浙江大学海洋学院（舟山校区）
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**

建立健全浙江大学海洋学院（舟山校区）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，维护学院和校区的安全和稳定。

**1.2 编制依据**

根据《浙江大学突发公共事件总体应急预案》(党委发〔2014〕33 号)、《浙江大学网络与信息安全管理办法》（党委发〔2017〕34 号）、《浙江大学网络与信息安全类突发公共事件应急预案》（党委发[2017]64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**

本预案适用于学院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《浙江大学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 组织体系和工作机制**

1.4.1 **校、院两级网络与信息安全应对处置工作组**

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。在学院党委、行政的统一领导下，海洋学院（舟山校区）网络与信息安全应对处置工作组（以下简称院应对处置工作组）负责建立健全处置海洋学院（舟山校区）网络与信息安全类突发公共事件的快速反应机制，确保发现、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。随时掌握事态发生、发展的情况，随时汇总、分析、上报情况，尽快平息事态，确保舟山校区网络与信息安全。

1.4.1.1**院应对处置工作组职责**

（1）在校指挥中心的领导下负责涉及海洋学院（舟山校区）的I级网络与信息安全类突发公共事件的紧急处置工作。

（2）在校应对处置工作组领导下负责涉及海洋学院（舟山校区）的Ⅱ级网络与信息安全类突发公共事件的紧急处置工作。

（3）在校应对处置工作组指导下负责海洋学院（舟山校区）的Ⅲ级网络与信息安全类突发公共事件的处置工作。

1.4.1.2**院应对处置工作组成员单位职责**

（1）学院党政办公室负责1.3.4类事件处置的应急机制建设，负责学院及下属单位开办BBS、论坛、聊天室、博客、微博等公众信息服务系统和在微信、QQ 等互联网社交平台上开办公众服务号的报备审批，以及落实其上的网络舆情信息的监控和管理，部署主办单位开展网上舆论疏导及正面宣传，并做好对外宣传工作。

（2）学院总务部负责1.3.6类事件的应急机制建设，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，负责协助学校党委安全保卫部对网络违规行为进行调查、取证、处理。

（3）学院图书信息中心负责1.3.1-1.3.3和1.3.5应急机制的建设，负责舟山校区网络设施的日常管理和维护，保障校区网络的正常运行，保存网络运行日志，根据校应急处置工作组的指示，隔离部分网络或相关主机，配合调查取证，以及协助学校信息技术中心进行事件评估、处置和技术恢复实施。

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。

1.4.2 **明确主体，分级负责**

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，各信息系统（网站）主管单位认真落实各项安全管理制度和措施。

（1）单位主要负责人为本单位网络信息安全工作的第一责任人，要掌握本单位网站和信息系统底数，加强对本单位及下属单位或部门的网站和信息系统的监管，制定应急处置预案，负责本单位所主管系统的应急管理，发生网络信息安全事件时，要立即深入第一线，掌握情况，开展工作，控制局面，24小时内向学院网络与信息安全应对处置工作组报告。

（2）新建、改建、扩建信息系统时，按照《浙江大学网络与信息安全管理办法》第十二条要求，落实本单位的信息系统、网站、公众服务号开办的报批备案制。系统安全保障措施同步规划、同步设计、同步建设、同步落实，达到《浙江大学网络与信息安全管理办法》第十九条要求方可上线运行，并在系统上线前进行登记报备和等级保护定级。

（3）落实各信息系统（网站）安全负责人和安全联络员，按照《浙江大学网络与信息安全管理办法》第二十三条要求，做好所负责系统的风险评估和隐患排查工作，参加安全培训和应急演练，负责做好所负责系统的信息安全值守，对安全事件早发现、早报告、早控制、早解决。

（4）对属于《浙江大学网络与信息安全管理办法》第二十四条范围的重点信息系统和等级保护定级二级及以上的信息系统，落实每月至少1次的安全检查，填写检查台账，加强数据、系统的备份，规范应急处置措施，提高防范能力和保持快速恢复的能力。

1.4.3 **统一协调，密切协同**

（1）学院党政办公室负责人是代表学院的联络人，负责与校应对处置工作组的联系沟通，接收网络信息安全类事件的报告并协调。各单位收到网络信息安全事件通知应及时转告，发现网络信息安全事件应及时报告。

（2）发生网络信息安全事件后，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，及时止损，并动态评估事态，及时向学院处置工作组报告。学院应对处置工作组根据事态，依据《浙江大学网络与信息安全类突发公共事件应急预案》事件分级，组织研判，决定是否启动III(一般)应急响应，或是向学院领导请示是否向学校应对处置工作组报告启动更高级别的响应，并向各单位下达协调处置意见，发布预警。

（3）网络与信息安全事件发生时，学院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。各单位共同承担网络与信息安全监测工作，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，组形成各单位系统联动、密切协同的处置工作格局。

**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)。参见《浙江大学网络与信息安全类突发公共事件应急预案》。

**3 应急处置**

**3.1 应急响应**

3.1.1 I级、Ⅱ级响应

出现Ⅰ、Ⅱ级事件时，按照上级部署做好处置。

3.1.2 Ⅲ级响应

出现Ⅲ级事件时，由学院应对处置小组发布预警并研究启动预案，协调有关单位根据类型按照3.2进行处置。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。

（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学院应对处置工作组。

（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，配合学校党委安全保卫部开展调查取证工作。

**3.2 应急处置措施**

3.2.1有害程序事件的应急处置

（1）在学校信息技术中心支持下，图书信息中心、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）图书信息中心、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。

3.2.2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）在学校信息技术中心支持下、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。

3.2.3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；党政办公室负责学院重要网站、论坛、微信公众号等新媒体的信息监控。

（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）党政办公室、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。

3.2.4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，由总务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，由总务部联系市供电部门，协调处理。

**3.3 网络安全事件处置程序**

3.3.1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，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。

3.3.2 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图书信息中心。图书信息中心应立即报告党政办公室和**学院分馆安全院领导**。总务部应派员至现场参与事件的处置工作。党政办公室做好相关配合工作和舆情管控。图书信息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，各有关单位要积极予以配合、协助。

3.3.3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。

3.3.4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。

3.3.5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院应对处置小组提交整改报告。

3.4 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。

**4 后期处置**

**4.1 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事件总结。

III级网络与信息安全事件由学院应对处置工作组进行调查处理和总结评估，并向学院党政联席会议报告，损失特别重大的向学校报告。

**4.2 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，学院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。

**5 保障措施**

**5.1 技术支撑队伍**

学院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。

**5.2 基础平台**

学院要强化学校网络与信息安全监测、应急平台的信息快速传递、共享机制，帮助各单位做到早发现、早预警、早响应，提高应急处置能力。

**5.3 对外合作**

学院要建立合作渠道，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。

**5.4 经费保障**

学院利用现有政策和资金渠道，积极支持网络与信息安全应急技术系统、人员队伍、预案演练、宣传培训等工作。学院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。

**6 宣传、培训和演练**

学院应对处置工作小组成员单位联合组织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。各单位负责人、分管安全负责人、行政管理干部和有关人员自觉参加网络与信息安全特别是网络与信息安全应急预案的培训，参加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。

**7 附则**

7.1 本预案自发布之日起施行。

7.2 本预案由学院应对处置工作组负责解释。