聊城大学网络与信息安全管理办法

第一章 总则

第一条 为加强学校网络与信息安全管理工作，提高安全防护能力，保障校园网络与信息安全，维护安全稳定的校园网络环境和正常工作秩序，维护我校师生合法权益，根据《中华人民共和国网络安全法》等法律法规，结合我校实际，制定本办法。

第二条 本办法所指网络与信息安全管理，是为维护校内服务于教学、科研或管理工作的校园网络（公共基础网络设施）、数据中心（公共基础信息系统平台）、应用系统（业务系统）和互联网站等的正常运行，防止网络攻击、信息破坏、有害程序入侵、信息化设备设施故障等隐患威胁而开展的预防和防御工作，可分为基础网络设施安全、信息系统安全和信息内容安全三个方面。

（一）校园网公共基础设施安全是指包括校园网出口层、核心层、接入层的服务器、路由器、交换机、光传输线路、中心机房、弱电间等网络互联设备设施的安全。

（二）信息系统安全是指承载信息系统的服务器和存储设备、软件运行环境以及系统数据的安全，包括公共基础信息平台安全和业务应用信息系统安全两个层面。

1.校园公共基础信息平台（数字化校园基础信息平台）的安全主要包括数字聊大统一身份认证平台、统一信息门户平台、统

一通讯平台、数据中心云平台、网站群系统、电子邮箱系统等软硬件设施的物理安全、系统与数据安全等。

2.业务应用信息系统包括各单位使用学校域名、IP 地址建设运行的互联网站及业务管理系统的运行安全，主要包括教务管理系统、研究生管理系统、学工系统、资产管理系统、人力资源管理系统、财务管理系统、图书管理系统等。

（三）信息内容安全是指通过互联网站发布的各种信息内容的安全、网络舆情管控等。

第三条 按照校内、校外防控并举，人防、技防并重的安全防护原则，监测、防御、处置来源于校内外的网络安全风险和威胁，保护信息系统、关键信息基础设施免受攻击、侵入、干扰和破坏；加强校园网络信息和舆情管控引导；维护学校网络空间安全和秩序。

第四条 坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络设施建设，促进信息系统互联互通、数据共享，鼓励网络技术创新和应用，加强网络安全技术队伍建设，健全网络安全保障体系，提高网络安全保护能力。

第五条 倡导诚实守信、健康文明的网络行为；围绕立德树人，推动传播社会主义核心价值观，构建积极向上的校园网络文化氛围；加强宣传教育与培训，提高全校师生的网络安全意识和水平，形成全员共同参与促进网络安全的良好环境。

第六条 全体师生使用网络应当遵守宪法法律，遵守公共秩

序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第二章 机构与职责

第七条 聊城大学网络安全与信息化工作领导小组（简称“领导小组”）是学校网络安全与信息化工作的组织领导与决策机构，负责研究、决策、部署全校网络安全和信息化工作重大事项。

第八条 网络安全与信息化工作领导小组办公室（简称“网络与信息化办公室”）分别设在宣传部和实验与网络信息中心，负责统一管理、具体落实学校网络安全与信息化工作。

（一）宣传部是学校网络信息内容发布与传播安全的监管职能部门，负责学校主网站建设与管理，网络舆情监管，全校二级单位网站的宏观管理。

（二）实验与网络信息中心是学校基础网络设施安全、信息系统安全的日常管理和技术支撑部门，负责定期开展网络安全等级保护测评与备案工作；负责网络安全技术防护体系的建设、维护；负责学校信息系统的日常安全检测、安全漏洞信息监测收集、安全漏洞预警及系统安全加固；监督各单位信息系统安全漏洞的

整改，并提供技术支持。

第九条 按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，全校各单位及全体师生员工应依照本办法及其相关标准规范履行网络与信息安全的义务和责任。学校各单位是本单位网络与信息安全工作的责任主体，单位主要负责人是本单位网络与信息安全工作第一责任人，并专设网络安全信息员（须为在职教职工），负责管理和协调本单位的具体网络信息安全工作，采取必要措施保障网络安全、稳定运行，有效应对网络安全威胁和事件，防范网络违法犯罪活动，维护网络数据信息的完整性、保密性和可用性。

第三章 业务应用信息系统安全

第十条 落实网络安全等级保护制度，及时开展网络安全等级保护工作。按照《网络安全法》和《计算机信息系统安全保护条例》的要求进行信息系统的定级和备案工作，并定期进行安全等级测评、整改、新建、改建、扩建信息系统应在设计阶段确定安全保护等级并同步建设安全防护措施。学校对已上线的信息系统定期开展网络安全等级保护工作；对拟上线的信息系统，需通过网络安全等级保护工作后，方可上线运行。

各单位建设使用维护信息系统，应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，制定网络安全隐患漏洞整改流程，制定网络安全事件应急预案，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据容灾备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第十一条 严禁“双非信息系统”（未经学校许可，内容与学校相关或带有学校标志标示，且使用非学校域名、非学校 IP 地址的网站和信息系统），落实执行国家有关法律规定。各单位网站和信息系统，须全部纳入学校统一规划与管理，使用学校域名、IP 地址，并与学校签署“聊城大学网络安全责任书”。

第十二条 定期清理“僵尸”信息系统。网络与信息化办公室将定期对存在安全隐患、无人管理、内容不做更新的“僵尸”信息系统（含网站）进行清理。

第十三条 加强对第三方信息系统服务的网络安全监管。各相关单位因业务需要，使用第三方信息系统与技术服务的，须在网络与信息化办公室进行登记备案，并提供和第三方信息服务商签订的合约、协议等，包括安全责任、服务内容、服务方式、服务级别和保密条款等内容。

第十四条 加强各管理部门业务信息系统（也称应用系统或

管理系统）的建设管理。

（一）鼓励优先采购安全、成熟和售后服务优良的商业软件或优秀软件开发商用于应用系统建设。没有相应成品商业软件，或商业软件不适应我校实际需求的，可以按照学校采购与招标相关办法委托资质和信誉良好的软件开发商进行开发。对于业务管理部门具有应用系统开发维护能力并能够保证其信息安全的，可在学校顶层设计和软硬件配置框架内自行组织开发。

（二）软件的采购、开发与维护管理。业务管理部门根据本部门业务需要撰写需求分析报告，明确详细的功能和性能需求。实验与网络信息中心负责软件所需的数据中心资源，包括硬件、运行平台软件和基础数据等，协助制定技术方案。网络与信息化办公室组织对技术方案进行论证和审批，并确定拟建应用系统信息安全保护等级。应用系统按照相应等级的规范要求进行建设。

对于购买商业软件或委托软件开发的，业务管理部门根据论证和审批通过后的方案，按照学校采购与招标相关办法进行采购。

业务管理部门为相关应用系统的安全管理责任部门，应指定专门人员负责系统的建设、运行维护和安全管理，组织软件提供商并会同实验与网络信息中心制定应用系统运维和安全管理方案。原则上应由业务管理部门全面负责应用系统运维，可根据实际需要委托软件开发方提供运维技术支持，并正式签订相关的安全保护协议。

（三）应用系统投入试运行后，由业务管理部门初步验收，

出具初步验收报告，并向网络与信息化办公室申请开展信息安全保护等级测评。

（四）网络与信息化办公室组织开展信息安全保护等级测评，形成测评报告，该报告为应用系统竣工验收的重要内容。网络与信息化办公室参与应用系统竣工验收。

第四章 网络信息内容安全

第十五条 学校网络信息发布遵循“谁主管、谁负责”的原则。各单位严格执行《聊城大学网站建设与管理办法》相关规定，加强网站管理与维护，落实信息发布审核机制。学校门户网站内容由宣传部负责审核发布，二级网站内容由各单位负责审核发布。

第十六条 学校各单位建设网站，必须使用学校域名和学校IP地址。

（一）各单位设立互联网站，网站架构可基于学校网站群平台建设，也可通过委托软件技术开发建设；各单位应按信息安全保护等级的相应规范落实信息安全防护。

（二）学校网站群平台由学校统一部署建设，其运行环境安全由实验与网络信息中心负责；运行在网站群平台上的网站内容安全由网站主办者负责。未在学校网站群平台运行的网站，网站主办者对其技术和内容安全全面负责。

（三）各互联网站的主管单位应建立网站应急值守制度，规

范应急处置流程，由专人对网站进行监测，发现网站运行异常及时处置。对于使用频度不大、阶段性使用的网站，可采取非工作时间或节假日关闭的方式运行。

第十七条 确保上网信息合法且不涉密。各单位网络安全负责人和信息员要切实负起责任，加强对信息发布的管理，涉密信息不上网，上网信息不涉密。发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散。

第十八条 严格执行《聊城大学舆情管理实施办法（试行）》，加强校园网络舆情监控管理。发现有害信息，积极开展舆情应对与处置。

第十九条 各单位采集、使用师生个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并采取技术措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失，严格保密。

第二十条 单位和个人发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

第五章　网络信息公共基础设施安全

第二十一条 校园信息化基础平台设施的建设须具备支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步

建设、同步使用。重要核心信息基础网络设施要符合行业标准规范要求进行建设部署与管理。学校对重要核心信息基础设施每年至少进行一次安全检查，对存在的安全隐患进行排查治理。

第二十二条 加强信息基础平台安全防护。健全完善多层级的校园网安全防护设施，按需配置各级网络安全防护设备和软件，构建可查、可管、可控的校园网络安全技术设施支撑环境；加强和完善身份认证威胁识别、态势感知、入侵检测、漏洞扫描、攻击防护、访问控制、操作审计、容灾备份等安全技术措施，确保关键信息基础设施安全稳定运行。

第二十三条 加强校园网基础设施安全管理

（一）校园信息网络包括校园网络、公用通信网络和专用通信网络，统一归口网络与信息化办公室管理。

（二）校园信息网络管道由网络与信息化办公室负责提出建设需求，并负责建成后的使用管理；校园建设规划管理部门和建设部门负责在学校地下管网统一管理的原则下，进行规划、建设和运行维护。

（三）校园网络管理包括校园有线网络和无线网络，涉及校园网出口层、核心层、接入层的服务器、路由器、交换机、光传输线路、网络中心机房、弱电间等网络互联设备设施光缆、域名管理、安全防护、认证计费、网络接入与运维等，由实验与网络信息中心负责建设和运行维护管理。

网络接入单位负责提供本单位所需的网络设备间和电源保障，协助解决网络布线和设备安装所需空间，负责其安防和消防

安全管理。

（四）校园网接入互联网遵循“统一出口、统一管理”的规定，由实验与网络信息中心负责实施。学校各单位在校园内不得擅自通过社会网络资源接入互联网。

（五）师生员工接入校园网络，实行实名注册、认证上网的制度。网络接入实名制由实验与网络信息中心负责实施。

（六）学校所有基建、修缮工程应将工程范围内的校园网络建设纳入工程设计、实施和竣工验收范畴。

（七）严禁任何单位和个人利用校园网络及其网络设施开展经营活动。

第二十四条 加强公共基础信息平台的安全管理

（一）公共基础信息平台主要包括支撑各类应用系统运行的软硬件基础设施、学校基础数据库、统一数据交换平台、统一身份认证系统及统一信息门户。实验与网络信息中心负责公共基础信息平台的建设和运行维护管理。

（二）实验与网络信息中心负责公共基础信息平台的物理安全、网络安全和主机安全。公共基础信息平台的资源使用单位负责所使用的操作系统、业务数据库系统、应用系统和数据的安全。

（三）实验与网络信息中心负责学校基础数据库和统一数据交换平台的建设和安全管理，负责各单位业务数据库与基础数据库之间完成数据交换和共享。

（四）各单位负责建设、维护本单位业务应用系统所配套的业务数据库；对本单位业务数据库的系统安全、数据安全及所申

请的共享数据的安全负责。

（五）实验与网络信息中心负责统一身份认证系统的管理维护。统一身份认证系统为校内信息系统提供统一的身份管理、安全的认证机制、审计及标准接口；校内各单位建设面向师生服务的应用系统时，应与统一身份认证系统进行认证集成并备案系统信息；各单位负责本单位应用系统的权限管理及安全。

（六）全校各单位的信息化建设项目（包括建设应用系统或互联网站）应建设部署在校内公共基础信息平台，严禁部署在境外的信息平台；涉及学校基础数据、师生个人信息或敏感信息的应用系统和互联网站，严禁部署在校外信息平台。

（七）学校公共基础信息平台的使用实行准入管理。实验与网络信息中心负责制定使用公共基础信息平台的技术规范和标准，在系统上线前进行安全检测。符合技术规范标准并检测通过的系统方可上线运行。

（八）各单位使用公共基础信息平台的应做好以下工作：

1.遵循公共基础信息平台相关管理制度和技术标准，按需申请、有序使用。

2.规范本单位公共基础信息平台资源的使用和管理，不得利用公共基础信息平台资源从事任何与申请项目无关或危害计算机信息系统安全的活动。

第二十五条 加强校园网内计算机终端、无线终端的安全管理。计算机使用正版操作系统，安装杀毒软件，及时更新系统和病毒库；校园网实行实名认证上网；杜绝弱密码和明文密码。

第二十六条 任何单位和个人不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具。

第六章 监测预警与应急处置

第二十七条 建立网络安全隐患发现、通报及处置机制。通过上级网络安全管理部门及我校网络安全技术防护人员提供的网络安全报告，及时获取我校网络安全情况；对出现安全隐患的信息系统，立即采取关、停、限等措施，及时处置、整改；对隐患整改情况进行查验核实，确认隐患排除后，解除访问限制、恢复系统正常运行，同时向有关部门及时反馈整改结果。

第二十八条 及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，消除安全隐患，防止危害扩大。网络安全突发事件应急处置见《聊城大学网络安全突发事件应急处置流程》（附件 1），信息系统安全漏洞处置见《聊城大学信息系统安全漏洞整改管理细则》（附件 2）。

第二十九条 加强网络安全应急演练。各相关单位按照“第一时间发现、第一时间上报、第一时间处置”的原则，建立健全信息安全值守制度和安全事件应急处置机制，制定安全事件应急预案，定期开展应急演练，提高网络安全事件应急响应与处置能

力，确保安全事件早发现、早报告、早控制、早解决。

第七章 宣传与教育

第三十条 加强网络安全的宣传、教育。各单位制定网络与信息安全教育培训规划，定期组织开展形式多样、针对性强的面向全员的普及型培训和网络安全宣传教育，提高管理人员、技术人员、开发运维人员、师生的信息安全和防范意识；按照上级部门网络安全宣传的部署要求，认真组织开展网络安全宣传月和网络安全宣传周等活动；通过加强学生的网络安全教育，提高安全和防范意识，增强识别有害信息的能力，培养学生良好的网络媒介素养和文明健康规范的网络行为习惯。

第三十一条 学校定期组织各单位信息系统管理员（包括网站信息员）参加校内外举办的信息化管理和技术人员网络安全技术专业培训，增强安全意识，提高安全技术和管理能力。

第八章 责任追究

第三十二条 对违反网络与信息安全相关管理规定建设使用信息系统、网站以及网络基础平台设施，或未及时处置整改网络安全隐患、漏洞及安全事件或处置、整改不力的单位，学校将视情节轻重追究相关人员的责任。

第三十三条 师生员工违反网络与信息安全相关管理规定，造成不良后果时，视情节轻重，分别由教职工人事管理部门或学生管理部门按相关规定给予批评教育或纪律处分；触犯法律时，

由相关国家机关依法追究法律责任。

第九章 经费保障

第三十四条 学校设立网络安全运行维护、网络安全等级保护、网站建设管理等专项经费，保障学校网络安全工作正常开展。

第十章 附则

第三十五条 本办法自发布之日起施行，由网络与信息化办公室负责解释。

附件：1.聊城大学网络安全突发事件应急处置流程

2.聊城大学信息系统安全漏洞整改管理细则

附件 1

聊城大学网络安全突发事件应急处置流程

第一章 总则

第一条 为加强我校网络信息安全工作，及时发现并报告网络信息安全事件，做好应急响应和处置，减少损失与影响，维护正常工作秩序和营造健康的网络环境，根据教育部《信息技术安全事件报告与处置流程》以及《聊城大学网络与信息安全管理办法》，结合学校实际，制定本流程。

第二条 网络信息安全事件的定义。根据《信息安全事件分类分级指南》[GB/T 20986-2007，简称《指南》，摘录部分见附件（1）]，本流程中所称的网络信息安全事件[简称“安全事件”]是指除信息内容安全事件以外的有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件等。

第三条 适用范围。本流程适用于我校各职能部门和各二级单位应对处置除信息内容安全及网络舆情事件以外的网络安全事件(网络安全事件类型级别见第八条)。信息内容安全及网络舆情事件的应对，参照学校有关规定和办法执行。

第二章 网络安全威胁监测与预警

第四条 安全威胁监测。实验与网络信息中心组织对网络安

全威胁进行监测，建立多方协作的信息共享机制，通过教育系统网络安全工作管理平台、教育行业漏洞报告平台、山东教育通用工作平台、山东省网信办、聊城市网信办、聊城市网安支队、中国教育和科研网山东赛尔公司等网络安全职能和服务部门提供的报告，汇聚漏洞、病毒、网络攻击等网络安全威胁信息，实现安全威胁信息的收集、校验、发布、跟踪。各单位加强对本单位网络和信息系统（网站）的网络安全威胁监测，对发生的威胁及时进行处置和上报。

第五条 事件监测。各单位对本单位网络和信息系统（网站）的运行状况进行密切监测，一旦发生网络安全事件，应当立即通过电话等方式向实验与网络信息中心报告，不得迟报、谎报、瞒报、漏报。实验与网络信息中心也通过多种渠道监测、发现已经发生的网络安全事件，并将掌握的情况立即通知相关单位。

第三章 安全事件的报告与处置

第六条 事发紧急报告与处置

（一）网络与信息系统运维操作人员一旦发现上述安全事件，应根据实际情况第一时间采取断网等有效措施进行处置，将损害和影响降到最小范围，保留现场，并报告相关单位安全责任人和主要负责人。

（二）相关单位安全责任人接到报告后，应立即组织人员赶赴现场进行紧急处置，同时以口头通讯的方式向实验与网络信息

中心紧急报告相关情况，并书面记录安全事件发现过程及口头汇报过程。涉及人为主观破坏事件应同时报告学校保卫部门。

（三）实验与网络信息中心接到口头紧急报告后，做好书面记录，并进一步判定安全事件的危害程度，报告网络安全与信息化领导小组相关领导。

（四）紧急报告内容包括：（1）时间地点；（2）简要经过；（3）事件类型；（4）影响范围；（5）危害程度；（6）初步原因分析；（7）已采取的应急措施。

（五）实验与网络信息中心立即组织相关技术力量赶赴现场进行协助处置工作，控制事态防止蔓延。实验与网络信息中心负责采取各种技术措施、管控手段，包括但不限于断开网络、关闭服务器、设置黑名单、暂停账号等，最大限度阻止和控制事态蔓延。涉及人为主观破坏事件的，学校保卫部门应组织人员赴现场协助处置，并协助公安机关做好相关取证和处置工作。

（六）各单位应及时跟进事件发展情况，出现新的情况应及时补报。

第七条 事中情况报告与处置

（一）事中情况报告应在安全事件发现后 6 小时内以书面报告的形式进行报送，报送内容和格式见附件(2)。

（二）事中情况报告由单位安全负责人组织编写，由本单位主要负责人审核后，签字并加盖公章报送实验与网络信息中心。涉及人为主观破坏事件的，事中情况报告应抄送给保卫处。

（三）安全事件的事中处置包括：及时掌握损失情况、查找

和分析事件原因，针对性制定解决方案，修复系统漏洞，恢复系统服务，备份数据、保护设备、排查隐患。对业务连续性要求高的受破坏网络与信息系统（网站）要在保证安全的前提下及时组织恢复。尽可能减少安全事件对正常工作带来的影响。如果涉及人为主观破坏的安全事件应由保卫处联系、配合公安部门和学校保卫部门开展调查。

第八条 事后整改报告与处置

（一）事后整改报告应在安全事件处置完毕后 4 个工作日内以书面报告的形式进行报送，报送内容和格式见附件(3)。

（二）事后情况报告由单位安全负责人组织编写，由本单位主要负责人审核后，签字并加盖公章报送实验与网络信息中心。

（三）安全事件事后处置包括：进一步总结事件教训，研判安全现状、排查安全隐患，进一步加强制度建设，提升安全防护能力。如涉及人为主观破坏的安全事件应继续配合公安部门和学校保卫部门开展调查。

第九条 预警类信息的报告与处置。各单位要按时、按要求完成国家、地方有关信息安全部门以及学校实验与网络信息中心等部门通报的预警类信息的处置工作，并形成书面报告，报送实验与网络信息中心。

第四章 制度与问责

第十条 人事变更报告。为保障联络通畅，各单位的信息技

术安全工作主管领导、联络员、联络方式发生变更的，应及时向网络与信息化办公室报备。

第十一条 相关机制。各单位应根据实际建立本单位的值守制度，做到安全事件早预警、早发现、早报告、早控制、早解决。各单位应建立健全本单位安全事件应急处置机制，制定安全事件应急流程，定期组织应急演练。

第十二条 整改原则。发生安全事件后，要认真做好整改落实工作，坚持做到事故原因不查清不放过、整改措施未落实不放过、责任人员未受到教育或处理不放过，尽力杜绝类似事件再次发生。

第十三条 问责制度。各单位应按照流程及时、如实地报告和妥善处置安全事件。如有瞒报、缓报、处置和整改不力等情况，网络与信息化管理办公室将对相关单位进行约谈或通报；情况严重的，根据《聊城大学网络与信息安全管理办法》的责任追究条款问责处理。

第五章 附则

第十四条 本流程自发布之日起施行，由实验与网络信息中心负责解释。

附件：(1)信息技术安全事件分类

(2) 聊城大学信息技术安全事件情况报告

(3) 聊城大学信息技术安全事件整改报告

(4) 网络安全事件报告及处理流程图

附件(1)

信息安全事件分类

《信息安全事件分类分级指南》（GB/Z 20986-2007）根据信息技术安全事件的起因、表现、结果等，将信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件和其他信息安全事件 6 个基本分类，每个基本分类分别包括若干个子类。

1.有害程序事件

有害程序事件是指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件。有害程序事件包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件等 7 个子类。

2.网络攻击事件

网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。网络攻击事件包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件等 7 个子类。

3.信息破坏事件

信息破坏事件是指通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。信息破坏事件包括信息篡改事件、信息假冒事件、信息泄漏事件、信 息窃取事件、信息丢失事件和其它信息破坏事件等 6 个子类。

4. 设备设施故障

设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件，以及人为的使用非技术手段有意或无意的造成信息系统破坏而导致的信息安全事件。设备设施故障包括软硬件自身故障、外围保障设施故障、人为破坏事故和其它设备设施故障等 4 个子类。

5. 灾害性事件

灾害性事件是指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件。灾害性事件包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的信息安全事件。

6. 其他事件

其他事件是指不能归为以上基本分类的信息技术安全事件。

附件 (2)

聊城大学网络信息技术安全事件情况报告

单位名称（公章）：　　事发时间：　年　月　日　分

联系人姓名		移动电话	
		电子邮箱	
事件分类	☐ 有害程序事件　☐ 网络攻击事件 ☐ 信息破坏事件　☐ 设备设施故障 ☐ 灾害事件　☐其他		
事件概况			
信息系统基本情况（如涉及请填写）	1. 系统名称： 2. 系统网址和 IP 地址： 3. 系统主管单位/部门： 4. 系统运维单位/部门： 5. 系统使用单位/部门： 6. 系统主要用途： 7. 是否定级 ☐是 ☐否，所定级别： 8. 是否备案 ☐是 ☐否，备案号： 9. 是否测评 ☐是 ☐否 10. 是否整改 ☐是 ☐否		
事件发现与处置的简要经过			

事件初步估计的危害和影响	
事件原因初步分析	
已采取的应急措施	
是否需要应急支援及需支援事项	
安全负责人意见	签名：　　年　　月　　日
主要负责人意见	签名：　　年　　月　　日

附件(3)

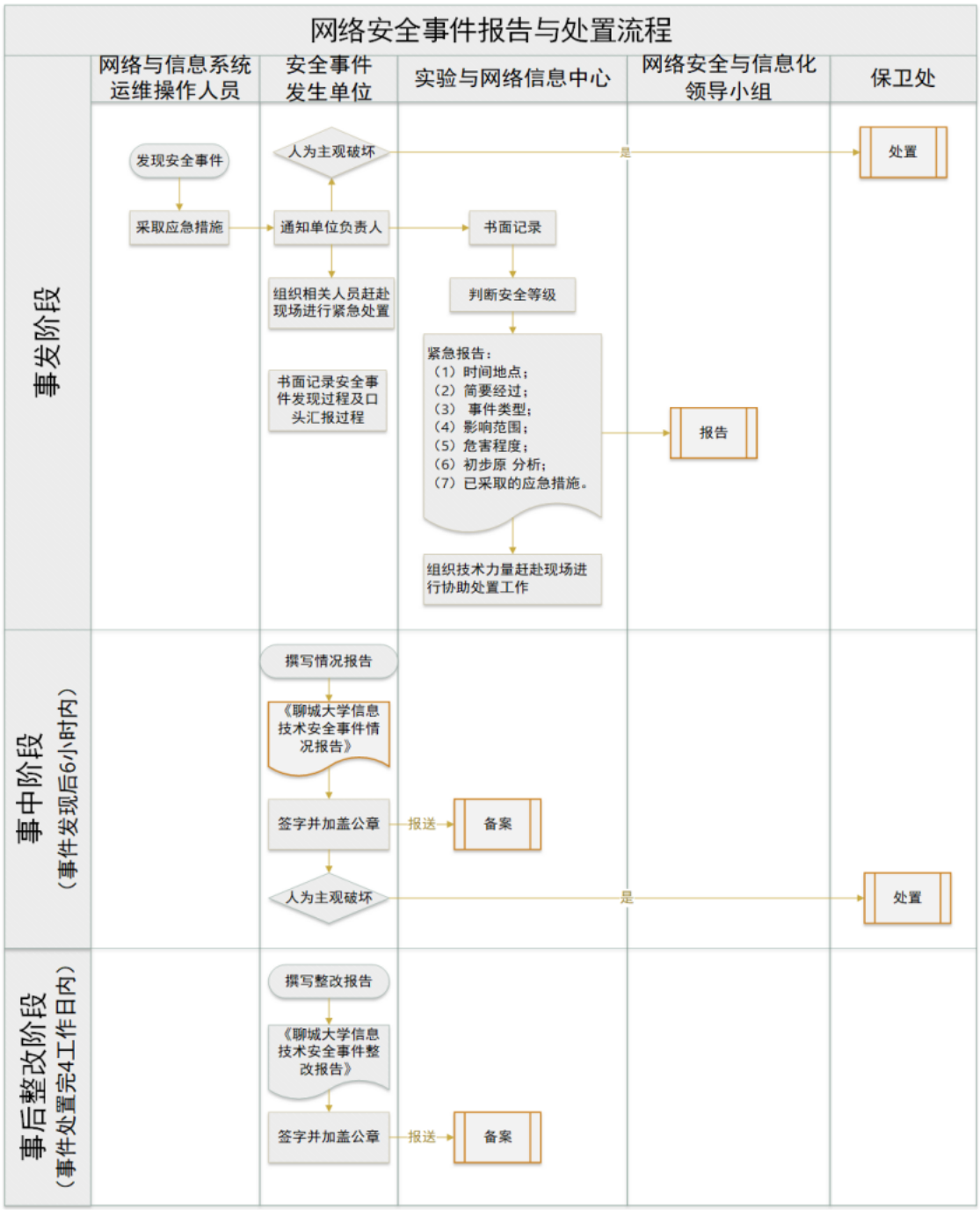
聊城大学信息安全事件整改报告

单位名称（公章）：　　报告时间：年　月　日

联系人姓名		移动电话	
		电子邮箱	
事件分类	☐ 有害程序事件　☐ 网络攻击事件 ☐ 信息破坏事件　☐ 设备设施故障 ☐ 灾害事件　☐其他		
事件概况			
信息系统基本情况（如涉及请填写）	1. 系统名称： 2. 系统网址和 IP 地址： 3. 系统主管单位/部门： 4. 系统运维单位/部门： 5. 系统使用单位/部门： 6. 系统主要用途： 7. 是否定级 ☐是 ☐否，所定级别： 8. 是否备案 ☐是 ☐否，备案号： 9. 是否测评 ☐是 ☐否 10. 是否整改 ☐是 ☐否		

事件发生的最终判定原因（可加页附文字、图片以及其他文件）	
事件的影响与恢复情况	
事件的安全整改措施	
存在问题及建议	
安全负责人意见	签名：　　年　　月　　日
主要负责人意见	签名：　　年　　月　　日

附件（4）


网络安全事件报告与处置流程
网络与信息系统运维操作人员
安全事件发生单位
实验与网络信息中心
网络安全与信息化领导小组
保卫处
事发阶段
发现安全事件
采取应急措施
人为主观破坏
是
处置
通知单位负责人
书面记录
组织相关人员赶赴现场进行紧急处置
判断安全等级
书面记录安全事件发现过程及口头汇报过程
紧急报告：
（1）时间地点；
（2）简要经过；
（3） 事件类型；
（4）影响范围；
（5）危害程度；
（6）初步原 分析；
（7）已采取的应急措施。
报告
组织技术力量赶赴现场进行协助处置工作
事中阶段
（事件发现后6小时内）
撰写情况报告
《聊城大学信息技术安全事件情况报告》
签字并加盖公章
报送
备案
人为主观破坏
是
处置
事后整改阶段
（事件处置完4工作日内）
撰写整改报告
《聊城大学信息技术安全事件整改报告》
签字并加盖公章
报送
备案

附件 2

聊城大学信息系统安全漏洞整改管理细则

第一条 为规范信息系统安全漏洞整改工作，提高我校信息系统安全防护能力，降低网络安全风险，维护安全稳定的校园网络环境和正常工作秩序，根据《中华人民共和国网络安全法》《关于加强教育行业网络与信息安全工作的指导意见》《教育部办公厅关于启动信息系统安全监测的通知》等法律法规与文件精神，结合学校实际，制定本管理细则。

第二条 信息系统安全漏洞定义。根据《信息技术安全漏洞划分指南》[GB/T 30279-2013，以下简称《指南》，摘录部分见附件(1)]，本细则所称的信息系统安全漏洞是指信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷。这些缺陷以不同形式存在于信息系统的各个层次和环节之中，一旦被恶意主体所利用，会对信息系统的安全造成损害，从而影响信息系统的正常运行。

第三条 适用范围。本细则适用于我校各类信息系统（包含承载其运行的服务器操作系统、中间件软件和数据库管理系统等）以及校园网基础网络平台（网络交换机、网络路由器、服务器等）安全漏洞的发现、处置与整改。

第四条 责任体系。根据《中华人民共和国网络安全法》第

二十五条要求，学校应当及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。

（一）实验与网络信息中心负责学校各类信息系统安全漏洞信息情况的通知、应急处置、整改督促和复查复测等；负责学校数据中心内的服务器操作系统、中间件系统和数据库系统级别信息安全漏洞技术处置；校内其他各业务系统信息安全漏洞的扫描和技术支持。

（二）学校各单位负责本单位所管理的各类信息系统的信息安全漏洞自查、堵塞整改和处置情况报告等。

第五条 信息系统安全漏洞等级划分。根据《指南》，信息系统安全漏洞等级划分要素包括访问路径、利用复杂程度和影响程度三方面。根据危害程度从低至高，将信息安全漏洞划分为四个等级，依次为低危、中危、高危和超危。

根据相关机构或相关安全软件有明确定义安全等级的漏洞按照其标准确定等级；没有明确级别的，实验与网络信息中心安全管理员负责对信息系统安全漏洞的危险等级进行评估，确定漏洞的危害等级。对不同等级的信息安全漏洞，将采取不同的处置措施。

第六条 信息系统安全漏洞监测发现。学校网络安全威胁与信息系统安全漏洞信息来源主要包含上级有关部门或其他机构通报的信息系统安全漏洞；学校通过网络安全扫描发现的信息系统安全漏洞；信息系统管理员自己发现的信息系统安全漏洞。

学校网络与信息化办公室负责建立多方协作的信息共享机制，及时收集掌握网络安全威胁与信息系统安全漏洞监测信息。通过教育系统网络安全工作管理平台、教育行业漏洞报告平台、山东教育通用工作平台、山东省网信办、聊城市网信办、聊城市网安支队、中国教育和科研网山东赛尔公司等网络安全职能和服务部门提供的报告，汇聚漏洞、病毒、网络攻击等网络安全威胁信息，实现安全威胁信息的收集、校验、发布、跟踪。各单位加强对本单位网络和信息系统（网站）的网络安全威胁监测，对发生的威胁及时进行处置和上报。

第七条 超危与高危信息安全漏洞处置。对于超危和高危信息安全漏洞，实验与网络信息中心应立刻采取断网措施，根据信息系统的登记备案信息，向信息系统责任单位发出《聊城大学信息系统安全漏洞整改通知》（简称“整改通知”）。

第八条 中危与低危信息安全漏洞处置。对于中危和低危信息安全漏洞，实验与网络信息中心采取限制访问范围的技术措施，发送电子邮件并电话通知责任单位，限定三个工作日内完成整改。

第九条 信息系统安全漏洞整改。信息系统责任单位收到整改通知后，应立即整改。整改完成后，填写《聊城大学信息系统安全漏洞整改报告》[以下简称整改报告，具体内容要求和格式见附件(2)]。整改报告的主要内容包括：信息系统基本信息、漏洞说明、整改情况说明、整改结果及单位审核，整改报告由本单

位主要负责人审核，签字并加盖公章后报送实验与网络信息中心。

实验与网络信息中心根据整改处置情况填写《网络安全事件与漏洞隐患处置情况反馈表》[附件(3)]向有关部门反馈整改结果。

第十条 整改原则与目标。各单位收到整改通知后，要查清信息系统安全漏洞原因，认真做好整改工作，切实有效清除出现的网络信息安全漏洞与隐患，杜绝类似信息安全漏洞再次发生。

第十一条 整改结果核验。责任单位提交整改报告后，实验与网络信息中心对信息系统漏洞整改结果进行核验，确认整改完成后，才能恢复正常网络连接。对于未按期完成整改的单位，继续采取断网、限网的措施，同时向责任单位发出重新整改通知。

第十二条 档案材料整理。收集整理漏洞扫描日报、周报、月报等资料信息，及时通报发布给工作组；起草、下达整改通知书，上报经过核查的整改情况报告；分类，分时，规范建立网络安全档案材料。

第十三条 人事变更报告。为保障联络通畅，各单位分管信息化负责人、信息化联络员、信息系统负责人、联络方式等发生变更的，应及时向实验与网络信息中心报备。

第十四条 责任追究。各单位应按照本细则及时完成信息系统安全漏洞整改。如有接到整改通知后不整改或整改不力等情况的，学校将进行通报；情节严重的，根据《聊城大学网络与信息

安全管理办法》的责任追究条款进行问责处理。

第十五条 本细则自发布之日起施行，由实验与网络信息中心负责解释。

附件(1)：信息安全技术安全漏洞等级划分指南

附件(2)：聊城大学网络信息安全漏洞整改报告

附件(3)：网络安全事件或漏洞隐患处置情况反馈表

附件(1)

信息安全技术安全漏洞等级划分指南

《信息安全技术安全漏洞等级划分指南》(GB/T 30279-2013)规定了信息系统安全漏洞(简称安全漏洞)的等级划分要素和危害程度级别。

一、安全漏洞等级划分要素

安全漏洞等级划分要素包括访问路径、利用复杂度和影响程度等三方面。

访问路径的赋值包括本地、邻接和远程，通常可被远程利用的安全漏洞危害程度高于可被邻接利用的安全漏洞，可被本地利用的安全漏洞次之。

利用复杂度的赋值包括简单和复杂，通常利用复杂度为简单的安全漏洞危害程度高。

影响程度的赋值包括完全、部分、轻微和无，通常影响程度为完全的安全漏洞危害程度高于影响程度为部分的安全漏洞，影响程度为轻微的安全漏洞次之，影响程度为无的安全漏洞可被忽略。影响程度的赋值由安全漏洞对目标的保密性、完整性和可用性三个方面的影响共同导出。

二、安全漏洞等级划分

安全漏洞的危害程度从低至高依次为低危、中危、高危和超危，具体危害等级划分方法见表1。

表 1：

安全漏洞危害等级划分表

序号	访问路径	利用复杂度	影响程度	安全漏洞等级
1	远程	简单	完全	超危
2	远程	简单	部分	高危
3	远程	复杂	完全	高危
4	邻接	简单	完全	高危
5	邻接	复杂	完全	高危
6	本地	简单	完全	高危
7	远程	简单	轻微	中危
8	远程	复杂	部分	中危
9	邻接	简单	部分	中危
10	本地	简单	部分	中危
11	本地	复杂	完全	中危
12	远程	复杂	轻微	低危
13	邻接	简单	轻微	低危
14	邻接	复杂	部分	低危
15	邻接	复杂	轻微	低危
16	本地	简单	轻微	低危
17	本地	复杂	部分	低危
18	本地	复杂	轻微	低危

附件(2)

聊城大学网络信息安全漏洞整改报告

单位名称		联 系 人	
网站（系统）名称		电子邮箱	
单位所属信息系统或网站存在的安全漏洞隐患			
整改情况说明			
整改结果	□完成　　□部分完成　　□未完成		
备注	如未完全整改或有其他说明，请在此备注。		
单位审核	单位负责人签字： （单位盖章）　　年 月 日		

请同时提交电子版和纸质**盖章（扫描版）**图片各一份，发送至邮箱：nicsec@lcu.edu.cn。

附件(3)

网络安全事件或漏洞隐患处置情况反馈表

<table>
<tr><td colspan="2">*事件名称</td><td colspan="3"></td></tr>
<tr><td colspan="2">*事件类型</td><td></td><td>*危害等级</td><td>中危</td></tr>
<tr><td colspan="2">*事件描述</td><td colspan="3"></td></tr>
<tr><td colspan="2">*相关网站或信息系统名称</td><td></td><td>*专线接入服务商</td><td></td></tr>
<tr><td colspan="2">*域名 URL</td><td></td><td>*IP 地址</td><td></td></tr>
<tr><td colspan="2">*单位名称</td><td colspan="3"></td></tr>
<tr><td colspan="2">*负责人</td><td></td><td>*联系电话</td><td></td></tr>
<tr><td colspan="2">*处置人</td><td></td><td>*联系电话</td><td></td></tr>
<tr><td rowspan="5">总结报告</td><td>*事件发生原因</td><td colspan="3">具体发生原因（如 SQL 注入、弱口令、目录遍历、任意文件下载与查看、文件包含、越权访问、远程命令执行、文件上传、反序列化等）及攻击者植入木马的方式（如下载恶意程序、FTP 上传、Webshell 上传、人员违规接入外接设备等）</td></tr>
<tr><td>*事件经过及处理</td><td colspan="3"></td></tr>
<tr><td>*今后防范措施</td><td colspan="3"></td></tr>
<tr><td>*网站是否恢复正常</td><td></td><td>*网站恢复时间</td><td></td></tr>
<tr><td>是否保留或发现作案软件</td><td></td><td>是否有网站日志</td><td></td></tr>
<tr><td colspan="3">涉事单位网络安全分管领导：（签字）

涉事单位：（盖章）</td><td colspan="3">实验与网络信息中心：（盖章）</td></tr>
</table>

注：*为必填项