长春人文学院网络安全应急预案

为了贯彻执行《中华人民共和国网络安全法》，严格落实网络安全责任，有效应对各类网络安全事件，有效降低网络安全事件影响，按照《教育系统网络安全事件应急预案》和《信息技术安全事件报告与处置流程（试行）》的要求，制定本应急预案。

第一章　总　则

一、指导思想：减轻和消除网络安全突发事件造成的危害和影响，维护学校的安全和稳定，“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、适用范围：学校建设、运行、维护或管理并支撑学校教学、科研和管理等各项事业的校园网络和所有信息化业务系统、网站、数据中心等信息资产（信息及信息系统）。

本预案所指学校各部门包括各机关部、处、室，学院、部，直属单位以及有关科研机构。

三、处置原则：快速、有效。

第二章　组织指挥和职责任务

四、组织指挥：由校网络安全与信息化建设工作领导小组或授权的领导组织指挥，数字化校园建设规划处（以下简称数建处）具体沟通协调。

五、职责任务

数建处负责学校网络安全应急处置沟通协调、校级层面处置

实施和信息上报工作；

学校各部门负责本单位信息系统(网站)网络安全事件处置、校内信息上报工作，应全力配合数建处技术人员进行应急处置、后期取证、事件回溯和排查等技术工作。

第三章　处置措施和处置程序

六、处置措施

（一）接到网络安全事件报告或安全威胁预警，数建处值班人员第一时间通过技术手段切断校园网络或指定信息系统（网站）IP 地址与校园网外的连接。

（二）学校信息系统（网站）管理人员接到网络安全事件报告或安全威胁预警，应第一时间使用各种手段关闭系统服务，并报告数建处。

（三）数建处网络安全事件处置相关管理人员和信息系统（网站）管理人员对出现安全事故的设备进行物理隔离，复制相关日志，并进行适当的技术处理以保持现状，等待后续处置工作开展。

七、处置程序

（一）学校信息系统（网站）主管部门网络安全与信息化建设联络员应监控信息系统（网站），对互动栏目、主要网页异动等网络安全事件充分利用高科技手段尽早发现。

（二）预案启动：一旦发现网页内容被篡改、数据被丢失、系统后台被未授权用户登录、系统服务出现非正常关闭等网络安全事件以及上级部门、网络安全相关国家部门等安全事件通报，

本预案即时启动，并通知学校主管网络安全的领导班子成员。

（三）应急处置：在安全事故发现第一时间响应，时间要求根据网信办、公安部、教育部等有关文件要求，取最高要求为准，尽可能保持现场，处置响应时间不高于5分钟，上报数建处时间不高于10分钟。

（四）情况报告：学校各部门应无条件向数建处上报网络安全事件和处置进展；数建处负责校内网络安全事件请示汇报、沟通协调，严格按照《信息技术安全事件报告与处置流程（试行）》要求上报教育部有关部门，并根据有关文件要求向省教育厅主管部门及省公安厅主管部门等汇报。

（五）发布预警：在网络安全与信息化建设工作领导小组的部署下，数建处可向学校有关部门发布预警。网络安全保障重要时期内，数建处可按需调整和实施重要时期网络防护策略；数建处面向学校各部门网络安全与信息化建设联络员通知重要时期期限和网络防护策略。

（六）预案终止：网络安全事件处置完毕后报请学校主管网络安全的领导班子成员批示，确定恢复网络连接及其相应措施以终止预案恢复正常使用。

第四章　保障措施

八、人员保障

数建处使用各类技术手段来主动监控学校校园网络、信息系统（网站）等信息资产运行状况。

网络安全保障重要时期内，学校各部门若因业务工作开展需

求，在重要时期需要面向互联网提供服务,需向数建处备案和提交《信息系统（网站）重要时期网络安全责任书》，开放指定的IP 地址和网络端口，并指定本单位工作人员落实 7×24 小时值守和每日“零报告”制度,严格执行《信息系统（网站）7×24 小时值班守则》。

九、技术保障

数建处负责学校网络安全防护体系的规划、建设和运维，包括但不限于防火墙系统、入侵检测系统、入侵防御系统、Web 应用防护系统、内容审计系统、网络防病毒系统、登录审计系统、数据库审计系统、流量分析系统、网络安全态势感知系统、信息资产发现与管理系统。

十、训练和演练

数建处通过校内各种宣传形式对师生员工进行正面引导、宣传并落实我校园网络安全相关管理制度,各部门应积极参与和做好本单位内部网络安全宣传教育工作。

在网络安全与信息化建设工作领导小组的统一部署下,数建处负责组织学校范围网络安全应急处置演练。

第五章　工作要求

所有数建处网络安全应急处置相关工作人员、数建处值班人员、学校各部门主管网络安全的领导班子成员、学校各部门网络安全与信息化建设联络员必须保证通讯畅通、工作认真负责。

数字化校园建设规划处

2023 年 6 月 26 日