**永州师范高等专科学校网络安全应急预案**

为做好学校网络安全事件的防范和应急处理工作，提高预防和遏制网络突发事件的能力和水平，避免和减轻突发事件的危害和影响，提高应急工作水平，确保我校网络信息的安全性与可靠性，结合我校网络信息安全工作实际,制定本预案。

一、总则

（一）本预案所称突发性事件，是指自然因素或者人为活动引发的危害学校网络设施及信息安全等有关的灾害。

（二）本预案的指导思想是学校有关计算机网络及信息安全的管理制度。

（三）本预案适用于发生在永州师范高等专科学校整个网络的突发性事件应急工作。

（四）应急处置工作原则：统一领导、统一指挥、各司其职、整体作战、发挥优势、保障安全。

二、组织指挥和职责任务

（一）组织指挥

成立网络信息安全应急处置工作领导小组。

组长：

副组长：

成员：

领导小组下设办公室：党政办公室。主任：盘家禄，副主任：周柏春

（二）职责任务

领导小组的主要职责与任务：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。

日常工作，由教育信息技术中心承担。

三、处置措施和处置程序

（一）处置措施

处置的基本措施分灾害发生前与灾害发生后两种情况。

1.灾害发生前，党政办公室要对灾害预警预报体系进行建设，开展灾害调查，编写灾害防治规划,建立健全灾情速报制度，保障突发性灾害紧急信息报送渠道畅通，规划建设灾害信息管理系统，及时处理灾害讯情信息。教育信息技术中心要充分发挥专业监测的作用，建设好网络监测系统，进行定期和不定期的检查，加强重点部位的监测和防范，发现有不良险情时，及时处理。

2.灾害发生后，立即启动应急预案，采取应急处置程序，判定灾害级别，并立即将灾情向领导小组报告，在处置过程中及时报告处置工作进展情况，直至处置工作结束。

（二）处置程序

1.发现情况

党政办公室要严格执行巡查制度，做好校园网信息系统安全的日常巡查及日志保存工作。全校师生员工都有监控校园网络的权力与义务，发现校园网络有异常情况得出现，都应及时报告和处理，以保证及时发现灾害并处置突发性事件。

2.预案启动

一旦灾害发生，立即启动应急预案，进入应急预案的处置程序。

3.应急处置方法

在灾害发生时，首先应区分灾害类型是否为自然灾害或人为破坏，根据这两种情况把应急处置方法分为两个流程：

流程一：当发生自然灾害时，应根据当时的实际情况，在保障人身安全的前提下，首先保障数据的安全，然后是设备安全。具体方法包括：硬盘的保护，设备的断电与拆卸、搬迁等。

流程二：当人为或病毒破坏等灾害发生时，具体按以下顺序进行：判断破坏的来源与性质，断开影响安全与稳定的信息网络设备，断开与破坏来源的网络物理连接，跟踪并锁定破坏来源的IP或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照灾害发生的性质分别采用以下方案：

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。

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。入侵来自外网的，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断开网络连接的方法。入侵来自内网的，查清入侵来源，如IP地址、MAC地址、上网账号等信息，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。

信息被篡改：这种情况，要求一经发现马上断开相应的信息上网链接，并尽快恢复。

网络故障：一旦发现，可根据相应工作流程尽快排除。

其它没有列出的不确定因素造成的灾害，可根据总的安全原则，结合具体的情况，做出相应的处理。不能处理的可以求助相关专业人员。

（三）情况报告

灾害发生后，按照应急处置方法进行处置，同时需要判定灾害的级别，第一时间向学校汇报并及时报告处置工作进展情况，直至处置工作结束。

具体的情况报告内容包括：灾害发生的时间、地点，灾害的级别，灾害造成的后果，应急处置的过程、结果，灾害结束的时间，以后如何防范类似灾害发生的建议与方案等。

（四）发布预警

灾害发生时，可根据灾害的危害程度适当地发布预警，特别是一些在其它地方已经出现，或在安全相关网站发布了预警而学校信息网络还没有出现相应的灾害，除了在技术上进行防范以外，还应当向网络信息用户发布预警，直至灾害警报解除。

（五）预案终止

险情或灾情已消除或者得到有效控制后，由学校的信息技术中心宣布险情或灾情应急期结束，并予以公告，同时预案终止。

四、保障措施

灾害应急防治是一项长期的、持续的、跟踪式的、深层次的与各阶段相互联系的工作，是有组织的科学与社会行为，而不是随每次灾害的发生而开始和结束的活动。因此，必须做好应急保障工作。

（一）人员保障

重视人员的建设与保障，确保日常工作中的人员正常履职，灾害处置过程和灾后重建中的人员在岗与战斗力。

（二）技术保障

重视网络信息技术的建设和升级换代，在灾害发生前保证网络信息系统的强劲与安全，提供灾害处置过程中和灾后重建中的相关技术支撑。

（三）物资保障

学校要根据信息系统安全防治工作所需经费情况，将灾害应急经费纳入预算，购买相应的应急设施设备。建立应急物资储备制度，保证应急抢险救灾队伍技术装备的及时更新，以确保灾害应急工作的顺利进行。

（四）训练和演练

加强对全校网络信息用户的防灾、减灾知识的宣传普及，增强其防灾意识和自救互救能力。有针对性地开展应急抢险救灾演练，确保受灾后应急救助手段的及时到位和有效。

五、附则

（一）本预案由党政办公室、信息技术中心负责解释。

（二）本预案自发布之日起施行。

永州师范高等专科学校

二〇一九年八月二十日