中共陕西国防工业职业技术学院委员会文件

陕国职党发〔2020〕68号

关于印发《陕西国防工业职业技术学院校园网络安全应急预案》的通知

校属各单位:

《陕西国防工业职业技术学院校园网络安全应急预案》经2020年10月26日学校第17次党委会议研究通过,现予以印发,请遵照执行。

附件:《陕西国防工业职业技术学院校园网络安全应急预案》

中共陕西国防工业职业技术学院委员会

2020年10月28日

附件

陕西国防工业职业技术学院
校园网络安全应急预案

为切实做好我校校园网络突发事件的防范和应急处理工作，进一步提高我校预防和控制网络突发事件的能力和水平，减轻或消除突发事件的危害和影响，确保我校校园网络与信息安全，特制定本预案。

一、网络与信息安全事件定义

根据网络与信息安全事件的发生原因、性质和机理，网络与信息安全事件主要分为以下三类:

（一）攻击类事件: 指网络与信息系统因计算机病毒感染、非法入侵等造成校园网网站主页被恶意篡改、交互式栏目里发表不良信息；应用服务器（如办公系统、财务系统等）被非法入侵，应用服务器上的数据被非法拷贝、修改、删除；在网站上发布的内容违反国家的法律法规、侵犯知识版权并已造成严重后果等，由此导致的业务中断、系统宕机、网络瘫痪等情况。

（二）故障类事件: 指网络与信息系统因计算机软硬件故障、人为误操作、网络设备故障等导致业务中断、系统死机、网络瘫

瘫等情况。

（三）灾害类事件：指因洪水、火灾、雷击、地震、台风等外力因素导致网络与信息系统损毁，造成业务中断、系统死机、网络瘫痪等情况。

二、网络与信息安全应急处置预案

（一）领导机构和责任分工

学校“网络安全与信息化工作领导小组”是实施校园网信息安全事件应急处置预案的领导机构，统一领导全校信息网络的灾害应急工作，全面负责学校信息网络可能出现的各种突发事件处置工作，协调解决灾害处置工作中的重大问题等。小组各成员单位按照责任分工具体负责相关处置工作的实施。

（二）加强信息审查

1.学校各单位要加强运行管理的信息系统（含部门网站）的信息审查工作。若发现系统内容被恶意更改，或被嵌入恶意代码，应立即恢复正确内容，同时联系网络与信息中心，共同分析查找被更改的原因，修复漏洞。

2.学校各单位所属独立物理服务器或服务器虚拟化中建立的服务器在对外提供信息服务时，必须经过网络中心的审核批准，并建立相关管理制度和安全防范措施，如：日志留存（6个

月）、安全认证、实时监控、防黑客、防病毒、防篡改等。落实管理责任人，加强对网络设备日志的分析，及时收集信息，排查不安定因素。

（三）加强实时监控，坚持科学处置

1.对校园网络现有信息系统和今后新建设的信息系统，参照国家有关信息安全等级保护的要求，按照最终确定的保护等级采取相应的安全保障措施。

2.建设安全事件预警预报体系和校园网络安全工作值班制度，加强对校园网络和重点信息系统的监测、监控，加强安全管理，对可能引发网络与信息安全事件的有关信息，要认真收集、分析判断，发现有异常情况时，及时处理并逐级报告。

3.网络与信息中心对校园网用户上网实行实时监控，若发现有异常行为应立即关闭该用户的网络连接，及时记录在案，并对其警告和批评教育，严重违法行为应立即上报有关部门。

4.特殊时期，可根据教育厅和学校的统一要求和部署，由网络中心进行统一安排，组织专业技术人员对网络和信息数据采取加强保护措施，对网络进行不间断的监控。

（四）加强技术防范措施

1.网络中心负责建立安全、稳定的校园网络运行环境，加强

网络与信息安全的防范措施。根据上级要求和实际需要，通过安全态势感知、防火墙等安全设备，定期对校园网进行安全状态监控，增强网络的安全性。

2.学校各单位所属信息系统要采用可靠设备和成熟软件，进行必要的数据备份，严格遵守安全操作规范，严格限制内部用户的访问权限，加强密码强度和管理，采取有效保护措施，构建安全的防护体系。

（五）突发事件的处置

在发生网络与信息安全事件后，网络中心应尽最大可能收集事件相关信息，鉴别事件性质，确定事件来源，以确定事件范围和评估事件带来的影响和损害，确认为网络与信息安全事件后，对事件进行处置和上报。

按照事件发生的性质分别采用以下处置措施:

1.病毒传播：针对这种现象，要及时断开传播源，判断病毒的性质、采用的端口，然后关闭相应的端口，在网上公布病毒攻击信息以及防御方法。

2.入侵：对于网络入侵，首先要判断入侵的来源，区分外网与内网。入侵来自校园网外的，定位入侵的 IP 地址，及时关闭入侵的端口，限制入侵地 IP 地址的访问，在无法制止的情况下

可以采用暂时断开网络连接的方法。入侵来自校园网内的，查清入侵来源，如 IP 地址、MAC 地址、上网用户账号等信息，同时断开对应的交换机端口。然后针对入侵方法建设或更新入侵检测设备。

3.信息被篡改：一经发现马上断开相应的信息上网链接，并尽快恢复。

4.网络故障：一旦发现，根据相应工作流程确定故障点，并尽快排除。

5.其它没有列出的不确定因素造成的灾害，可结合具体的情况，做出相应的处理。不能处理的网络与信息中心将请示相关机构的专业人员尽快进行修复，根据保留的取证，进行分析、查找原因。

（六）上级通报信息安全事件处置

对于国家网监或上级部门通报的有关我校信息安全事件，按相关程序要求由网络中心牵头，校内相关部门配合进行处置。

（七）严重信息安全事件紧急处置

对于严重的信息安全事件，网络与信息中心管理人员可视情况直接采取关闭相关应用系统、关闭服务器（含虚拟机）、断网、断电等紧急处置手段，同时向学校“网络安全与信息化工作领导

小组”汇报事故情况和处理措施，并按相关程序向上级有关部门通报情况。

三、应急处置后续处理

（一）在进行最初的应急处置以后，应及时采取行动，抑制安全事件影响的进一步扩大，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。在发生网络故障时，优先保证要害部门的网络畅通。

（二）在事件被抑制之后，通过对有关事件或行为的分析结果，找出事件根源，明确相应的补救措施并彻底清除。

（三）在确保安全事件解决后，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。

（四）记录和上报。网络发生故障时，应及时向网络中心报告，由网络中心及时处理。重大网络与信息安全事件发生时，应及时向党委及网络安全与信息化领导小组汇报。并在事件处置工作中作好完整的过程记录，及时报告处置工作进展情况，保存各相关系统日志，直至处置工作结束。

（五）结束响应。系统恢复运行后，网络中心对事件造成的损失、事件处理流程和应急预案进行评估，对响应流程、预案提出修改意见，总结事件处理经验和教训，撰写事件处理报告，同

时确定是否需要上报该事件及其处理过程，需要上报的应及时准备相关材料；根据情况上报公安部门及陕西省教育厅。

抄送：党委委员，校领导。

陕西国防学院党政办公室　　2020年11月5日印发