

杭州师范大学文件

杭师大发〔2023〕8号

杭州师范大学关于印发网络与信息安全 管理办法的通知

各学院（部）、部门：

现将《杭州师范大学网络与信息安全管理办法》印发给你们，请认真遵照执行。

杭州师范大学

2023年5月31日

杭州师范大学网络与信息安全管理办法

第一章 总则

第一条 为保障学校网络安全与信息化建设工作规范有序，确保校园网络环境安全稳定，根据《中华人民共和国网络安全法》等相关法律法规要求，结合学校工作实际，制定本办法。

第二条 本办法所称的网络与信息安全管理是指学校采取技术、管理等措施，保护学校网络与信息化建设基础设施、信息系统及信息数据的安全，使其不受到破坏、篡改、泄露等。

第三条 网络安全工作是学校信息化建设的重要工作，校内各单位应通力合作，在人员、资金、技术、设备等方面提供充足的支持与保障。

第二章 组织机构及职责分工

第四条 学校网络安全和信息化工作领导小组为学校网络安全工作的领导机构，负责学校网络安全工作的战略决策，统筹指导学校网络信息安全建设，研究处理重大网络信息安全事件。领导小组下设办公室，办公室设在信息中心，负责学校网络信息安全的管理和协调工作。

第五条 信息中心负责学校网络与信息系统运行的日常监管，保障学校网络和相关信息系统的正常运行；保存网络运行

日志，配合调查取证；负责入网单位和个人办理入网登记手续，签署相应的安全责任书。

第六条 党委宣传部负责网络信息内容的安全监管，负责校园网站准入审核，网络舆情信息的监控和管理，开展网上疏导和正面宣传，做好对外宣传工作。

第七条 党委保卫部（保卫处）负责对网络违规行为进行调查、取证、处理，根据相关证据及事态影响或破坏程度，对违规者按照有关规定进行处理。

第八条 各学院（部）、部门（以下简称各二级单位）应按照“谁主管谁负责、谁主办谁负责、谁运行谁负责、谁使用谁负责”的原则，负责本单位主管使用的主机、信息系统及数据、网站及新媒体平台的安全管理工作，建立本单位网络安全管理制度和应急处置预案。

第九条 师生应主动学习网络安全相关知识，培养科学健康用网习惯，配合做好宣传工作，积极参与网络安全的建设和管理，遵守学校网络安全管理的相关规定，不得从事危害国家安全、泄露国家秘密、侵犯知识产权、传播不良信息、破坏计算机信息系统等违法犯罪活动。

第三章 校园网络及基础设施安全管理

第十条 杭州师范大学校园网络（以下简称“校园网”）基础设施是指承载校园网正常运行的光纤通信线路、弱电设施设备、网络设备等基础设施设备。

第十一条 各二级单位及个人不得擅自建设、拆卸、更改、损毁、挪用校园网及相关基础设施，不得改变网络结构，私接外网出口。

第十二条 校园网主要服务于学校教学、科研及校务管理等，严禁利用校园网开展商业宣传等未经许可的其它活动。

第十三条 校园网入网实行实名认证，除专用机房、实验室等特殊场所经信息中心备案外，校园网用户必须通过学校统一身份认证接入校园网，未经登记不得以任何方式私接校园网，严禁盗用其他用户上网账号使用校园网。

第十四条 校园网用户应文明上网，规范网络行为，并做好个人信息安全防范。严禁利用校园网从事入侵、破坏、窃取、修改存储设备和计算机信息系统中的数据资源、配置参数等，不得利用校园网以任何形式攻击校内外网络。

第十五条 信息中心对内网 IP、公网 IP 和域名的使用进行统一规划、分配和管理，并定期审查其使用情况，有权禁用涉嫌违法违规及存在安全隐患的 IP 和域名。

第十六条 信息中心以保障学校教学与科研的稳定顺畅为首要目标，有权根据运行情况对校园网进行适时调整与优化，对流量过高、挤占带宽资源严重的流量及应用进行限时、限速或封停操作。

第十七条 信息中心负责对校园网的安全进行监测管理，依法利用上网行为审计系统，对网站、软件、邮件等应用的违

规上网行为进行审计，及时发现并追溯违法违规行为；对办公协同应用进行敏感信息审计，追溯学校泄密源头。对散布病毒、木马、违规使用校园网等危害校园网安全行为的，信息中心有权封停计算机或其使用人账号。

第四章 物理安全管理

第十八条 物理安全管理是指通过技术和管理手段，保护校园服务器机房网络设备、服务器存储设备、动力环境设备等硬件设施免遭自然灾害（地震、水灾、火灾、爆炸等环境事故）和人为操作错误或失误而造成的破坏。

第十九条 单独设立服务器机房的二级单位应建立机房安全管理制度，严控机房进出人员，规范机房各项管理操作。

第二十条 学校电力维护部门应确保机房用电不间断，若确实须停电维护的，须提前通知后方可实施。

第二十一条 未经信息中心允许，任何单位或个人不得擅自对弱电间设备设施和校园通信线路进行操作。增加、安装、调试、更换、拆除弱电间的设备设施或通信线路时，必须做好相关操作记录，并向信息中心提前报备。

第二十二条 机房所属单位应做好机房动力环境工作，要有防火、防盗、防雷、防电磁防护、恒温、恒湿等安全措施，定期巡检，做好记录，发现异常及时处理，避免安全事故发生。

第五章 主机安全管理

第二十三条 主机安全管理是指通过一系列安全技术和安

全管理措施，保证服务器、存储等主机设备（包括虚拟主机）数据存储和处理的保密性、完整性、可用性，以及主机硬件、固件和系统软件的自身安全。

第二十四条 各二级单位应指派专人负责本单位各类主机的安全维护和管理，定期对各类主机进行安全检查、漏洞修复和病毒扫描，及时发现、解决软硬件系统故障。

第二十五条 各二级单位可向信息中心申请主机托管服务。托管的主机原则上只允许对外开放以 web 服务为主的用于教学、科研和管理的互联网基本信息服务，以及校园内部使用的业务系统等。托管主机达到报废年限且不再使用的，应及时关停并移出托管机房。

第二十六条 托管主机的软硬件维护以及内部系统、软件的安装及安全管理由托管单位自行负责。

第二十七条 信息中心有权对托管主机进行必要的监控，以保证学校网络线路的正常运行。若托管单位违反校内网络安全相关制度，或托管服务器出现中毒、被黑客侵入等异常情况时，信息中心有权终止服务器运行的权利。

第六章 信息系统安全管理

第二十八条 学校信息系统建设使用应遵循校内网络安全相关制度、技术、规范和流程开展。

第二十九条 各二级单位应定期对本单位使用的信息系统和网站的安全状况、安全保护制度及措施的落实情况进行自查、

修复等，并配合有关部门的信息安全检查、信息内容检查、保密检查与审批等。每年将本单位信息系统和网站等信息提交信息中心备案，内容包括：系统名称、域名、IP 地址、使用单位、系统管理员及联系方式等。

第三十条 各单位建设的面向在校师生开放的各类信息系统应使用学校统一身份认证。

第三十一条 信息中心定期对校内的信息系统进行安全监测，对长期无人管理、内容不做更新、存在安全隐患、管理制度缺失或无固定的管理和维护人员的信息系统，有权予以清理和关闭。

第三十二条 各二级单位应落实信息系统安全等级保护制度。按照要求开展信息系统定级和备案工作。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。对于计算机信息系统安全状况未达到安全保护等级要求的，相应系统主管的二级单位应及时整改。

第三十三条 涉密信息系统不得直接或者间接地与国际互联网或其它公共信息网络相联接，应当根据国家涉密信息分级保护管理规定和技术标准进行保护。

第三十四条 涉密人员的非密计算机如需联接外网，须申请审批，坚持“谁上网谁负责”的原则，做到涉密的信息不上网，上网的信息不涉密。

第七章 数据安全

第三十五条 本办法所涉及的数据是指各类信息系统所覆盖的相关业务数据，包括但不限于：信息门户、人事系统、学生管理系统、教务管理系统、研究生管理系统、科研系统以及其他各类信息系统产生的数据。

第三十六条 信息中心是学校数据资产的统筹管理部门，负责主数据中心、数据仓库平台、数据共享平台的安全管理，并规范数据服务流程，确保数据流向清晰，实现数据可控、可管、可查。

第三十七条 数据生产部门为权威数据的单一来源部门，负责数据收集、维护、使用、备份、归档等全程安全，需遵循学校信息标准规范及数据服务规范。

第三十八条 数据使用部门根据实际需求向数据生产部门提出申请，获得批准后，信息中心或数据生产部门向数据使用部门开放数据接口。数据使用部门有义务和责任保护所获得数据的安全，未经允许，不得将数据用于申请使用外的其他用途。

第三十九条 未经批准，任何单位和个人不得擅自提供信息系统产生的内部数据。对于非法泄露或擅自提供数据的单位或个人，依照相关法律法规予以处理。

第八章 内容安全

第四十条 任何单位和个人必须遵守《中华人民共和国计算机信息网络国际互联网络管理暂行规定》、国家有关法律法规和学校的有关管理规定，严格执行信息安全保密制度，并对所

提供和发布的信息负责。

第四十一条 任何单位和个人不得利用网络制作、复制、传播下列信息：

- （一）煽动抗拒、破坏宪法和法律、法规实施的；
- （二）煽动颠覆国家政权，推翻社会主义制度的；
- （三）煽动分裂国家、破坏国家统一的；
- （四）煽动民族仇恨、民族歧视，破坏民族团结的；
- （五）煽动非法集会、结社、游行、示威、聚众扰乱社会秩序的；
- （六）捏造或者歪曲事实，散布谣言，扰乱社会秩序的；
- （七）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；
- （八）公然侮辱他人或者捏造事实诽谤他人的；
- （九）损害国家荣誉和利益的；
- （十）以非法民间组织名义组织活动的；
- （十一）损害杭州师范大学荣誉和利益的；
- （十二）其他违反宪法和法律、行政法规的。

第四十二条 各二级单位须严格遵循内容审核机制，规范信息发布审批流程，加强信息安全监控，防止出现内容篡改等安全事故。

第九章 检测预警与网络安全事件的处置

第四十三条 信息中心不定期对校内各类信息系统、网络、

其他网络相关设备开展网络安全检测工作，并发布检测报告。各单位应根据《杭州师范大学网络安全漏洞整改流程》(附件 1)，及时落实网络安全自查和问题修复，避免网络安全事件发生。

第四十四条 校内网络安全事件的处理由信息中心协同有关部门负责组织实施，按照《杭州师范大学信息技术安全事件报告与处置流程》(附件 2) 进行分级、分类处理。安全事件相关单位及人员应积极配合，认真落实网络安全事件处置相关工作。为避免安全事件不良影响扩大，信息中心有权直接对安全事件相关的网络及信息系统进行断网、停止服务等应急处理。

第四十五条 各二级单位应制定网络安全应急预案，定期开展应急演练，提高网络安全事件处置能力，发现网络安全问题应及时向信息中心报告并进行必要的应急处理。

第四十六条 信息中心负责组织校内网络安全处置应急演练，相关部门应积极参与，通过演练提高校内网络安全事件处置能力。

第十章 责任追究

第四十七条 网络安全事件的责任认定，由信息中心提交校网络安全和信息化工作领导小组讨论后，经学校相关会议审议处理。

第四十八条 对于违反法律、法规，造成国家、学校和个人损失的单位或个人，学校将依据《中华人民共和国网络安全法》等法律法规配合公安、网信等主管部门进行处理。

第十一章 附则

第四十九条 本办法由信息中心负责解释，自印发之日起施行。

附件 1

杭州师范大学网络安全漏洞整改流程

第一条 为加强我校网络安全保障能力，规范信息技术安全漏洞整改流程，降低网络安全风险，维护正常工作秩序和营造健康的网络环境，根据《中华人民共和国网络安全法》《信息安全技术网络安全漏洞分类分级指南》(GBT30279—2020)等法律法规，结合学校实际，制定本流程。

第二条 网络安全漏洞的定义。根据《信息安全技术网络安全漏洞分类分级指南》(GBT30279—2020，以下简称《指南》)，本流程中所称的网络安全漏洞(以下简称安全漏洞)是指计算机信息系统在需求、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计算机信息系统的各个层次和环节之中，一旦被恶意主体所利用，会对计算机信息系统的安全造成损害，从而影响计算机信息系统的正常运行。

第三条 适用范围。本流程适用于我校各类网站、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)以及网络交换机、网络路由器、服务器、网络打印机、视频监控、大屏发布等其他计算机信息系统(以下均统称为信息系统)安全漏洞的发现、处置与整改。

第四条 责任体系。根据《网络安全法》第二十五条要求，

网络运营者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。

信息中心负责学校各类网络安全漏洞的通知、应急处置和整改督促等；负责学校核心数据中心内的虚拟服务器的操作系统、中间件系统和数据库系统级别网络安全漏洞技术处置；负责学校网站群平台的操作系统及平台级网络安全漏洞的处置；负责校内其他各系统网络安全漏洞的扫描和技术支持。

学校各单位负责本单位自行搭建服务器及所管理的各类信息系统的网络安全漏洞自查、堵塞整改、复查复测和处置情况报告等。

第五条 网络安全漏洞等级划分。根据《指南》依据危害程度从低至高，将网络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，信息中心安全管理员负责对网络安全漏洞的危险等级进行评估，确定漏洞的危害等级。对不同等级的网络安全漏洞，将采取不同的处置措施。

第六条 网络安全漏洞发现。学校网络安全漏洞主要包含：(1)上级有关部门或其他机构通报的网络安全漏洞；(2)学校通过网络安全扫描发现的网络安全漏洞；(3)信息系统管理员自己发现的网络安全漏洞；(4)其他途径获取的网络安全漏洞。

第七条 网络安全漏洞的处置。

1. 超危与高危网络安全漏洞的处置。对于超危和高危网络安全漏洞，信息中心应进行风险评估，根据需要采取断网措施。信息中心根据信息系统的登记备案信息，向信息系统责任单位通过学校网络安全预警和处置平台，发出《杭州师范大学网络安全风险隐患整改通知》（以下简称整改通知）并电话告知责任单位直接负责人。

2. 中危与低危网络安全漏洞的处置。对于中危和低危网络安全漏洞，信息中心通过学校网络安全预警和处置平台，发出整改通知并通知责任单位进行整改，限定十个工作日内完成整改。单位整改完成后，信息中心对整改结果进行检查，确认是否已完成整改。对于未按期完成整改的单位，采取断网措施，同时再次向责任单位发出整改通知。

第八条 网络安全漏洞整改。信息系统责任单位收到整改通知后，由单位直接责任人在限定时间内完成整改。整改完成后，通过学校网络安全预警和处置平台进行反馈。

第九条 整改落实机制。各单位收到整改通知后，要认真做好整改工作，坚持做到查清网络安全漏洞原因、按时整改，尽力杜绝类似网络安全漏洞再次发生。

第十条 整改结果验证。责任单位提交整改报告后，信息中心对信息系统进行整改结果检测，确认整改完成后才能开放网络连接。

第十一条 责任追究。各单位应按照流程及时地完成网络

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，信息中心将进行通报。因漏洞造成网络安全事故的，根据学校相关规定，对相关责任人问责处理。

第十二条 本流程自印发之日起施行，由信息中心负责解释。

附件 2

杭州师范大学信息技术安全事件报告与 处置流程

为加强我校网络安全工作，及时处置信息技术安全事件，协调相关力量做好应急响应处理，降低安全事件带来的损失与影响，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》（教技厅函〔2014〕75号）等文件精神，结合学校实际，制定本流程。

第一章 总则

第一条 网络安全事件的定义。根据《信息安全事件分类分级指南》（GB/20986-2007，以下简称《指南》，摘录部分见附件 2.1），本流程中所称的网络安全事件（以下简称安全事件）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、灾害事件和其他信息安全事件，详见附件 2.1。

第二条 适用范围。本流程适用于我校各单位发生的网络安全事件的报告与处置工作。

第二章 安全事件等级划分与判定

第三条 安全事件等级划分。根据《指南》，将安全事件划分为四个等级：特别重大事件（I 级）、重大事件（II 级）、较大事

件(Ⅲ级)和一般事件(Ⅳ级),详见附件 2.1。

第四条 安全事件判定。一旦发生安全事件,应根据《指南》,视信息系统重要程度、损失情况以及对工作和社会造成的影响,由主办部门迅速初步判定安全事件等级。信息中心在接到报告后,根据事件情况,进一步做出判定。必要时,信息中心组织专家组进行判定或报告学校网络安全与信息化建设领导小组判定。

第三章 安全事件的报告与处置

第五条 I至Ⅲ级信息安全事件的报告与处置。报告与处置分为三个步骤:事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置。

(一)事发紧急报告与处置

1. 网络与信息系统运维操作人员一旦发现安全事件,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,并报告本单位第一责任人和直接责任人。

2. 本单位第一责任人接到报告后,应立即组织相关人员赶赴现场进行紧急处置,同时以口头通讯的方式将相关情况通报至信息中心,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的,应同时报告学校保卫部门。

3. 信息中心接到报告后,应做好书面记录,并进一步判定安全事件等级,对确认属 I至Ⅲ级安全事件的,应报告网络安

全和信息化工作领导小组相关领导。

4. 紧急报告内容包括：(1) 时间地点；(2) 简要经过；(3) 事件类型与分级；(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。

5. 对确认属 I 至 III 级安全事件的，信息中心应立即组织相关技术力量赶赴现场进行协助处置工作。必要时联系属地公安机关做好相关取证和处置工作。

6. 相关单位应及时跟进事件发展情况，出现新的重大情况应及时补报。

(二) 事中情况报告与处置

1. 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 2.2。

2. 事中情况报告由单位直接责任人组织撰写，由本单位第一责任人审核后，签字并加盖公章报送信息中心。

3. 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，修复系统漏洞，恢复系统服务，尽可能减少安全事件对正常工作带来的影响。

(三) 事后整改报告与处置

1. 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 2.3。

2. 事后情况报告由单位直接责任人组织撰写，由本单位第一责任人审核后，签字并加盖公章报送信息中心。

3. 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。

第六条 一般安全事件(IV级)报告与处置。各单位发生一般安全事件,应及时、自主组织应急处置工作;需要信息中心协助的,联系信息中心予以协助。在事件处置完毕后6天内向信息中心报送整改报告,报告内容和格式见附件2.3。

第七条 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信息中心等部门通报的预警类信息的处置工作,并按要求形成书面报告,报送信息中心。

第四章 配套制度与问责

第八条 人员责任。各单位主要负责人是网络安全的第一责任人,网站管理员及相关负责人是直接责任人。

第九条 相关配套机制。各单位应建立健全本单位安全事件应急处置机制,制定安全事件应急预案,定期组织应急演练。

第十条 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,对相关责任人进行约谈或通报;情况严重的,根据学校相关规定问责。

第十一条 整改落实机制。发生I至III级安全事件后,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。

第五章 附则

第十二条 本流程自印发之日起施行，由信息中心负责解释。

附件 2.1

信息技术安全事件分类与等级划分

《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,将信息技术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;根据信息系统重要程度、系统损失和社会影响,将信息技术安全事件划分为4个等级。

一、信息技术安全事件分类

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

二、信息技术安全事件等级划分

1. 特别重大事件(I 级)

特别重大事件是指能够导致特别严重影响或破坏的信息安全事件,包括以下情况:

- (1) 会使特别重要信息系统遭受特别严重的系统损失;
- (2) 产生特别重大的社会影响。

2. 重大事件(II级)

重大事件是指能够导致严重影响或破坏的信息安全事件,包括以下情况:

- (1) 会使特别重要信息系统遭受严重的系统损失、或使重要信息系统遭受特别严重的系统损失;
- (2) 产生重大的社会影响。

3 较大事件(III级)

较大事件是指能够导致较严重影响或破坏的信息安全事件,包括以下情况:

- (1) 会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失、一般信息信息系统遭受特别严重的系统损失;
- (2) 产生较大的社会影响。

4. 一般事件(IV级)

一般事件是指不满足以上条件的信息安全事件,包括以下情况:

- (1) 会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失,一般信息系统遭受严重或严

重以下级别的系统损失；

(2) 产生一般的社会影响。

附件 2.2

杭州师范大学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 时 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		
事件分级	☐ I 级 ☐ II 级 ☐ III 级 ☐ IV 级		
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	
直接责任人 意见	签名：年 月 日
第一负责人 意见	签名：年 月 日

附件 2.3

杭州师范大学信息技术安全事件整改报告

单位名称(公章):

事发时间: 年 月 日 时 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		
事件分级	☐ I 级 ☐ II 级 ☐ III级 ☐ IV级		
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)			

