惠州经济职业技术学院网络突发事件应急预案

（2024 年 9 月 23 日修订）

一、总则

为确保校园网络的安全稳定运行，及时应对和处置网络突发事件，根据《中华人民共和国计算机信息系统安全保护条例》《计算机病毒防治管理办法》等相关法律法规，结合本校实际情况，制定本预案。

本预案适用于惠州经济职业技术学院校园网络内发生的各类突发事件，包括但不限于火灾、网络病毒、黑客攻击、数据泄露、设备故障、线路中断、被盗案件等。

二、组织机构与职责

（一）应急领导小组

成立校园网络突发事件应急领导小组，由主管校领导担任组长，信息中心、安全保卫处（保卫部）、各部门负责人等为成员。负责突发事件的决策、指挥、协调及后续处理工作。

（二）信息中心

信息中心负责网络突发事件的监测、预警、应急处置及恢复工作。

（三）安全安全保卫处（保卫部）

安全保卫处（保卫部）负责校园安全及突发事件的安保工作，包括现场控制、协助公安部门处理案件等。

三、应急响应流程

（一）预警与报告

校园网络监测系统发现异常或收到师生员工报告后，立即进行初步判断，并立即向应急领导小组报告。

（二）启动应急预案

应急领导小组根据事件性质，启动相应的应急处置预案，组织相关人员进行处置。

四、应急处置

（一）火灾事故应急预案

1.报警：

迅速判断火情，立即拨打119消防电话，待对方记录完毕后方可挂机。电话内容如“惠州经济职业技术学院信息中心发生火灾。地点：实训中心二楼202室，马安镇新乐路，请迅速前来扑救”。同时向学校安全保卫处（保卫部）值班人员和主管领导报告，安排人员等待和引导消防车辆。

学校安全安全保卫处（保卫部）值班电话：内线7991，外线3617991，手机13829904818。信息中心电话：内线：6700，外线3256700手机：13719680619。

2.组织实施：

（1）消防车到来之前尽力组织在场人员使用机房灭火器具灭火，将火势控制在最小。

（2）消防车到来之后校内人员配合消防专业人员扑救和做好辅助工作。

（3）随时判断火情，在可能失控或自动灭火器启动前迅速组织人员通过紧急通道逃生。

3.扑救方法：

（1）无论发生固体火灾还是电气火灾须首先切断电源。

（2）必须使用机房配备的专用气体灭火器具进行扑救，绝对不能用水扑救。

4.注意事项：

（1）发现火灾应掌握“边救火，边报警”原则。

（2）须确保人员不受伤害的前提下进行火灾事故扑救。

（3）在逃生时应掌握正确的逃离方法。

（二）网络病毒突发事件应急预案

1.发现计算机被感染上病毒后，应立即向本部门网络管理员报告，将该机从网络上隔离开；解决不了的，再向信息中心报告。

2.各部门信息安全人员负责对本部门设备硬盘进行重要数据备份和杀毒处理。

3.信息中心应及时判明病毒，将感染情况通报各部门，做好病毒扩散预防工作。

4.如果现行杀毒软件无法清除该病毒，应立即向信息中心领导报告，迅速联系有关产品商研究解决。

5.学校应急领导小组经会商，认为情况严重的，应立即向当地人民政府信息化主管部门和公安部门报警。

6.若校园网感染病毒程度严重，经应急领导小组同意立即通知相关部门做好停网准备，实物物理断网查杀。

（三）网络突发事件应急预案

1.网站、网页出现不良信息事件紧急处置措施

（1）校园网网站和网页由信息中心和保卫部门值班人员负责随时密切监视信息内容。

（2）发现校园网出现学校信息泄密情况、擅自传播公布违法信息或利用公众号、微博、微信工具和手段散布违法言论等，值班人员应先及时采取删除等处理措施，或立刻查封违法者的 IP 地址，必要时可采取切断网络的方式控制事态的发展，再按程序向信息安全负责人汇报。

（3）信息安全负责人应在接到通知后立即赶到现场，做好必要记录，清理非法信息，妥善保存有关记录及日志或审计记录，强化安全防范措施后，网站网页重新投入使用。

（4）追查非法信息来源，并将有关情况向学校信息化网络领导小组汇报。

（5）应急领导小组召开小组会议研究处理，如事态严重，应立即向公安部门报警。

2.黑客攻击事件紧急处置措施

（1）当管理人员发现网页内容被篡改，或通过入侵检测系统发现黑客正在进行攻击时，应立即向信息安全负责人通报情况。

（2）信息安全负责人应在接到通知后立即赶到现场，并首先将被攻击的服务器等设备从网络中隔离出来，保护现场，并将有关情况向学院信息化领导小组汇报。

（3）应急领导小组组长召开小组会议，如认为事态严重，则立即向公安部门报警。

（4）对现场进行分析，并写出分析报告存档。

（5）恢复、重建被攻击或被破坏的系统。

3.软件系统遭破坏性攻击的紧急处置措施

（1）重要的软件系统平时必须存有备份，与软件系统相对应的数据必须按备份规定的时间按时进行备份，并将它们保存于安全处。

（2）一旦软件遭到破坏性攻击，应立即向信息安全负责人报告，并将该系统停止运行。

（3）检查信息系统的日志等资料，确定攻击来源，并将有关情况向学校信息化领导小组汇报，再恢复系统和数据。

（4）应急领导小组组长召开小组会议，如认为事态严重，则立即向公安部门报警。

4.数据库安全紧急处置措施

（1）主要数据库系统应按双机热备设置，并至少要准备两个数据库备份。

（2）一旦数据库崩溃，值班人员应立即启动备用系统，并向信息安全负责人报告。

（3）在备用系统运行期间，信息安全工作人员应对主机系统进行维修并做数据恢复。

（4）如果系统崩溃无法恢复，应立即向有关厂商请求紧急支援。

5.广域网外部线路中断紧急处置措施

（1）广域网线路中断后，值班人员应立即向信息中心领导报告，并在校内发布公告。

（2）信息中心领导接到报告后，应迅速判断故障节点，

查明故障原因。

（3）如属学校管辖范围，由信息安全工作人员立即组织予以恢复。

（4）如属校外运营商管辖范围，应立即与该公司维护部门联系修复。

6.局域网中断紧急处置措施

（1）信息中心平时应准备好网络备用设备，存放在指定的位置。

（2）局域网中断后，信息安全负责人员应立即判断故障节点，查明故障原因，并向主管领导汇报。

（3）如属线路故障，应重新安装线路。

（4）如属路由器、交换机等网络设备故障，应及时处理。

（5）如属路由器、交换机配置文件破坏，应迅速按照要求恢复配置，并调测通畅。

（6）如有必要，应向主管领导汇报。

7.设备安全紧急处置措施

（1）监控到交换机、服务器等关键设备损坏后，管理人员应立即报告。

（2）信息中心立即查明原因。

（3）如有库存备件并且能够自行更换，应立即用备件替换受损部件。

（4）如果不能自行修复，应立即与设备提供商联系，请求派维护人员前来维修。

（四）被盗案件应急预案

（1）发现案件时应及时向学校安全保卫处（保卫部）值班室报警（值班电话：内线 7991，外线 3617991，手机 13829904818）。

（2）向信息中心领导报告。内线：6700，外线 3256700 手机：13719680619

（3）根据案情报告分管领导和学校主管领导。

（4）经领导同意后向公安机关报案。

（5）注意保护现场，以便为侦破案件提供条件。积极协助公安人员勘查现场，为侦破提供条件。

五、保障措施

（一）人员保障

组建专业的应急处置队伍，定期进行培训和演练，提高应急处置能力。

（二）技术保障

加强网络安全监测和预警系统建设，确保及时发现并处置网络突发事件。

（三）物资保障

储备必要的应急物资和设备，包括灭火器材、备份设备、应急通信工具等。

六、附则

本预案自发布之日起施行，由信息中心负责解释并组织实施。如有未尽事宜，将根据实际情况进行修订和完善。