桂林学院文件

桂院政办〔2023〕38号

关于印发《桂林学院网络安全事件应急预案》的通知

各二级学院，各部门：

《桂林学院网络安全事件应急预案》已经2023年秋季学期第9次校长办公会议审议通过，现予以印发，请认真组织学习并遵照执行。

桂林学院学校办公室

2023年12月7日

桂林学院网络安全事件应急预案

第一章 总 则

第一条 根据《中华人民共和国网络安全法》《国家网络安全事件应急预案》、教育部《教育系统网络安全事件应急预案》《广西壮族自治区教育系统网络安全事件应急预案》等法律法规及文件精神，为健全完善学校网络安全事件应急工作机制，规范网络安全事件工作流程，提高学校安全应急处置能力，预防和减少网络安全事件造成的损失和危害，维护学校安全稳定，结合学校实际，制定本预案。

第二条 本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对学校网络和信息系统或者其中的数据造成危害，对学校造成负面影响的事件，可分为有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害性事件和其他事件。

第三条 本预案坚持以下工作原则:

一、统一指挥、密切协同。学校网络安全和信息化工作领导小组统筹协调学校网络安全应急指挥工作，建立与自治区教育厅和桂林市网络安全职能部门、专业机构等多方参与的协调联动机制，加强预防、监测、报告和应急处置等环节的紧密衔接，做到快速响应、正确应对、果断处置。

二、分级管理、强化责任。按照“谁主管谁负责、谁运维谁负责”的原则，学校是网络安全工作的责任主体，学校校长、党委书记是学校网络安全工作第一责任人。图文信息中心对学校网络安全工作负直接责任，各二级学院、各单位对本单位网站和业务信息系统安全工作负直接责任。

三、预防为主、平战结合。坚持事件处置和预防工作相结合，做好事件预防、预判、预警工作，加强应急支撑保障能力和安全态势感知能力建设；提高网络安全事件快速响应和科学处置能力，早发现、早报告、早控制、早解决，严控网络安全事件风险和影响范围。

第二章　网络安全事件分级

第四条　根据《广西壮族自治区教育系统网络安全事件应急预案》事件分级规定，网络安全事件分为四级：特别重大网络安全事件（Ⅰ级）、重大网络安全事件（Ⅱ级）、较大网络安全事件（Ⅲ级）、一般网络安全事件（Ⅳ级）。

一、符合下列情形之一的，为特别重大网络安全事件（Ⅰ级）：

（一）教育网全国或多省份范围大量用户无法正常上网。

（二）edu.cn 域名的权威系统解析效率大幅下降。

（三）关键信息基础设施或统一运行的核心业务信息系统（网站）遭受特别严重损失，造成系统大面积瘫痪，丧失业务处理能力。

（四）网络病毒在全国教育系统或多省教育系统大面积爆发。

（五）关键信息基础设施或统一运行的核心业务信息系统（网站）的重要敏感信息或关键数据丢失或被窃取、篡改。

（六）其他对教育系统安全稳定和正常秩序构成特别严重威胁，造成特别严重影响的网络安全事件。

二、符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件（II级）：

（一）教育网全区大量用户无法正常上网。

（二）关键信息基础设施或核心业务信息系统（网站）遭受严重系统损失，造成系统瘫痪，业务处理能力受到重大影响。

（三）网络病毒全区教育系统范围内大面积爆发。

（四）核心业务信息系统（网站）的重要敏感信息或关键数据发生丢失或被窃取、篡改。

（五）其他对教育系统安全稳定和正常秩序构成严重威胁，造成严重影响的网络安全事件。

三、符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件（III级）：

（一）全校范围内大量用户无法正常上网。

（二）学校重要业务信息系统（网站）遭受较大系统损失，明显影响系统效率，业务处理能力受到影响。

（三）网络病毒在全校范围内广泛传播。

（四）学校重要业务信息系统（网站）的信息或数据发生丢失或被窃取、篡改、假冒。

（五）其他对学校安全稳定和正常秩序构成较大威胁，造成较大影响的网络安全事件。

四、一般网络安全事件（IV级）：

除上述情形外，对学校安全稳定和正常秩序构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

第三章　组织领导与职责

第五条　领导机构与职责

学校网络安全和信息化工作领导小组是学校网络安全事件应急指挥的领导机构，其职责为:

一、负责网络安全事件应急处置的组织、协调、指导和监督，制定应急预案;

二、根据网络信息安全事件程度提出相应级别预案的启动，组织协调相关单位落实应急预案，共同做好处置工作;

三、负责及时收集、通报和上报网络信息安全事件处置的有关情况;

四、对全校各单位贯彻执行预案以及在事件处置工作中履行职责情况进行检查督办。

发生特别重大网络安全事件和重大网络安全事件时，应在自治区教育系统网络安全事件应急工作组组织指挥下开展应急处置工作。

第六条　办事机构与职责

学校网络安全和信息化工作领导小组办公室负责网络安全应急管理事务性工作，统筹组织网络安全监测工作，对接自治区教育厅网络安全应急办公室和网络安全职能部门，负责网络安全事件的应急处置和技术支持。

第七条 其他单位职责

一、学校办公室：牵头组织重大敏感时期、重要活动、重要会议期间发生的信息安全事件的协调处置；负责协调处理涉密级信息网络泄密类事件；负责向自治区教育厅网络安全应急办公室报告网络安全事件情况及有关材料报送工作；负责网络安全事件预警、应急响应信息等的发布工作。

二、党委工作部：负责学校网络舆情监测与处置、以及网络信息内容安全类事件的处置。

三、后勤保卫处：协助负责涉及人为破坏类网络安全事件的处置，密切联系公安部门，配合重大安全事件的处置。

四、各二级学院、各单位负责本单位网站和业务系统的信息安全管理工作，对照本预案建立本部门应急处置机制。

第四章 监测与预警

第八条 预警分级

学校建立网络安全事件预警制度。按照紧急程度、发展态势和可能造成的危害程度，网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生教育系统特别重大、重大、较大和一般网络安全事件。

第九条 安全监测

一、事件监测

学校网络安全和信息化工作领导小组办公室接到自治区教育厅网络安全应急办公室、自治区网络安全应急办公室以及公安机关网安部门监测通知的网络安全事件，或通过多种渠道监测、发现已经发生的网络安全事件，须第一时间将掌握的情况上报学校网络安全和信息化工作领导小组。各二级学院、各单位对本单位的网络和信息系统（网站）开展网络安全监测工作，一旦发生网络安全事件，应立即通过电话等方式向学校网络安全和信息化工作领导小组办公室报告，不得迟报、谎报、瞒报、漏报。

二、威胁监测

学校网络安全和信息化工作领导小组办公室组织监测全校网络安全威胁，通过多种途径监测、汇聚漏洞、病毒、网络攻击等网络安全威胁信息；各二级学院、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。

第十条 预警研判和发布

一、学校网络安全和信息化工作领导小组办公室对监测信息进行研判。对发生网络安全事件的可能性及其可能造成的影响进行分析评估，认为需要立即采取防范措施的及时向学校网络安全和信息化工作领导小组报告；认为可能发生重大以上（含重大）网络安全事件的信息，向学校网络安全和信息化工作领导小组报

告并经同意后，由学校办公室立即向自治区教育厅网络安全应急办公室报告。

各二级学院、各单位对本单位监测信息进行研判，认为可能发生网络安全事件的信息，立即向学校网络安全和信息化工作领导小组办公室报告。

二、红色预警和橙色预警由上级网络安全应急办公室发布。

学校网络安全和信息化工作领导小组办公室可根据监测研判情况，提出发布黄色预警和蓝色预警的建议，上报学校网络安全和信息化工作领导小组批准后由学校办公室发布。对达不到预警级别但又要发布警示信息的，学校网络安全和信息化工作领导小组办公室可发布风险提示信息。

预警信息包括预警级别、起始时间、可能影响范围、警示事项、应采取的措施、时限要求和发布机关等。

第十一条 预警响应

一、红色预警和橙色预警响应

红色预警和橙色预警响应按照自治区网络安全应急办公室、教育厅网络安全应急办公室的指示和要求执行。

（一）学校网络安全和信息化工作领导小组办公室根据上级网络安全应急办公室统一部署，密切关注事态发展，做好全校范围信息搜集工作，在学校网络安全和信息化工作领导小组指导下，研究制定学校防范措施和应急工作方案；学校办公室协调调

度各种校内资源，做好校内各项准备工作，并将重要情况上报自治区教育厅网络安全应急办公室。

（二）学校网络安全和信息化工作领导小组办公室及有关单位实行24小时值班，相关人员保持通信联络畅通，做好监测分析和信息搜集工作；开展应急处置或准备、风险评估和控制工作；应急技术人员进入待命状态，检查设备、软件工具等，确保其处于良好状态。

二、黄色预警和蓝色预警响应

（一）在学校网络安全和信息化工作领导小组指导下，学校网络安全和信息化工作领导小组办公室组织预警响应工作，研究制订防范措施和应急工作方案，做好风险评估、应急准备和风险控制工作并将有关情况报告学校网络安全和信息化工作领导小组。

（二）应急技术队伍保持联络畅通，检查应急设备、软件工具等，确保处于良好状态。

（三）学校办公室及时将事态发展情况上报自治区教育厅网络安全应急办公室。

三、预警解除

党委工作部根据上级网络安全应急办公室的部署，及时转发红色预警或橙色预警解除信息；学校网络安全和信息化工作领导小组办公室根据实际情况，确定是否解除黄色预警或蓝色预警，

经学校网络安全和信息化工作领导小组批准后由学校办公室及时发布预警解除信息。

第五章　应急处置

第十二条　初步处置

网络安全事件发生后，学校立即启动应急预案，立即组织应急队伍和相关人员根据不同的事件类型和事件原因，采取科学有效的应急处置措施，尽最大努力将影响降到最低，并注意保存网络攻击、网络入侵或网络病毒等证据。经分析研判，初判为特别重大、重大网络安全事件的，应立即报告教育厅网络安全应急办公室；对于人为破坏活动，同时报桂林市网信部门和公安机关。

第十三条　应急响应

网络安全事件应急响应分为Ⅰ级、II级、III级、IV级等四级，分别对应教育系统特别重大、重大、较大和一般网络安全事件。

一、Ⅰ级响应

发生特别重大网络安全事件，按照教育部网络安全应急办公室、自治区网络安全应急办公室、教育厅网络安全应急办公室的指示和要求执行。由教育部网络安全应急办公室向部网信领导小组提出启动Ⅰ级响应的建议，经批准后，成立工作组。

（一）启动指挥体系

学校网络安全和信息化工作领导小组进入应急状态， 在上级工作组统一领导、指挥、协调下履行学校应急处置工作统一领导、指挥、协调的职责，组织人员开展应急处置或支援保障工作。

领导小组成员保持24小时联络畅通，学校网络安全和信息化工作领导小组办公室24小时值守。

（二）掌握事件动态

1.跟踪事态发展。学校网络安全和信息化工作领导小组办公室与教育厅网络安全应急办公室保持联系，及时填写《教育系统网络安全事件情况报告》，经学校网络安全和信息化工作领导小组审批后由学校办公室将事态发展变化情况和处置进展情况上报教育厅网络安全应急办公室。

2.检查影响范围。学校网络安全和信息化工作领导小组办公室立即全面了解学校的网络和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学校网络安全和信息化工作领导小组，经审批后由学校办公室上报教育厅网络安全应急办公室。

3.及时通报情况。学校网络安全和信息化工作领导小组办公室及时将上级通报的情况向学校网络安全和信息化工作领导小组汇报。

（三）学校网络安全和信息化工作领导小组组织有关单位、专家组、应急技术支撑队伍等方面及时研究对策意见，对处置工作进行决策部署。

（四）处置实施

1.控制事态防止蔓延。学校网络安全和信息化工作领导小组办公室采取各种技术措施、管控手段，最大限度阻止和控制事态蔓延。

2.消除隐患恢复系统。根据事件发生原因， 学校网络安全和信息化工作领导小组办公室针对性制定解决方案，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要及时组织恢复。

3.调查取证。学校网络安全和信息化工作领导小组办公室应在保留相关证据的基础上，开展问题定位和溯源追踪工作。积极配合桂林市网信部门和公安机关开展调查取证工作。

4.信息发布。党委工作部根据上级的指导和协调，开展新闻发布和舆论引导工作。未经批准，其他单位不得擅自发布相关信息。

5.协调上级支持。处置中需要技术及工作支持的，由学校办公室根据实际情况，请求教育厅网络安全应急办公室予以支持。

6.次生事件处置。对于引发或可能引发其他安全事件的，学校办公室应及时按程序上报，并在学校相关部门应急处置中做好协调配合工作。

二、 II 级响应

网络安全事件的 II 级响应，由教育部网络安全应急办公室确定并发布，或由自治区网络安全应急办公室、教育厅网络安全应急办公室根据事件性质和情况确定并发布。

（一） 学校网络安全和信息化工作领导小组响应发布单位进入应急状态，领导小组办公室按照相关应急预案做好应急处置工作。

（二） 学校网络安全和信息化工作领导小组办公室及时填写《教育系统网络安全事件情况报告》，由学校办公室报教育厅网络安全应急办公室，教育厅网络安全应急办公室报教育部网络安全应急办公室和自治区网络安全应急办公室。

（三）处置中需要其他单位和网络安全应急技术支撑队伍配合和支持的，学校办公室报教育厅网络安全应急办公室予以协调。

（四）学校网络安全和信息化工作领导小组办公室根据通报，结合学校实际有针对性地加强防范，防止造成更大范围影响和损失。

二、III级应急响应

发生较大网络安全事件，由学校网络安全和信息化工作领导小组办公室向领导小组提出启动III级响应建议，经批准后启动III级响应。

（一）学校网络安全和信息化工作领导小组响应发布单位进入应急状态，领导小组办公室按照相关应急预案做好应急处置工作。

（二）学校网络安全和信息化工作领导小组办公室及时填写《教育系统网络安全事件情况报告》，由学校办公室报教育厅网络安全应急办公室，教育厅网络安全应急办公室报教育部网络安全应急办公室和自治区网络安全应急办公室。

（三）处置中需要其他单位和网络安全应急技术支撑队伍配合和支持的，学校办公室报教育厅网络安全应急办公室予以协调。

（四）学校网络安全和信息化工作领导小组办公室结合学校实际有针对性地加强防范，防止造成更大范围影响和损失。

三、Ⅳ级应急响应

发生一般网络安全事件，事发单位应立即向学校网络安全和信息化工作领导小组办公室报告，领导小组办公室指导事发单位按照相关应急预案做好应急处置工作，并指导有关单位有针对性地加强防范，防止造成更大范围影响和损失。

第十四条 应急处置具体措施

当发生网络安全事件时，学校网络安全和信息化工作领导小组办公室应立即启动应急预案，技术人员根据不同的事件类型和事件原因，采取科学有效的应急处置措施，并注意保存网络攻击、网络入侵或网络病毒等证据。

一、当发生自然灾害时，应根据当时实际情况，在保障人身安全的前提下，首先保障数据安全，然后是设备安全。具体处置方法为：硬盘拔出与保存，设备断电、拆卸、搬迁等。

二、当发生人为或病毒破坏事件时，应及时判断破坏来源与性质，断开影响安全与稳定的信息网络设备，断开与破坏来源的网络物理连接，跟踪并锁定破坏来源的 IP 或其他网络用户信息，

修复被破坏的信息，恢复信息系统。并按照事件发生的性质分别采取以下处置措施:

（一）病毒传播：及时断开病毒传播源，判断病毒的性质、采用的端口，然后关闭相应端口或断开网络，防止造成其他内网设备的安全事故，公布病毒攻击信息以及清除、防御方法。

（二）网络入侵:

1.网络入侵来自互联网的，及时定位入侵 IP 地址，关闭入侵端口，限制入侵的 IP 地址访问，在无法制止的情况下可断开网络连接。

2.网络入侵来自校园网内部的，通过 IP 地址及时查清入侵来源，阻断 IP 地址或断开相应设备的网络端口，并针对入侵方式建立或更新安全设备防护策略。

（三）信息被篡改：一经发现马上断开服务器网络连接，保留相关记录并删除有害信息，及时恢复被篡改信息，修补系统漏洞，修改系统口令，经安全检查测评后再上线使用。

（四）网络故障：一旦发现，可根据相应工作流程尽快排除。

（五）其它没有列出的不确定因素造成的事件，可根据总体安全原则，结合具体情况做出相应处置。

第十五条 应急结束

一、I 级和 II 级响应结束

根据自治区、教育厅网络安全应急办公室应急响应结束的通报，经学校网络安全和信息化工作领导小组批准后结束应急响应。

二、III级响应结束

学校网络安全和信息化工作领导小组办公室完成应急处置并根据实际情况提出解除III级响应建议，经学校网络安全和信息化工作领导小组批准后，由学校办公室在全校范围内通报有关情况。

三、IV级响应结束

由事发单位完成应急处置并报学校网络安全和信息化工作领导小组办公室同意后，根据实际情况自行解除IV级响应状态。

四、调查与评估

（一）特别重大网络安全事件由教育部网络安全应急办公室组织有关单位开展调查处理和总结评估工作，并将调查评估结果汇总上报教育部网信领导小组及国家网络安全应急办公室。重大网络安全事件根据事发单位属性，由教育部网络安全应急办公室或教育厅网络安全应急办公室组织开展调查处理和总结评估工作。教育厅网络安全应急办公室应将调查评估结果汇总上报教育部网络安全应急办公室和自治区网络安全应急办公室。

（二）较大网络安全事件和一般网络安全事件由学校组织开展调查处理和总结评估工作，相关调查总结报告按照自治区教育厅关于印发《网络安全事件报告与处置流程（试行）》的通知（桂教规范〔2017〕11号）由学校办公室上报教育厅网络安全应急办公室。

网络安全事件总结调查报告应对事件的起因、性质、影响、

责任等进行分析评估，提出处理意见和改进措施。网络安全事件的调查处理和总结评估工作应在应急响应结束后 5 天内完成。

第六章　预防工作

第十六条　日常管理

图文信息中心网络与校园数字化办公室应做好网络安全事件日常预防工作，根据本预案制定完善相关的专项应急预案和配套的管理制度，建立完善的应急管理体制；按照网络安全等级保护、关键信息基础设施防护等相关要求落实各项防护措施，做好网络安全检查、风险评估和容灾备份，加强信息系统（网站）的安全保障能力。

第十七条　监测预警和通报

图文信息中心网络与校园数字化办公室应加强网络安全监测预警和通报，及时发现并处置安全威胁，全面掌握学校信息系统（网站）情况，指导、监督学校各二级学院、各单位及时修复安全漏洞，全面排查安全隐患，提高发现和应对网络安全事件的能力。

第十八条　应急演练

图文信息中心网络与校园数字化办公室须积极参加教育厅每年组织的广西教育系统网络安全攻防演习，并认真进行分析和总结，不断提高网络安全防范能力；同时结合学校实际，每年组织一次应急演练，年底前将本年度学校演练情况上报自治区教育厅网络安全应急办公室。

第十九条 宣传教育

一、党委工作部、学生事务处（部）应将网络安全教育作为全校师生国家安全教育的重要内容，加强网络安全、突发网络安全事件预防和处置的有关法律、法规和政策的宣传教育。

二、图文信息中心网络与校园数字化办公室应充分利用国家网络安全宣传周，通过各种活动形式和传播媒介，开展网络安全基本知识和技能的宣传活动，提高全校师生和相关人员的网络安全意识。

第二十条 工作培训

一、图文信息中心应定期组织学校网络信息专业技术人员和兼职管理人员开展网络安全知识和技能培训，加强网络安全特别是网络安全事件应急预案的学习，提高网络安全管理和技术人员的防范意识及安全技能。

二、党委工作部、人力资源处（部）应将网络安全事件的应急知识和网络安全知识列入领导干部和教职工的培训内容，学生事务处（部）应加强对学生网络安全知识的培训。进一步提高学校领导干部、教职工员和学生的网络安全意识和防范技能。

第七章 工作保障

第二十一条 机构和人员

学校建立健全网络安全应急工作责任制， 将网络安全应急工作作为重点工作予以部署。图文信息中心是学校网络安全职能部门，各二级学院、各单位应按照“谁主管谁负责”的原则，把

网络安全应急工作责任落实到具体岗位和个人，明确工作责任，建立健全应急工作机制。

第二十二条 技术支撑

图文信息中心网络与校园数字化办公室作为网络安全技术支撑单位，应加强网络安全技术队伍建设，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支撑工作。发生网络安全应急事件时，应联系网络运营商提供技术支持并请求其协助处置。

第二十三条 专家队伍

图文信息中心、人力资源处（部）应建立学校网络安全专家组，为全校网络安全事件的预防和处置提供技术咨询和决策建议，提高应急保障能力。

第二十四条 信息共享与应急合作

图文信息中心网络与校园数字化办公室应加强与周边高校、网络安全专业机构、行业学会（协会）等单位的合作，建立网络安全威胁的信息共享机制和网络安全事件的快速发现和协同处置机制。

第二十五条 经费保障

学校每年提供必要的专项经费，支持和保障开展网络安全应急技术支撑队伍建设、专家队伍建设、基础平台建设、监测通报、宣传教育培训、预案演练、物资保障等工作。

第二十六条 责任与奖惩

学校对网络安全事件应急管理工作中作出突出贡献的先进集体和个人给予表彰和奖励；对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者在应急管理工作中有其他失职、渎职行为的，依照上级及学校相关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

第八章　附 则

第二十七条 预案管理

本预案根据上级及学校实际情况适时修订，修订工作由学校网络安全和信息化工作领导小组组织，领导小组办公室具体落实。

第二十八条 本预案由学校网络安全和信息化工作领导小组负责解释。

第二十九条 本预案自印发之日起实施，原《广西师范大学漓江学院信息网络安全应急预案》（漓院政办〔2017〕26号）同时废止。学校原有规定与本预案不一致的，以本预案为准。

附件：1. 网络安全事件分级与预警分级

2. 网络安全事件应急处置流程

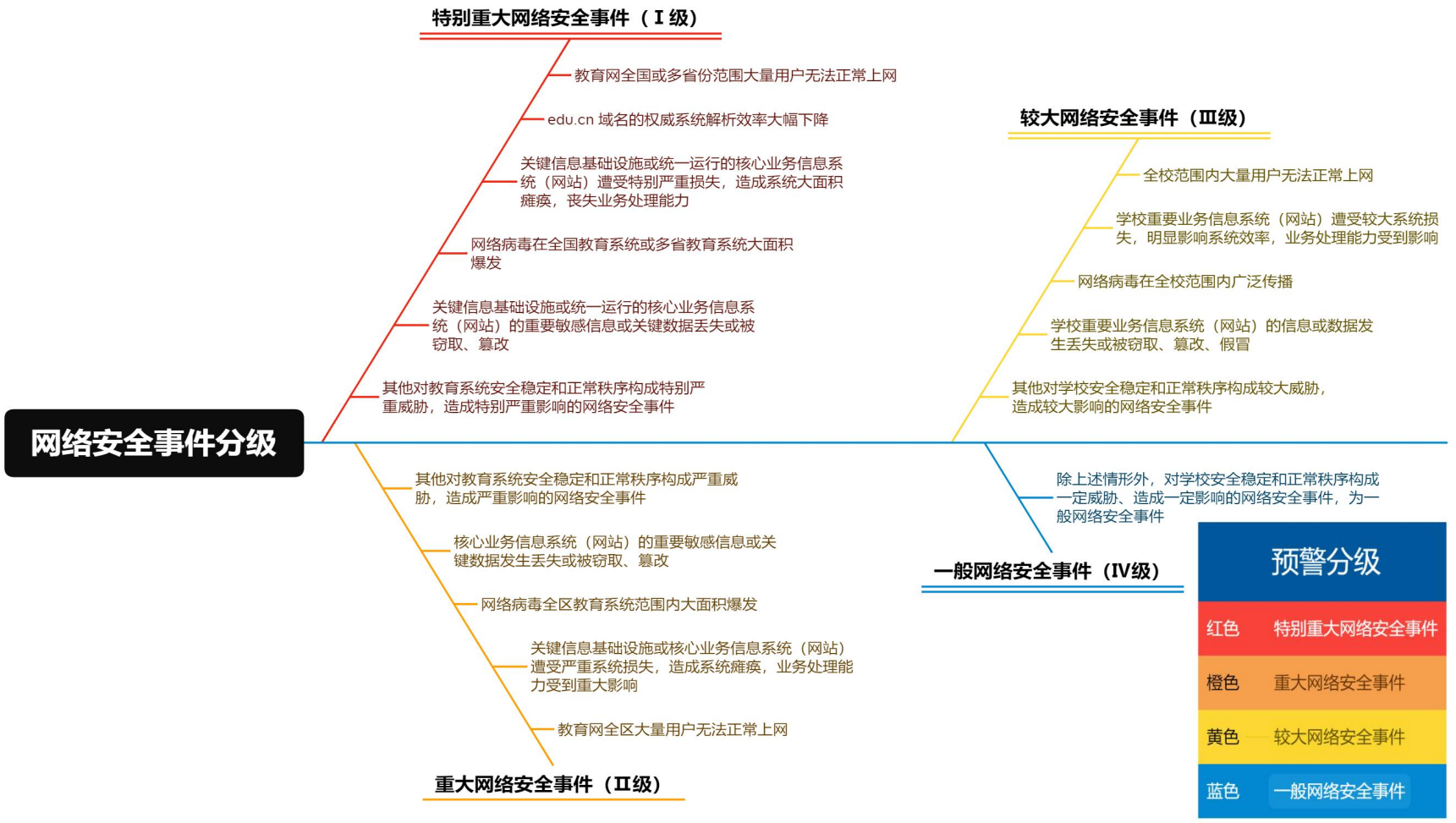
3. 网络安全事件应急响应流程

4. 网络安全事件应急结束流程

5. 网络安全事件调查与评估流程

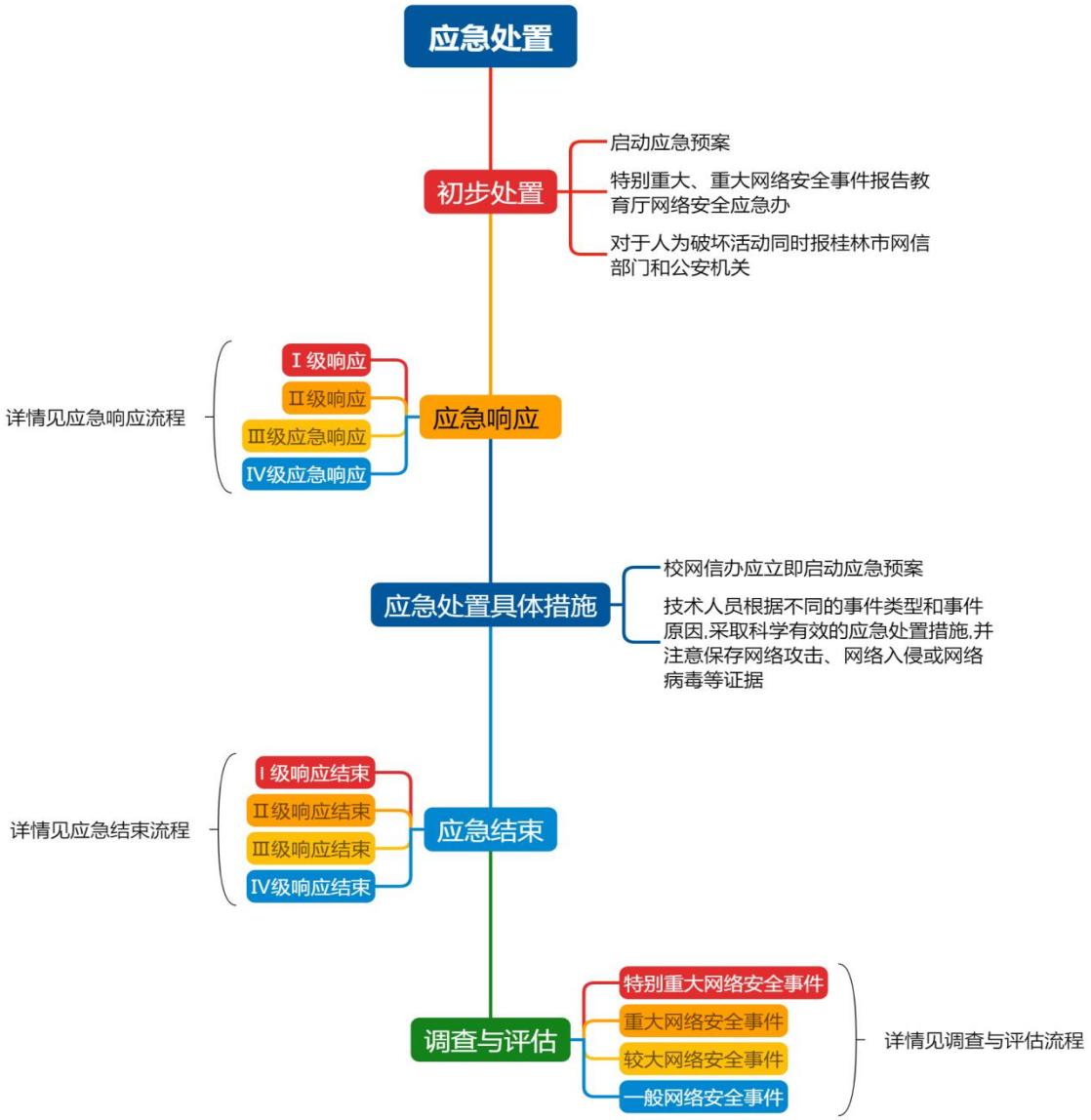
附件 1

网络安全事件分级与预警分级



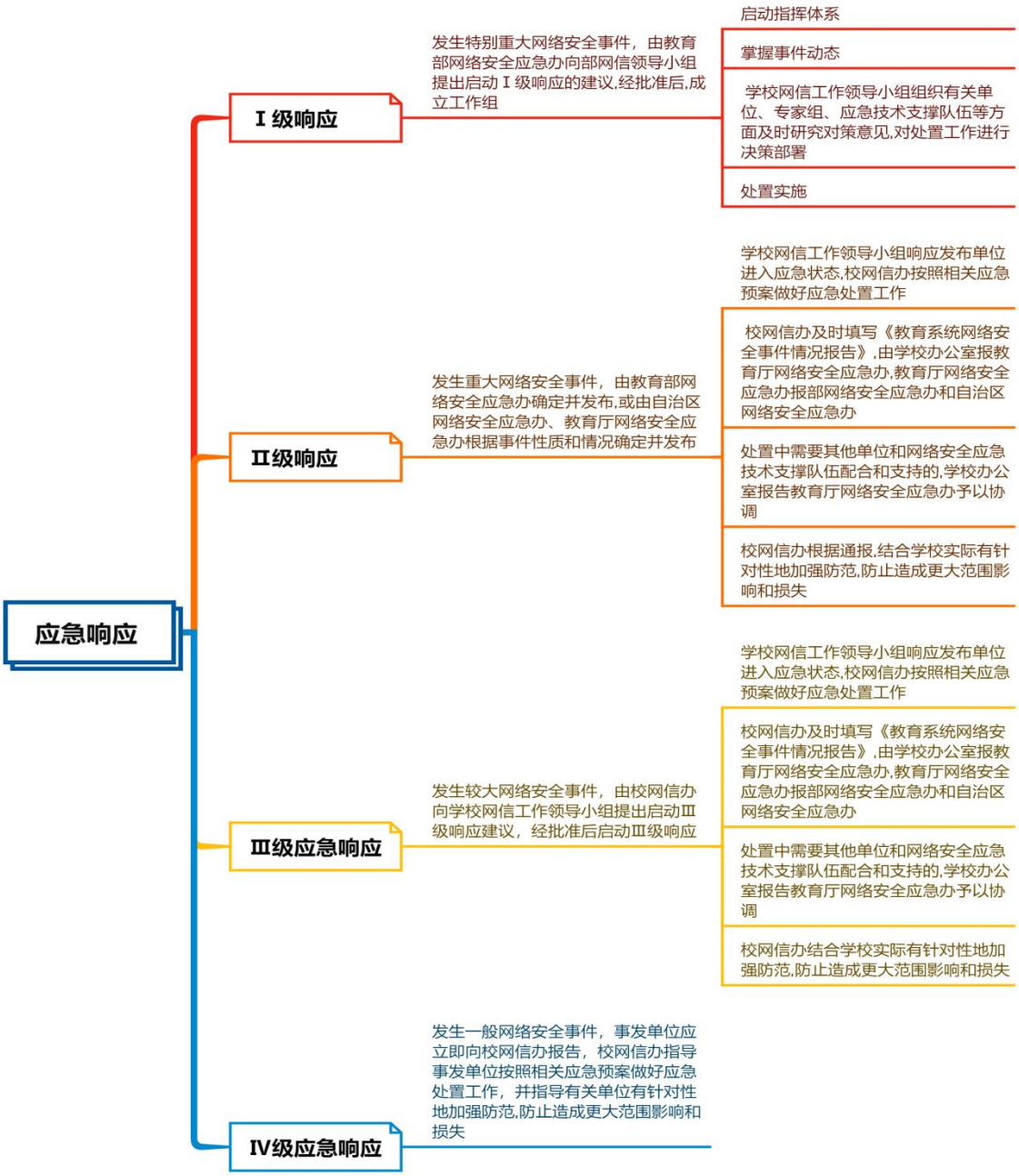
附件 2

网络安全事件应急处置流程



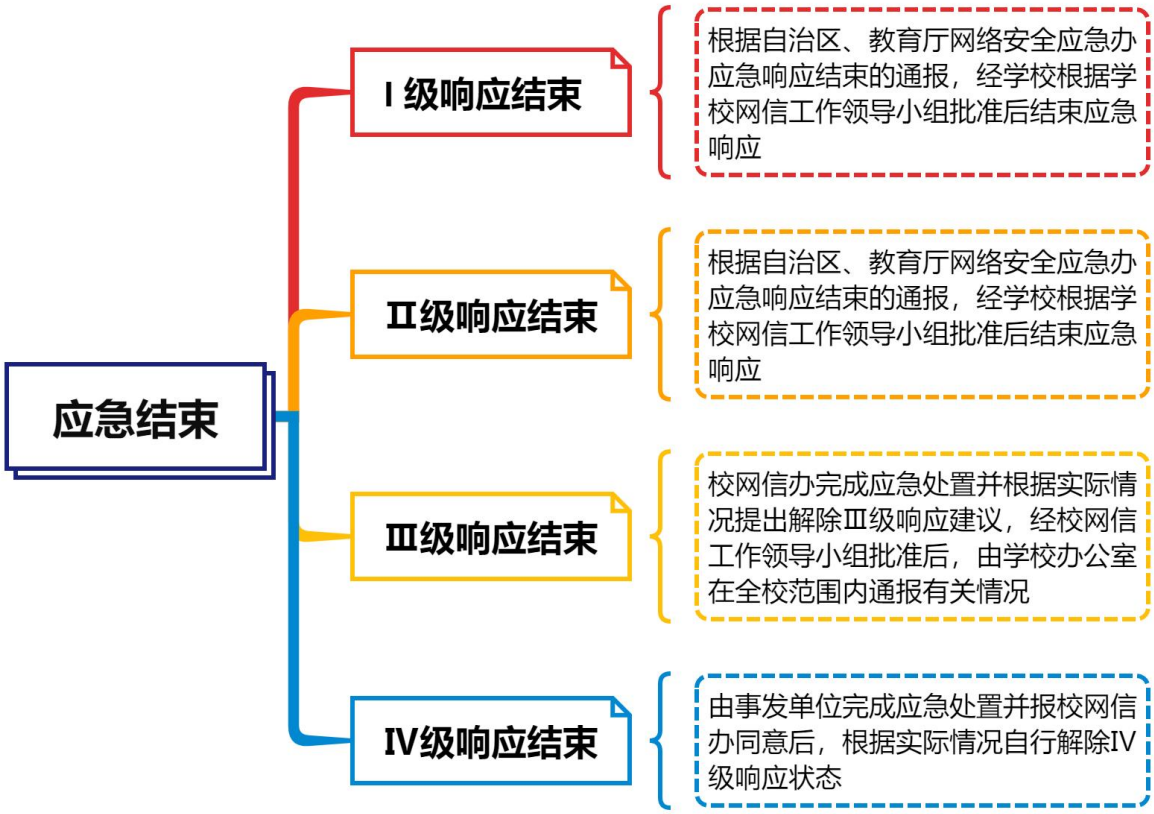
附件 3

网络安全事件应急响应流程



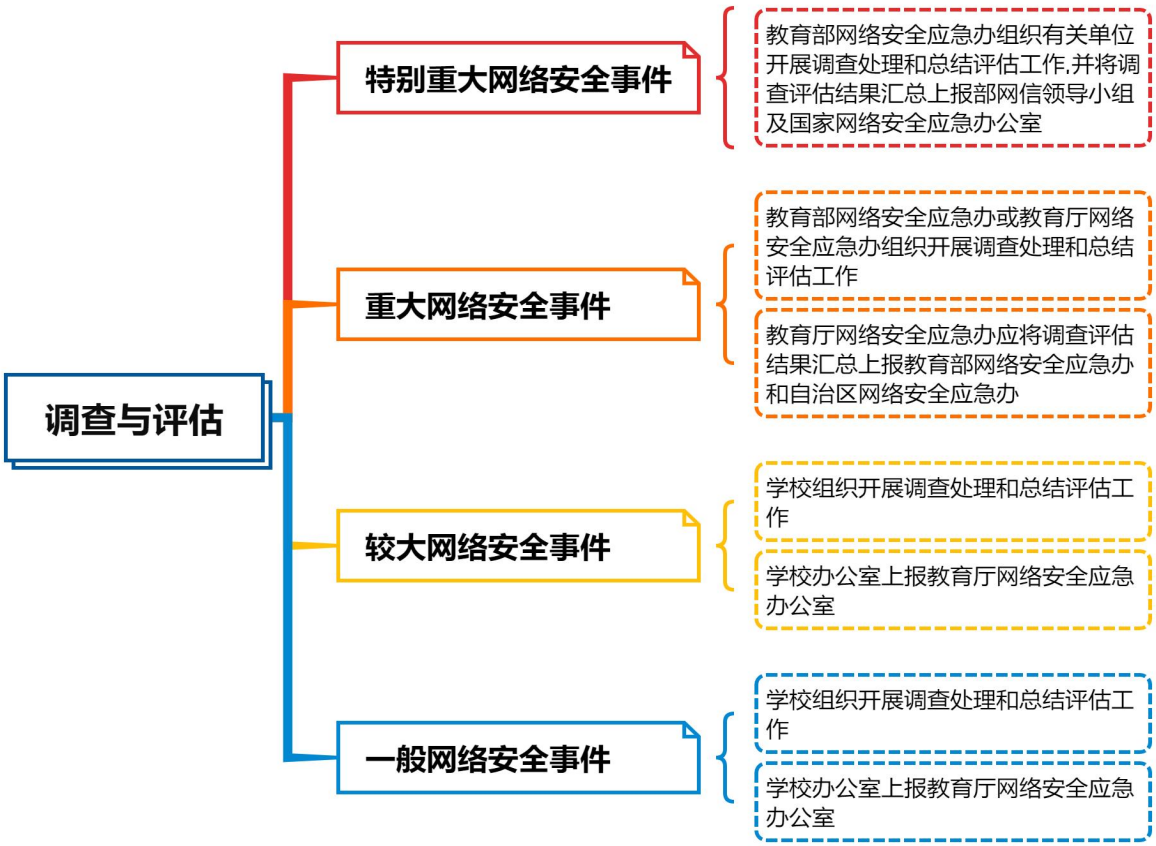
附件 4

网络安全事件应急结束流程



附件 5

网络安全事件调查与评估流程



桂林学院学校办公室　　2023 年 12 月 11 日印发