普洱学院网络与信息安全应急预案

一. 总 则

（一）编制目的

为提高普洱学院处置网络与信息安全突发事件的能力，加强和完善网络与信息安全应急管理措施，层层落实责任，有效预防、及时控制和最大限度地消除信息安全突发事件的危害和影响，形成科学、有效、反应迅速的应急工作机制，确保重要计算机信息系统的实体安全、运行安全和数据安全，最大程度地预防和减少网络与信息安全突发事件及其造成的损害，保障信息资产安全，完善安全责任制、各处室部门二级学院应积极支持和协助应急处置工作，特制定本应急预案。

（二）编制依据

根据《国家网络安全事件应急预案》、《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国网络安全法》、《全省教育行业网络与信息安全应急预案（试行）》和公安部《计算机病毒防治管理办法》《信息安全技术信息安全事件分类分级指南》（GB/z20986-2007）等制定本预案。

（三）分类分级

教育行业网络与信息安全事件分为八类：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、网络舆情事件、

信息破坏事件、设备设施故障事件、灾害性事件上、其它网络安全事件等。

网络与信息安全突发事件，特指校园网络软硬件系统、站群系统、信息化业务系统、教学信息化设施，遭受不可预知外力的破坏、毁损、故障，发生对学校、社会造成或者可能造成重大危害，危及校园安全或公共安全的紧急事件。

1.事件分类

根据网络与信息安全突发事件的性质、机理和发生过程，网络与信息安全突发事件主要分为以下三类：

（1）自然灾害。指地震、台风、雷电、火灾、洪水等引起的网络与信息系统的损坏。

（2）事故灾难。指电力中断、网络损坏或者软件、硬件设备故障等引起的网络与信息系统的损坏。

（3）人为破坏。指人为破坏网络线路、通信设施，黑客攻击、病毒攻击、恐怖袭击等引起的网络与信息系统的损坏。

2.事件分级

根据全省教育行业网络与信息安全突发事件分级为依据，将我校信息安全事件严重程度和影响范围，一般分为四级：Ⅰ级(特别重大网络和信息安全事件)、Ⅱ级（重大网络安全和信息安全事件）、Ⅲ级（较大网络和信息安全事件）和Ⅳ级（一般网络和信息安全事件）。

（1） Ⅰ级（特别重大）

国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

重要网络和信息系统受到特别严重的系统损失，造成大面积瘫痪，丧失业务处理能力。

其他对国家安全，社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络和信息安全事件。

校园网络和信息安全事件，导致全局大规模瘫痪或产生恶劣影响的社会事件，事态发展超出我校的控制能力，需要由教育厅或公安信息化安全部门应急协调解决的，对国家安全、社会秩序、公众利益造成特别严重损害的信息安全突发事件。

符合以上情形之一即为特别重大网络和信息安全事件。

（2） Ⅱ级（重大）

重要网络和信息系统遭受严重的系统损失，造成系统长时间中断和局部瘫痪，业务处理能力受到极大影响。

国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。

其他对国家安全，社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络和信息安全事件。

符合以上情形之一且未达特别重大网络和信息安全事件。即为重大网络和信息安全事件。

（3） Ⅲ级（较大）

重要网络和信息系统遭受严重的系统损失，造成系统中断，

明显影响系统效率，业务处理能力受到影响。

国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。

其他对国家安全，社会秩序、经济建设和公众利益构成严重威胁、造成较严重影响的网络和信息安全事件。

符合以上情形之一且未达重大网络和信息安全事件，即为较大网络和信息安全事件。

（4） IV级（一般）

除属于特别重大网络和信息安全事件、重大网络和信息安全事件、较大网络和信息安全事件所出现的情形外，但对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络和信息安全事件，即为一般网络和信息安全事件。

（四）适用范围

本预案是普洱学院依据云南省教育网络与信息安全应急预案制定的专项预案，适用于普洱学院发生或可能导致发生网络与信息安全突发事件的应急处置工作。

（五）工作原则

1.预防为主

根据《计算机信息安全管理规定》的要求，建立、健全工会计算机信息安全管理制度，有效预防网络与信息安全事故的发生。立足安全防护，加强预警，重点保护基础信息网络和关系校园安全、教学秩序、师生稳定的重要信息系统，从预防、监控、

应急处理、应急保障和打击犯罪等环节，在法律、管理、技术、人才等方面，采取多种措施，充分发挥各方面的作用，共同构筑网络与信息安全保障体系。

2、果断处置，快速反应

一旦发生网络与信息安全事故，应迅速反应，及时启动应急处置预案，尽最大力量减少损失，尽快恢复网络与系统运行。

加强网络与信息安全科学研究和技术开发，采用先进的监测、预测、预警、预防和应急处置技术及设施，充分发挥专业人员的作用，在网络与信息安全突发事件发生时，按照快速反应机制，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。

3、以人为本，减少损害

把保障国家安全、社会秩序、经济建设和公众利益以及全校师生合法权益的安全作为首要任务，及时采取措施，最大限度地避免信息安全、数据资源遭受损失。

4.加强管理，分级负责

按照 “谁主管谁负责、谁建设谁负责、谁运维谁负责、谁使用谁负责”的原则，建立和完善安全责任制及联动工作机制。根据部门职能，各司其职，加强部门间协调与配合，形成合力，共同履行应急处置工作的管理职责。

5.定期演练，常备不懈

加强技术储备，规范应急处置措施与操作流程，定期进行预

案演练，确保应急预案切实有效，实现网络与信息安全突发事件应急处置的科学化、程序化与规范化。

二．组织指挥机构与职责

（一）组织体系

普洱学院成立网络与信息安全应急领导小组及应急办公室（具体名单见附件），组长、副组长由校领导担任，成员包括：学院各二级学院、处室部门负责人；应急办公室设在信息中心。

（二）工作职责

1.研究制订普洱学院网络与信息安全应急处置工作的规划、计划和政策，协调推进普洱学院网络与信息安全应急机制和工作体系建设。

2.研究提出网络与信息安全应急机制建设规划，检查、指导和督促网络与信息安全应急机制建设。指导督促重要信息系统应急预案的修订和完善，检查落实预案执行情况。

3.指导应对网络与信息安全突发事件的科学研究、预案演习、宣传培训，督促应急保障体系建设。

4.负责提供技术咨询、技术支持，参与重要信息的研判、网络与信息安全突发事件的调查和总结评估工作，进行应急处置工作。

5.及时收集网络与信息安全突发事件相关信息，分析重要信息并提出处置建议。对可能演变为Ⅰ级、Ⅱ级、Ⅲ级的网络与信

息安全突发事件，应及时向学校领导提出启动本预案的建议；如果发生Ⅰ级、Ⅱ级网络与信息安全突发事件后，本预案立即自行启动，并第一时间通报学校主要领导，同时向省教育厅、公安局有关部门通报并请求上级机关协助处理；发生Ⅲ级网络与信息安全突发事件后，第一时间通报学校主要领导，并根据事态发展研究决定是否启动应急预案。

三．监测、预警和先期处置

（一）信息监测与报告

1.要进一步完善各重要信息系统网络与信息安全突发事件监测、预测、预警制度。按照“早发现、早报告、早处置”的原则，加强对各类网络与信息安全突发事件和可能引发网络与信息安全突发事件的有关信息的收集、分析判断和持续监测。当发生网络与信息安全突发事件时，在按规定向有关部门报告的同时，按紧急信息报送的规定及时向学校领导汇报。初次报告最迟不得超过 4 小时，较大、重大和特别重大的网络与信息安全突发事件实行态势进程报告和日报告制度。报告内容主要包括信息来源、影响范围、事件性质、事件发展趋势和采取的措施等。

2.重要信息系统管理人员应确立 2 个以上的即时联系方式，避免因信息网络突发事件发生后，必要的信息通报与指挥协调通信渠道中断。

3.信息安全定期汇报。信息安全应急办公室，每周应向学校

领导报告我校网络与信息安全自查工作进展情况：

（1）泛及国家安全，社会秩序、经济建设和公众利益的安全事件，恶意人士利用我校网络从事违法犯罪活动的情况。

（2）网络或信息系统通信和资源使用异常，网络和信息系统瘫痪、应用服务中断或数据篡改、丢失等情况。

（3）网络恐怖活动的嫌疑情况和预警信息。

（4）网络安全状况、安全形势分析预测等信息。

（5）其他影响网络与信息安全的信息。

（二）预警处理与预警发布

1.对于可能发生或已经发生的网络与信息安全突发事件，系统管理员应立即采取措施控制事态，并在 2 小时内进行风险评估，判定事件等级并发布预警。必要时应启动相应的预案，同时向学院网络与信息安全应急领导小组汇报。

2.领导小组接到汇报后应立即组织现场救援，查明事件状态及原因，技术人员应及时对信息进行技术分析、研判，根据问题的性质、危害程度，提出安全警报级别。

（三）先期处置

1.当发生网络与信息安全突发事件时，及时请技术人员做好先期应急处置工作并立即采取措施控制事态，必要时采用断网、关闭服务器等方式防止事态进一步扩大，同时向上级信息安全领导小组通报。

2. 网络与信息安全应急领导小组在接到网络与信息安全突

发事件发生或可能发生的信息后，应加强与有关方面的联系，掌握最新发展态势。Ⅳ 级网络与信息安全突发事件由相关工作人员及时进行处理，并报知部门领导，对有可能演变为Ⅲ级网络与信息安全突发事件，技术人员处置工作提出建议方案，并作好启动本预案的各项准备工作。信息安全领导小组根据网络与信息安全突发事件发展态势，视情况决定现场指导、组织设备厂商或者系统开发商应急支援力量，做好应急处置工作。对有可能演变为Ⅱ级或Ⅰ级的网络与信息安全突发事件，要根据上级有关部门的要求，上报省教育厅、市公安局关部门，请求上级安排技术力量赶赴现场指挥、组织应急支援力量，积极做好应急处置工作。

四．应急处置

（一）应急指挥

1.本预案启动后，领导小组要迅速建立与现场通讯联系。抓紧收集相关信息，掌握现场处置工作状态，分析事件发展趋势，研究提出处置方案，调集和配置应急处置所需要的人、财、物等资源，统一指挥网络与信息安全应急处置工作。

2.需要成立现场指挥部的，学院信息中心立即在现场开设指挥部，并提供现场指挥运作的相关保障。现场指挥部要根据事件性质迅速组建各类应急工作组，开展应急处置工作。

（二）应急支援

本预案启动后，网络与信息安全应急领导小组可根据事态的

发展和处置工作需要，及时向省教育厅、公安局相关单位申请增派专家小组和应急支援单位，调动必需的物资、设备，支援应急工作。参加现场处置工作的有关人员要在现场指挥部统一指挥下，协助开展处置行动。

（三）信息处理

现场信息收集、分析和上报。技术人员应对事件进行动态监测、评估，及时将事件的性质、危害程度和损失情况及处置工作等情况及时报领导小组，不得隐瞒、缓报、谎报。符合紧急信息报送规定的，属于Ⅰ级、Ⅱ级信息安全事件的，同时报省教育厅、市公安局相关网络与信息安全部门。

（四）扩大应急

经应急处置后，事态难以控制或有扩大发展趋势时，应实施扩大应急行动。要迅速召开网络与信息安全应急领导小组会议，根据事态情况，研究采取有利于控制事态的非常措施，并向有关部门请求支援。

（五）应急结束

网络与信息安全突发事件经应急处置后，得到有效控制，将各监测统计数据报网络与信息安全应急领导小组，提出应急结束的建议，经领导批准后实施。

五．后期处置

（一）善后处置

在应急处置工作结束后，要迅速采取措施，抓紧组织抢修受损的基础设施，减少损失，尽快恢复正常工作，统计各种数据，查明原因，对事件造成的损失和影响以及恢复重建能力进行分析评估，认真制定恢复重建计划，迅速组织实施。

（二）调查和评估

在应急处置工作结束后，网络与信息安全应急领导小组应立即组织有关人员和专家组成事件调查组，对事件发生及其处置过程进行全面的调查，查清事件发生的原因及财产损失状况和总结经验教训，写出调查评估报告。

六．应急保障

（一）通信与信息保障

领导小组各成员应保证电话 7×24 小时开机，以确保发生信息安全事故时能及时联系到位。

（二）应急装备保障

各重要信息系统在建设系统时应事先预留出一定的应急设备，做好信息网络硬件、软件、应急救援设备等应急物资储备工作。在网络与信息安全突发事件发生时，由领导小组负责统一调用。

（三）数据保障

重要信息系统应建立容灾备份系统和相关工作机制，保证重要数据在受到破坏后，可紧急恢复。

（四）应急队伍保障

按照一专多能的要求建立网络与信息安全应急保障队伍。选择若干经国家有关部门资质认可的，具有管理规范、服务能力较强的企业作为我校网络与信息安全的社会应急支援单位，提供技术支持与服务；必要时能够有效调动机关团体、企事业单位等的保障力量，进行技术支援。

（五）交通运输保障

应确定网络与信息安全突发事件应急交通工具，确保应急期间人员、物资、信息传递的需要，并根据应急处置工作需要，由领导小组统一调配。

（六）经费保障

网络与信息系统突发公共事件应急处置资金，应列入年度工作经费预算，切实予以保障。

七．监督管理

（一）宣传教育和培训

要充分利用各种传播媒介，采取多种形式，加强有关网络与信息安全突发事件应急处置的法律法规和政策的宣传，开展预防、预警、自救、互救和减灾等知识的宣讲活动，普及应急救援的基本知识，提高我校信息安全防范意识和应急处置能力。

将网络与信息安全突发事件的应急管理、工作流程等列入学校各部门主要负责人的培训内容，增强应急处置工作中的组织能

力。加强对网络与信息安全突发事件的技术准备培训，提高工作人员的防范意识及技能。

（二）预案演练

建立应急预案定期演练制度。通过演练，发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

（三）责任与奖惩

要认真贯彻落实预案的各项要求与任务，建立分级布置、监督检查和奖惩机制。按普洱学院网络与信息安全应急领导小组预案的规定不定期进行检查。

对在应急管理工作中做出突出贡献的部门和个人给予表彰和奖励。

对不按规定有效落实预案各项规定进行通报批评，责令限期改正，在应急管理中有失职、渎职行为的，依照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。

八．附则

（一）预案管理与更新

本预案原则上两年评估一次，根据现行法律法规及实际情况适时修订。

本预案由普洱学院信息中心制订，结合信息网络快速发展的特点和我校实际状况，及时更新修订本预案。

（二）解释部门

普洱学院网络与信息安全应急领导小组及信息中心负责解释。

（三）实施时间

本预案自发布之日起实施。

附：

普洱学院网络与信息安全应急领导小组及应急办公室

成员名单

1. 组织机构：

组长：　毛保祥　成文章

副组长：郑颖松　于于千 代红兵　白应华

成员：各二级学院院长　各部门负责人

2．信息安全应急公办室：

主任：李春

副主任：邱成相

成员：陈洪磊　罗阳静　施秋萍