中共浙江大学委员会文件

党委发〔2017〕64 号

中共浙江大学委员会　浙江大学
印发《浙江大学网络与信息安全类突发
公共事件应急预案》的通知

纪委，各院级党委、直属党总支，党委各部门，各党工委，工会、团委，各学院（系），行政各部门，各校区管委会，直属各单位:

经学校研究决定，现将《浙江大学网络与信息安全类突发公共事件应急预案》印发给你们，请遵照执行。

中共浙江大学委员会　浙江大学

2017 年 8 月 8 日

浙江大学网络与信息安全类
突发公共事件应急预案

1 总则

1.1 编制目的

建立健全浙江大学网络与信息安全类突发公共事件应急工作机制，提高应对网络与信息安全类突发公共事件的能力，预防和减少网络与信息安全类突发公共事件造成的损失和危害，维护学校的安全和稳定。

1.2 编制依据

根据《中华人民共和国突发事件应对法》、《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网安全保护管理办法》、《教育系统网络与信息安全类突发公共事件应急预案》（教思政〔2009〕13号）、《教育部办公厅关于信息技术安全事件报告与处置流程（试行）》(教技厅函〔2014〕75号)、《浙江省教育厅关于加强全省教育系统网络与信息安全管理的意见》（浙教电〔2003〕230 号）、《浙江大学突发公共事件总体应急预案》(党委发〔2014〕33号)，结合我校网络与信息工作实际，制订本应急预案。

1.3 适用范围

本预案适用于学校应对网络与信息安全类突发公共事件的

应对处置工作。按照《教育系统网络与信息安全类突发公共事件应急预案》规定，本预案所指的网络与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、信息内容安全事件、设备设施故障和灾害性事件。

1.3.1 有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

1.3.2 网络攻击事件分为拒绝服务攻击事件、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。

1.3.3 信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

1.3.4 信息内容安全事件是指通过网络传播法律法规禁止的信息，组织非法串联、煽动集会游行或炒作敏感问题并危害校园安全、学校稳定和师生权益的事件。

1.3.5 设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

1.3.6 灾害性事件是指由自然灾害等其他突发事件导致的网络与信息安全事件。

1.4 工作原则

1.4.1 统一指挥，快速反应

学校突发公共事件应急处置指挥中心（以下简称校指挥中心），负责统一指挥、协调学校内各类突发公共事件的应急处置工作。校网络与信息类突发事件应对处置工作组（以下简称校应对处置工作组）负责学校全局性网络与信息安全类突发事件的应急处置工作。建立健全处置学校全局性网络与信息安全类突发公共事件的快速反应机制，确保预警、发现、报告、指挥、处置等环节的紧密衔接，做到快速反应，正确应对，果断处置，防止事态升级和蔓延扩大。

1.4.2 明确责任，分级负责

按照“谁主管、谁负责”的原则，加强网络与信息安全管理，认真落实各项安全管理制度和措施。加强网络与信息安全的宣传和教育，进一步提高师生的信息安全意识。各部门、单位、学院（系）（以下统称各单位）应根据本预案的标准，建立本单位的应急处置预案，并加强技术储备、规范应急处置措施，树立常备不懈的观念，定期进行预案演练，确保应急预案切实可行。

1.4.3 积极防御，综合防范

立足安全防护，加强预警，重点保护关系学校稳定的重要网络和信息系统；从预防、监控、应急处理、应急保障和打击不法行为等环节，在管理、技术、宣传等方面，采取多种措施，充分发挥各方面的作用，构筑我校网络与信息安全保障体系。

1.4.4 系统联动，密切协同

发生突发公共事件后，各相关单位负责人要立即深入第一线，掌握情况，开展工作，控制局面。形成各单位系统联动、密切协同的处置工作格局。

1.4.5 依法办事，科学处置

在处置突发公共事件过程中，做到合情合理、依法办事，切实维护师生合法权益。处置工作要自觉维护法律法规的权威性和规章制度的严肃性，注意工作的方式方法，防止矛盾激化和事态扩大。根据事件发展情况，必要时要采取果断措施，坚决制止违法犯罪行为。

1.4.6 加强保障，重在建设

从法规、制度、组织、技术等方面全面加强保障措施。在经费保障和力量部署等方面加强软硬件建设，增强工作能力，提高工作效率。

2 事件分级

网络与信息安全突发公共事件分为三级：Ⅰ级(特别重大)、Ⅱ级(重大)、Ⅲ级(一般)。

2.1 特别重大事件(Ⅰ级)

符合下列情形之一的，为特别重大事件(Ⅰ级):

2.1.1 校园网内信息系统数据丢失或被窃取、篡改、假冒，或校园网全面中断，对学校安全和稳定构成特别严重威胁。

2.1.2 出现通过校园网传播反动信息、煽动性信息、涉密信

息、谣言等情况，对学校安全和稳定构成特别严重危害，引发学校大规模突发群体性事件，对学校教学、科研和生活秩序产生严重影响，教育教学活动无法正常进行，师生反映强烈并有过激行为的事件。

2.1.3 其他对学校安全和稳定构成特别严重威胁、造成特别严重影响的网络与信息安全事件。

2.2 重大事件(Ⅱ级)

符合下列情形之一且未达到特别重大网络与信息安全事件(Ⅰ级)的，为重大事件(Ⅱ级):

2.2.1 校园网内信息系统中的数据丢失或被窃取、篡改、假冒，或校园网在多个校区内大面积中断，对学校安全和稳定构成重大威胁。

2.2.2 出现通过校园网传播反动信息、煽动性信息、涉密信息、谣言等情况，对学校安全和稳定构成重大危害，引发学校突发群体性事件，对学校教学、科研和生活秩序产生较大影响，师生反映强烈的事件。

2.2.3 其他对学校安全和稳定构成重大威胁、造成重大影响的网络与信息安全事件。

2.3 一般事件(Ⅲ级)

除上述情形外，校园网内出现对学校安全和稳定构成一定威胁，对学校教学、科研和生活秩序产生一定影响的网络与信息安

全事件。

3 组织机构与职责

3.1 组织机构

校应对处置工作组办公室设在党委宣传部，涉及网络安全事项的日常工作由信息技术中心承担，涉及网络信息内容安全事项的日常工作由党委宣传部承担。

3.2 工作职责

3.2.1 校应对处置工作组职责

（1）在校指挥中心的领导下负责I级网络与信息安全类突发公共事件的紧急处置工作。

（2）负责II级网络与信息安全类突发公共事件的紧急处置工作，指导III级网络与信息安全类突发公共事件的处置工作。

（3）通过技术手段对校园网信息实施24小时监控。及时阻止重大有害信息在校园网上大面积传播，或校园网系统遭受大范围黑客攻击和计算机病毒扩散事件。

（4）及时处置和报告校园网遭受境内外严重攻击，以及其他影响校园网安全的事件。

在学校党委、行政的统一领导下，校应对处置工作组随时掌握事态发生、发展的情况，随时汇总、分析、上报情况，确保校园网络与信息安全，尽快平息事态，确保校园网络与信息安全。

3.2.2 校应对处置工作组成员单位职责

（1）党委宣传部负责网络舆情信息的监控和管理，开展网上舆论疏导及正面宣传、校内网络危害信息管控、校内论坛管理，并做好对外宣传工作。

（2）党委安全保卫部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。

（3）信息技术中心负责学校网络与信息系统的日常管理和维护，保障网络与信息系统的正常运行；保存网络运行日志，配合调查取证。根据校应急处置工作组的指示，隔离部分网络或相关主机。

（4）后勤管理处负责校园网络和信息系统的日常电力供应，确保交换机、服务器等设备的正常供电。

其他应急组织体系及工作职责按《浙江大学突发公共事件总体应急预案》相关条款执行。

4 预防预警

4.1 预防措施

学校各单位应做好网络与信息安全事件的风险评估和隐患排查工作，制订、完善相关应急预案，及时采取有效措施，避免和减少网络与信息安全事件的发生及其危害，全面做好以下预防措施：

4.1.1 加强教育引导

各单位要全面加强师生思想政治教育工作，掌握师生动态。按照早发现、早报告、早控制、早解决的要求，把问题解决在萌芽状态，把风险控制在一定范围内。

4.1.2 完善应急管理制度

各单位要建立严格的应急管理制度，负责制订应急预案、网络管理、机房管理、保密协议等规定，通过培训等手段不断提高管理人员的技术水平、责任意识和安全意识。

各单位网络信息安全主管领导、分管领导、信息安全员等发生人员变动或联络方式变更的，应及时报送校应对处置工作组办公室。

4.1.3 加强技术防范措施

各单位要建立安全、稳定的网络运行环境，加强网络与信息安全的防护措施，定期对校园网进行网络漏洞扫描，实时监测校园网和关键信息系统。要对机房、网络设备、服务器等设施定期开展安全检查，对发现安全漏洞和隐患的进行及时整改；在国际互联网上已建立网站的单位要实行网站的巡察制度，密切关注互联网信息动态，及时获取充分而准确的信息，跟踪研判，果断决策，迅速处置，最大程度地减少危害和影响。

各单位要建立严格的信息上网审查制度，有效阻止网上不良信息传播。建立 BBS 等交互式栏目实名制度。

4.2 监测预警

学校各单位和个人都有义务向学校有关单位、事发单位报告网络与信息安全事件及其隐患。网络与信息安全事件发生后，学校有关单位、事发单位在做好先期处置的同时，应立即组织研判，注意保存证据，向校应对处置工作组报告。

4.3 发布预警

网络与信息安全事件发生时，校应对处置工作组可根据事件的危害程度及时发布预警，直至事件警报解除。当其他地方出现安全事件或相关安全网站发布预警时，可根据重要程度向用户发布预警。

4.4 预警响应

学校各单位共同承担学校网络与信息安全监测工作。各单位要加强对本单位网络与信息系统安全状况的监测，做好应急处置的准备工作。

5 应急处置

5.1 应急响应

5.1.1 I级响应

出现Ⅰ级事件时，由校指挥中心发布并研究启动该级预案，统一领导和指挥全校的应急处置工作。根据事态发展，先期可由校指挥中心副总指挥组织处置，并将处置情况及时报总指挥。事态有进一步扩大趋势时，则由总指挥组织处置，必要时可商请上级有关部门、公安机关予以支持，处置情况应及时报上级有关部

门。

5.1.2 Ⅱ级响应

发生Ⅱ级事件时，校应对处置工作组发布并研究启动预案，并结合《浙江大学突发公共事件总体应急预案》迅速开展处置工作。

（1）启动指挥体系

①校应对处置工作组进入应急状态，履行应急处置工作职责。工作组成员保持24小时联络畅通。

②校应对处置工作组成员单位进入应急状态，在校应对处置工作组的统一领导、指挥、协调下，负责本部门的应急处置工作或支援保障工作。

③校应对处置工作组到位、处置人员进入现场后，立即按照职责分工，决定处置措施，向全校发出相应指令，负责安排全校性值班。

（2）掌握事件动态，跟踪事态发展。事发单位和成员单位及时将事态发展变化情况和处置进展情况报校应对处置工作组。根据事件实际影响，请示改变应急响应等级。

（3）决策部署。校应对处置工作组组织成员单位及时研究对策意见，进行决策部署。

（4）检查影响范围。各信息系统的主管单位立即全面了解主管的信息系统是否受到事件的波及或影响，并将有关情况及时报校应对处置工作组。

（5）及时通报情况。校应对处置工作组负责汇总上述有关情况，重大事项及时报校指挥中心。

（6）处置实施

①控制事态，防止蔓延。信息技术中心和事发单位采取技术措施，尽快控制事态，有针对性地加强防范，防止事件蔓延至其他信息系统。对于信息内容安全事件，党委宣传部和事发单位采取必要的管控措施，防止网上不良信息传播扩散。

②做好处置，消除隐患。信息技术中心和事发单位应根据事件发生原因，有针对性地采取措施，恢复受破坏信息系统正常运行。

③及时开展调查取证。事发单位在应急恢复过程中应尽量保留相关证据，对于人为破坏活动，党委安全保卫部负责组织开展侦查和调查工作，并及时向校应对处置工作组通报调查情况。

（7）信息发布。根据校应对处置工作组的意见，党委宣传部负责做好对外信息发布工作，对受影响的学校师生和公众进行解释、疏导。

5.1.3Ⅲ级响应

出现III级事件时，由事发单位发布并研究启动预案，按照本单位网络与信息安全预案开展应对处置工作，一旦发现有升级趋势时，及时将有关情况报校应对处置工作组；根据事件实际影响，请示改变应急响应等级；校应对处置工作组可根据需要或应有关单位的请求，派出工作组赴事发单位指导处置工作。

（1）跟踪报告事态发展。事发单位及时将事态发展变化情况和处置进展情况报校应对处置工作组。

（2）事发单位应采取技术措施，尽快控制事态，有针对性地加强防范，防止事件蔓延至其他信息系统。对于信息内容安全事件，事发单位应采取必要的管控措施，防止有害非法信息传播扩散。

（3）事发单位在应急恢复过程中应尽量保留相关证据，配合党委安全保卫部开展调查取证工作。

5.2 应急处置措施

5.2.1有害程序事件的应急处置

（1）信息技术中心、事发单位应及时公布有害程序的特征、可能造成的影响、相应的处理方法，提供查杀工具下载。

（2）各单位应加强信息系统安全防范，及时更新计算机和服务器上的防病毒软件特征库，对重要数据进行备份。及时清除有害程序，恢复系统正常运行。

（3）信息技术中心、事发单位在必要时应隔离遭到感染情

况严重的区域或主机，避免有害程序扩散造成更大影响。

5.2.2网络攻击事件的应急处置

（1）事发单位应立即断开被攻击设备的网络连接，并检查信息系统遭到损害的程度。

（2）信息技术中心、事发单位应果断采取技术措施，切断攻击入侵途径，并立即定位攻击的来源，分析攻击方式。

（3）事发单位应及时修复被攻击设备的安全漏洞，查明攻击所带来的损失，恢复系统正常运行。

（4）事发单位应及时备份日志，以备调查取证。

5.2.3信息内容安全事件、信息破坏事件的应急处置

（1）各单位应针对校园网内可能发生的信息内容安全事件和信息破坏事件，对主办网站的信息实施动态监控，加强防范；党委宣传部负责对学校重要网站和BBS的信息监控。

（2）各单位对发现的有害非法信息，应在备份留查后立即删除，阻止不良信息传播。

（3）党委宣传部、事发单位应密切监控事件的发展动态，及时报送舆情信息，加强与网站、论坛管理人员的联系、沟通，防止事件蔓延，防控事件升级。做好网上思想教育工作，组织、发动网络信息员、评论员进行正面引导，争取主动。

（4）事发单位在必要时应关闭相关网站，进行全面清理。

5.2.4设备设施故障、灾害性事件的应急处置

（1）设备使用单位应首先保障数据安全，确保数据存储与数据备份的有效性、完整性，对被破坏、丢失的数据进行修复。

（2）设备使用单位应尽快维修故障，启用备用设备，减少服务中断所带来的损失。查明故障发生原因，采取补救措施，防范类似事件的再次发生。

（3）网络运行相关事件由信息技术中心负责处理，包括：线路中断、路由故障、流量异常、域名系统故障等。

（4）对火灾、盗窃、破坏等紧急事件，由党委安全保卫部按照国家有关法律法规和学校有关规定处理。

（5）遇停电等紧急事件，由后勤管理处联系市供电部门，协调处理。

5.3 网络安全事件处置程序

5.3.1发现情况

各单位网络与信息系统的维护操作人员一旦发现安全事件或接到有关单位的安全事件通报，应立即启动应急预案，根据实际情况第一时间采取关停、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，并立即报告本单位安全责任人和主要负责人。

5.3.2 紧急处置

事发单位安全责任人接到报告后，应立即组织技术人员赶赴现场进行紧急处置，同时将相关情况报告信息技术中心。信息技

术中心应立即报告党委办公室、校长办公室和学校网络与信息安全领导小组负责人。党委安全保卫部应派员至现场参与事件的处置工作。党委宣传部做好相关配合工作和舆情管控。信息技术中心做好事件处置的技术支持工作。公安机关、国家安全机关到现场处置时，学校各有关单位要积极予以配合、协助。

5.3.3事中处置

事发单位应及时、主动组织开展事中处置。安全事件的事中处置包括：及时掌握损失情况、查找分析事件原因，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，积极配合公安机关、国家安全机关开展调查。

5.3.4事后整改

事件结束后，事发单位应当深入分析事件原因和存在问题，提出整改报告并积极落实整改。安全事件的事后整改包括：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，继续配合公安机关、国家安全机关开展调查。

5.3.5情况报告

安全事件处置过程中，事发单位应当及时向学校报告处置工作进展情况。处置结束后，事发单位应当及时向学校提交整改报告。

5.4　应急响应级别降低或结束

当网络与信息系统恢复正常运行，或网络与信息安全事件造成的影响减弱或消除时，则根据实际情况相应降低应急响应级别，直至应急响应结束。

6 后期处置

6.1 事件总结

Ⅱ级以上的网络与信息安全事件由校应对处置工作组及以上工作机构进行调查处理和总结评估，并向校务会议报告，损失特别重大的向校党委常委会和教育部、浙江省报告。

6.2 表彰和惩处

处置网络与信息安全类突发公共事件实行问责制，对在处置工作中作出突出贡献的集体和个人，学校将给予表彰和奖励。对迟报、谎报、瞒报和漏报突发事件重要情况，或在处置工作中有其他失职、渎职行为的，根据其性质和造成后果的严重程度，依据法律法规以及规章制度和党内有关规定给予纪律处分或党内处理；构成犯罪的，移送司法机关依法追究刑事责任。

7 保障措施

7.1 技术支撑队伍

学校要加强网络与信息安全技术支撑队伍建设，做好重大网络与信息安全事件的应急技术支援工作，提高应对突发网络与信息安全事件的能力。

7.2 基础平台

学校要加强互联网信息分析检测系统等网络与信息安全应急平台建设，做到早发现、早预警、早响应，提高应急处置能力。

7.3 技术研发

学校要加强网络与信息安全防范技术研究，为应急响应工作提供技术支撑。

7.4 对外合作

学校要建立合作渠道，必要时和校外相关单位合作共同应对网络与信息安全突发公共事件。

7.5 经费保障

学校利用现有政策和资金渠道，积极支持网络与信息安全应急专业队伍、基础平台建设、技术研发、预案演练、宣传培训等工作。学校为网络与信息安全类突发公共事件的应急工作提供必要的经费保障。

8 宣传、培训和演练

8.1 宣传教育

各单位要采取有效措施，加强网络与信息安全类突发公共事件预防和处置的有关法律、法规和政策的宣传，开展网络与信息安全基本知识和技能的宣讲活动。

8.2 培训

各单位要将网络与信息安全事件的应急知识等列为行政管理干部和有关人员的培训内容，加强网络与信息安全特别是网络

与信息安全应急预案的培训，提高防范意识和技能。

8.3 演练

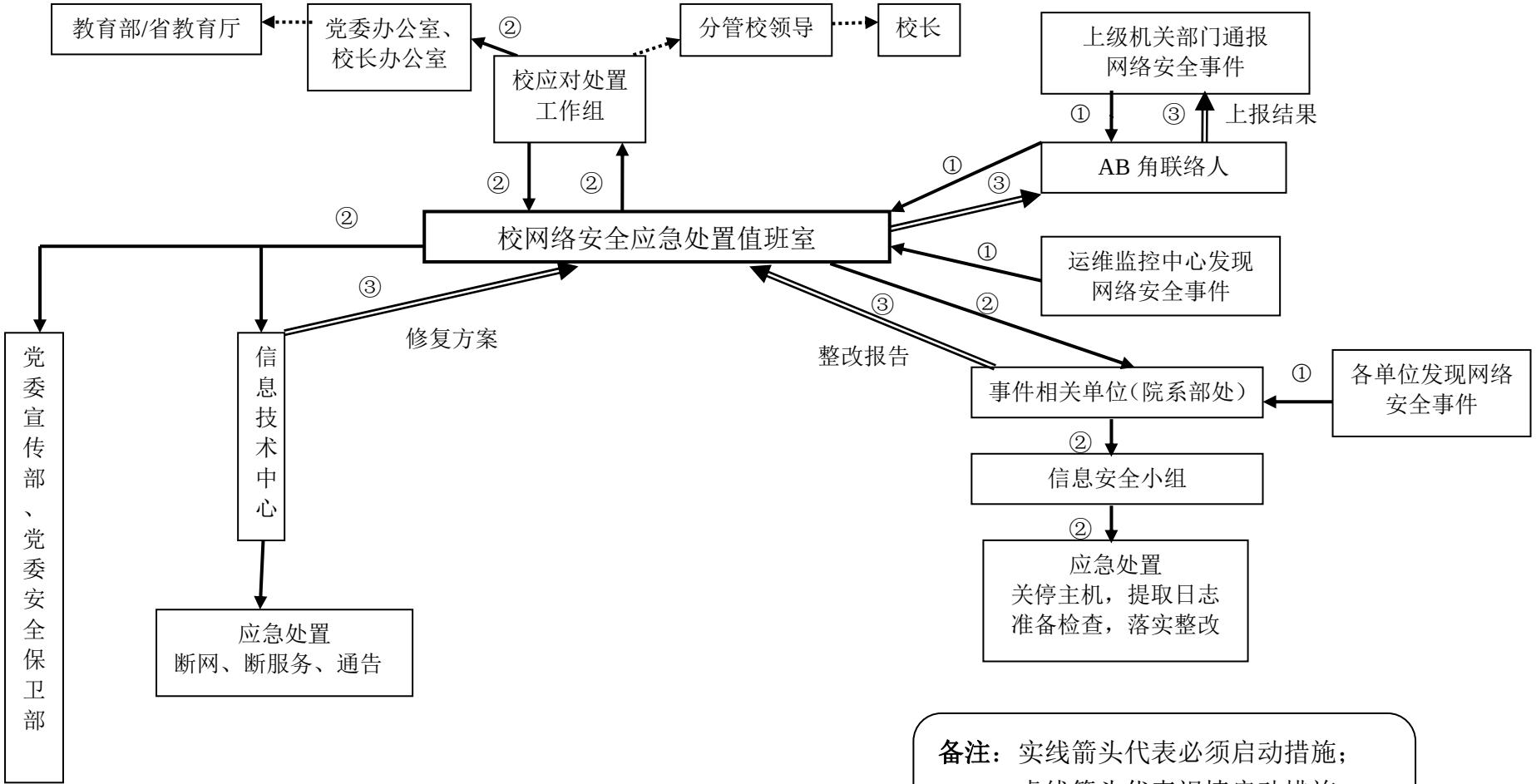
重要单位要根据本预案的要求，定期组织落实重大网络与信息安全类突发公共事件的演练，模拟处置各类网络与信息安全事件，提高实战能力，检验和完善预案。

9 附则

9.1 本预案自发布之日起施行。

9.2 本预案由校网络与信息类突发事件应对处置工作组负责解释。

附：浙江大学网络安全应对处置流程



中共浙江大学委员会办公室　　2017 年 8 月 8 日印发