作中出现的各种突发事件，研究解决突发事件中的重大问题;

（二）组织制定学校网络与信息安全应急预案及其修订、完善工作，对突发事件相关信息进行及时收集、分析和研判，有效处置网络与信息安全工作;

（三）及时收集、通报和上报网络信息安全事件处置的有关情况;

（四）对全校各单位贯彻执行预案以及在事件处置工作中履行职责情况进行检查督办。

第五条 党委（校长）办公室负责重大敏感时期、重要活动、重要会议期间发生的信息安全事件的协调处置;负责涉密级信息网络泄密类事件的处理。

第六条 信息化建设与管理处负责校园基础网络系统安全，确保校园网络服务不中断;负责网络攻击、设备故障类事件的处置;负责全校网络信息安全事件处置的技术支持工作。

第七条 党委宣传部负责学校舆情监测和信息内容安全类事件的处置，加强对师生政治思想方面的倾向性、苗头性问题的预警分析研判，妥善有效应对措施。

第八条 保卫处负责涉及人为破坏类事件的处置，联系公安部门，配合重大安全事件的处置。

第九条 各单位负责本单位网站和业务系统信息安全事件的处置工作，应对照本预案建立相应机制。

第三章 网络信息安全事件分级

第十条 网络信息安全事件依据发生过程、性质和特征不同，可分为以下四类:

（一）网络攻击事件: 由于遭受有害程序感染、非法入侵或

其他技术手段攻击，造成校园网络和信息系统运行异常或存在潜在危险，或造成信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。

（二）设备故障事件：由于信息系统或外围软硬件设施故障、人为误操作等，造成信息系统破坏、业务中断、系统宕机、网络瘫痪等导致的信息安全事件。

（三）灾害性事件：因洪水、火灾、雷击、地震、台风、非正常停电等外力因素造成网络与信息系统损毁，导致业务中断、系统宕机、网络瘫痪等安全事件。

（四）信息内容安全事件：利用校园网络在校内外传播法律法规禁止的信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

第十一条 网络信息安全事件按照可控性、严重程度和影响范围不同，可划分为四级：

（一）Ⅰ级（特别重大）：事件导致发生全校性大规模瘫痪，或由于网站非法信息引发学校大规模群体性事件，对学校正常工作造成特别严重损害，事态发展超出学校控制能力。

（二）Ⅱ级（重大）：事件导致校园网发生全校性瘫痪，或由于网站非法信息引发师生反应强烈并有过激行为，对学校正常工作造成严重损害，事态发展超出学校网络安全和信息化领导小组控制能力，需要跨部门协同处置。

（三）Ⅲ级（较大）：事件导致校园网某一区域的重要网络与信息应用系统瘫痪，或由于网站敏感信息、谣言等，对学校正常工作造成一定损害。

（四）IV级（一般）：事件导致某一局部网络或信息应用系统受到一定程度损坏，学校工作受到一定影响，但不危害学校整体工作。

第四章 预防措施

第十二条 健全技术防护体系，在校园网出入口、数据中心、重要信息系统等重要部位，安装必要的安全防御检测工具，进行实时监测和定期扫描，发现异常情况及时防范处理并逐级报告。同时做好操作系统升级杀毒，数据备份、安全审计等日常管理工作。

第十三条 网络安全关键保障时期，遵守安全操作规范，加强用户权限管理，调整限制访问权限，关闭不必要的网上服务等。

第十四条 各单位应随时监控网站内容，做好校园网络与信息安全的日常巡查及日志保存工作，严格执行值班制度，以保证最先发现灾害并及时处置突发性事件。

第五章 处置程序

第十五条 启动预案：发生网络信息安全事件后，信息化建设与管理处和涉事部门应第一时间采取断网等有效措施，将损害和影响降低到最小范围，保留现场，并报告相关负责人。

第十六条 事件定级：信息化建设与管理处及时做好网络信息安全事件定级，收集事件相关信息，确定事件来源，弄清事件范围，鉴别事件性质，评估事件影响和危害。

第十七条 应急响应：根据事件等级采取相应的响应方式，涉及人为主观破坏事件时由保卫处报告当地公安部门：

I 级：信息化建设与管理处（领导小组办公室，下同）立即

上报领导小组组长，由学校报告上级教育主管部门和当地公安部门，公安部门指挥协调有关单位和学校协同进行应急处置。

II 至 III 级：信息化建设与管理处应立即上报领导小组组长，由组长或常务副组长指挥、协调成员单位进行应急处置。

IV 级：信息化建设与管理处组织相关单位及时、自主进行应急处置，做好处置记录。

第十八条 应急处理方式：根据网络与信息安全事件类型采取不同应急处置方式：

（一）网络攻击事件：判断攻击来源与性质，关闭影响安全的网络设备和服务器设备，断开信息系统与攻击来源的网络物理连接，跟踪并锁定攻击来源的 IP 地址或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照事件发生的性质采取以下方案：

病毒传播：及时寻找并断开传播源，判断病毒的类型、性质、可能的危害范围，必要时可关闭相应端口，甚至相应楼层的网络，及时请有关技术人员协助进行杀毒处理。

外部入侵：判断入侵来源，评价入侵危害。对威胁较小的入侵，定位入侵 IP 地址，及时关闭入侵端口，限制 IP 地址访问。对于已造成危害的，应立即采用断开网络连接的方法，避免造成更大损失和影响。

内部入侵：查清入侵来源，如 IP 地址、所在位置等信息，同时断开对应的交换机端口。对于无法制止的多点入侵和造成损害的，应及时关闭被入侵的服务器或相应设备。

（二）设备故障事件：判断故障发生点和故障原因，及时抢

修故障设备，优先保证校园网主干网络和主要应用系统的运转。

（三）灾害性事件：在突发重大灾害性事件时，在保障人身安全的前提下，保障数据安全和设备安全，妥善做好硬盘的保存以及设备断电、拆卸与搬迁等。

（四）信息内容安全事件：出现信息内容安全事件后，应迅速屏蔽该网站网络端口或拔掉网络连接线，阻止有害信息传播，查找信息发布人并做好善后处理。对公安机关要求协查的外网不良信息事件，积极做好相关配合工作。

（五）其它不确定安全事件：根据中省网络信息安全相关要求，结合具体情况，做出相应处理，不能处理的及时咨询国家有关信息安全机构。

第十九条 后续处理：

（一）安全事件应急处置后，应及时采取措施，抑制其影响进一步扩大，限制潜在的损失与破坏，同时要确保应急处置措施对涉及的相关业务影响最小。

（二）安全事件处置后，应通过对有关事件或行为的分析结果，找出问题根源，明确相应补救措施并彻底清除。

（三）安全事件处置后，要及时清理系统，恢复数据、程序、服务，恢复工作应避免出现误操作导致的数据丢失。

第二十条 系统恢复运行后，网安办对事件造成的损失、事件处理流程等进行分析评估，总结经验教训，撰写事件处理报告。

第六章 保障措施

第二十一条 加强队伍建设，不断提高工作人员的信息安全防范意识和技术水平，确保安全事件应急处置科学得当。

第二十二条 加强技术保障，不断完善网络安全整体方案，加强技术防护，确保信息系统的稳定与安全。

第二十三条 加强资金保障，网安办应根据校园网安全防护和应急处置工作实际需要，提出软硬件设备及运行维护经费预算，以专项经费列支。

第二十四条 加强培训和演练，定期组织相关人员开展网络信息安全培训，增强防范意识和应急处置能力，开展应急处置演练，确保安全措施有效落实。

第七章 附则

第二十五条 学校原有相关制度如与本办法不一致，以此为准。

第二十六条 本办法由信息化建设与管理处负责解释，自公布之日起实施。

杨凌职业技术学院院长办公室　　2023 年 12 月 27 日印发