普洱学院重大信息安全事件应急处置和报告制度

为预防和及时处置网络突发事件，保证网络信息安全，维护社会稳定，特制订网络信息安全事件应急处置和报告制度。

一、在普洱学院党委的统一领导下，贯彻执行《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互联网管理暂行规定》等相关法律法规，坚持积极防御、综合防范的方针，本着以防为主、注重应急工作原则，预防和控制风险，在发生信息安全事故或事件时最大程度地减少损失，维护社会和学校稳定，尽快使网络和系统恢复正常，做好网络运行和信息安全保障工作。

二、信息网络安全事件定义

1. 人为因素或灾难性事件如水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致网络突然发生中断。

2. 恶意攻击，篡改网站主页、在交互式栏目里发表以下信息的：

- ✧ 煽动分裂国家、破坏国家统一和民族团结、推翻社会主义制度；
- ✧ 煽动抗拒、破坏宪法和国家法律、行政法规的实施；
- ✧ 炒作评论社会敏感热点、非法组织串连、煽动集会游行的；
- ✧ 捏造或者歪曲事实，故意散布谣言，扰乱社会秩序；
- ✧ 发送危害国家安全、宣扬宗教极端势力的信息；
- ✧ 宣扬淫秽、色情、赌博、暴力、凶残、恐怖、教唆犯罪的；
- ✧ 破坏社会稳定的信息及损害国家、学院声誉和稳定的谣言；
- ✧ 其他违反宪法和法律、行政法规的。

3．内网应用服务器被非法入侵，应用服务器上的数据被非法拷贝、修改、删除，发生泄密事件。

4．在网站上发布的内容违反国家的法律法规、侵犯知识产权等，已经造成严重后果。

三、加大培训和宣传力度，加强和完善互联网安全管理，设置网络应急小组，采取统一管理体制，落实负责人。学院内各部门要建立健全内部安全保障制度，按照“谁主管、谁负责”、“谁主办、谁负责”的原则，落实责任制，明确责任人和职责，细化工作措施和流程，建立完善管理制度和实施办法，加强信息的审查和备案工作，确保网络与信息安全。

四、切实落实信息审查制度。若发现主页被恶意更改，应立即停止主页服务并恢复正确内容，同时检查分析被更改的原因，在被更改的原因找到并排除之前，不得重新开放主页服务。各二级学院、部门信息发布，必须落实责任人，实行审核制度，并具备相应的安全防范措施(如日志留存、安全认证、实时监控、防黑客、防病毒等)，加强网络设备日志分析，及时收集信息，排查不安定因素。建立有效的网络防病毒工作机制，及时做好防病毒软件的升级和病毒库的更新。

五、信息中心对校园网络实施 24 小时值班责任制，必要时实行远程控制。网络管理人员应定期对互联网的硬件设备进行状态检查。对用户上网进行监控，若发现有异常行为应立即关闭该用户的网络连接，及时记录在案，并对其警告和批评教育，严重违法行为立即上报有关部门。

六、强化突发事件的快速反应能力。网络管理员具体负责相应的网络安全和信息安全工作，不允许有任何触犯国家网络管理条例的网络信息，对突发的信息网络安全事件应做到：

1．及时发现、及时报告，在发现后在第一时间向上一级领导或部门报告。

2．保护现场，立即与网络隔离，防止影响扩大。

3．及时取证，分析、查找原因。

4．隔离有害信息，防止进一步传播，将事件的影响降到最低。

5．在处置有害信息的过程中，任何部门和个人不得私自保留、贮存、散布、传播所发现的有害信息。

6．追究相关责任。根据实际情况提出口头警告、书面警告、停止使用网络，情节严重和后果影响较大者，提交学校及国家司法机关处理，追究部门负责人和直接责任人的行政或法律责任。

七、及时整顿，加强防范。各部门要积极配合上级网络安全管理部门的例行检查，并接受其技术指导。针对网络存在的安全隐患和出现的问题，及时提出整治方案并具体落实到位，完善网络安全机制，防范网络安全事件再度发生。建立普洱学院网络信息安全管理长效工作机制，实现信息安全管理，创造良好的网络环境。

八、在重要、敏感时期，加大网络安全教育宣传力度，加强教职员工及学生的法律意识和安全意识教育，提高其安全意识和防范能力；开展安全文明上网的教育引导工作，净化网络环境，及时收集信息，排查不安定因素；密切保持与上级主管部门、电信部门和当地公安机关的联系，积极做好预防工作，发现问题及时处理，防患于未然。

九、做好机房、办公场所及户外网络设备的防火、防盗窃、防雷击、防鼠害等工作。若发生事故，应立即组织人员自救，并报警。

十、网络安全事件报告与处置。

事件发生并得到确认后，相关人员应立即将情况报告上级领导，由领导指挥处理网络安全事件，并及时向当地公安机关报案。阻断网络连接，进行现场保护，协助调查取证和系统恢复等工作，有关违法事件移交公安机关处理。