关于加强网络信息安全工作的意见

川工商院委〔2020〕18 号

为进一步加强和规范学校信息系统及网站的安全管理，保障学校各部门管理的信息系统、网站的安全正常运行，适应新形势下对网络信息安全管理的需要，根据《中华人民共和国网络安全法》《中国互联网管理条例》、教育部《关于加强教育行业网络与信息安全工作的指导意见》，结合学校实际情况，现就进一步加强我校网络安全工作提出如下意见：

一、加强学习，提高认识

学校各级党团组织和各部门要高度重视信息网络安全工作，严格遵守《中华人民共和国网络安全法》《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互联网管理暂行规定》《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》及我校有关网络管理规定，积极组织开展形式多样的《网络安全法》和网络管理规定学习宣传活动，进一步强化对“互联网+”时代加强网络安全教育工作重要性的认识，牢固树立“安全第一，预防为主”的思想，全面提高师生网络信息安全防范意识。

二、明确职责，压实责任

（一）进一步明确网络信息安全领导责任。按照“谁主管谁负责”“谁使用谁负责”“谁运行谁负责”的原则压实责任，学校信息技术中心负责学校网站群安全防护综合管理，开展网络信息安全检查，排查隐患，保障学校网络信息安全。各部门党政负责人是本部门二级网站网络信息安全第一责任人，负责本部门网站建设与管理，保障网络信息安全。各部门要进一步规范管理流程，设立网络安全管理员，向学校签订网络安全责任承诺书，报学校信息技术中心备案。

（二）进一步明确网络信息安全管理员责任。网络安全管理员负

责信息系统、部门二级网站信息管理及维护工作，并保证能随时、随地浏览本部门所管理的信息系统、网站信息，一经发现有异常内容或异常情况，能在 5 分钟以内处理或与学校信息化安全领导小组办公室（信息技术中心）取得联系。在信息系统、二级网站管理员发生变更时，应做好交接工作，及时与学校信息化安全领导小组办公室沟通，重新签订或登记变更信息。

（三）严格执行实名制认证上网要求。校园网用户必须严格遵守国家相关法律法规，必须本人实名认证上网，并对上网产生的一切行为负责。严禁将个人上网账号外借他人或作为公共账号使用，严禁私接路由器等共享上网设备。特殊教学、科研、办公等上网需求报信息技术中心审批。

三、加强建设，严格审核

（四）切实做好二级网站建设。各部门负责本部门二级网站和网页栏目与版面的设计建设管理及部门新闻信息、有关部门动态消息、部门通知、资料的审核及发布工作；二级网站、网页的版面的设计风格应与主页保持基本一致，各部门有权利自行设置栏目，信息技术中心负责整个网络的技术支持工作。

（五）严格审核信息发布内容。学校二级网站发布的所有信息和资料由本部门第一负责人审阅，对内容的合法性、准确性把关。涉及国家形势政策和学校的重要信息须经学校党委宣传部审阅后才能上传发布。各部门对所负责的信息系统、网站栏目中发布的内容，包括文字、图片、音像等一切信息负有责任，一旦出现问题，后果由本部门承担。

（六）强化信息发布的安全性。各部门要健全网站和信息系统信息发布审核和保密审查机制，以确保数据和信息发布的安全性、有效性。对上网信息（发布的文字、图片、音视频），应该由两人仔细核对无误后，再发布到网站上。根据系统、网站的重要程序，应该每天、

每周、每个月、每学期定期做好有关数据的备份工作。

四、严格管理，做好维护

（七）加强系统密码管理。各部门在信息系统正常部署完成后，应该修改系统后台调试期间的密码，不得继续使用工程师调试系统时所使用的密码；各部门要牢记系统密码并做好密码的保密工作，定期更改有关密码，注意密码的复杂度，至少 8 位以上，字母加数据加特殊符号的组合方式。管理员变更后，相关密码也应该随之变更。对于所管理的系统中的子帐号，在相关人员离职等原因不再管理时，应该将有关帐号禁用或删除，避免带来安全隐患。

（八）加强计算机终端安全管理。为保证系统的性能和运行的稳定性，在不影响业务的情况下，建议定期对服务器进行重启操作。要在服务器上安装杀毒软件，保证病毒库及时升级至最新版本，至少每周对操作系统进行一次病毒扫描检查、修补系统漏洞，清理未知可疑插件和临时文件，检查用户数据是否有异常（增加一些非管理员添加的用户），检查安装的软件是否有异常（不是管理员安装的未知程序），减少计算机被侵入的危险。正常工作日应该保证至少登录、浏览一次系统相关页面，及时发现有无被篡改等异常现象，特殊时间应增加检查频率。不用的信息系统及时关闭（如有些系统只是在开学、期末、某一阶段使用几天，寒暑假不使用的系统应当关闭）。

五、及时处置，迅速报告

（九）明确信息安全事件级别。根据《信息安全事件分类分级指南》（GB/T20986-2007，），将信息安全事件划分为四个级别：特别重大事件、重大事件、较大事件和一般事件。特别重大事件（Ⅰ级）是指能够导致特别严重影响或破坏的信息安全事件，主要包括会使特别重要信息系统遭受特别严重的系统损失，产生特别重大的社会影响。重大事件（Ⅱ级）是指能够导致严重影响或破坏的信息安全事件，主要包括会使特别重要信息系统遭受严重

的系统损失、或使重要信息系统遭受特别严重的系统损失，产生的重大的社会影响。较大事件（III级）是指能够导致较严重影响或破坏的信息安全事件，主要包括会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失、一般信息信息系统遭受特别严重的系统损失，产生较大的社会影响。一般事件（Ⅳ级）是指不满足以上条件的信息安全事件，主要包括会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失，产生一般的社会影响。

（十）事发处置与报告。若发生有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件和其他网络相关的安全事件等，学校信息技术中心应第一时间组织技术人员采取断网等有效处置措施，最大限度的降低安全损失和不良影响，同时保留现场，保全相关审计日志和证据，口头报告学校分管领导和主要领导，并按规定报告有管辖权的公安机关。学校对属于Ⅰ至III级安全事件的，应口头紧急报告省教育厅。紧急报告内容包括时间地点、简要经过、事件类型与分级、影响范围、危害程度、初步原因分析、已采取的应急措施。对Ⅳ级安全事件的，直接在四川省教育系统安管平台上报告。

（十一）事中处置与报告。学校信息技术中心对属于I至III级安全事件的，应在安全事件发现后2小时内填写《网络与信息安全事件情况报告》，《情况报告》由学校信息技术中心和运维单位共同编写，经学校主要领导审核后，以书面形式报告省教育厅。安全事件的事中处置包括：及时掌握损失情况、查找和分析事件原因，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。如果涉及人为主观破坏的安全事件应积极配合公安部门开展调查。

（十二）事后整改处置与报告。学校信息技术中心应在安全事件处置完毕后5个工作日内填写《网络与信息安全事件整改报告》，《整

改报告》由学校信息技术中心和运维单位共同编写，经学校主要领导审核后，以书面形式报告省教育厅。安全事件事后处置包括：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。如涉及人为主观破坏的安全事件应继续配合公安部门开展调查。

六、完善机制，严格奖惩

（十三）完善应急预案。学校信息技术中心要建立健全学校网络安全事件应急处置机制和值守制度，完善网络安全应急预案，定期组织应急演练，做到早发现、早报告、早控制、早解决。

（十四）加强隐患排查。学校信息技术中心要定期开展网络安全风险评估和隐患排查，通过自查、重点抽查、远程安全检测、现场检查等形式，分析主要风险和威胁，评估威胁应对能力，查找网络安全短板，掌握各部门重要信息系统的安全主体责任的落实情况。

（十五）建立奖惩机制。各部门要承担师生健康网络与信息安全的监管责任，对责任分工不明，超授权范围信息利用、不执行安全存储规定、未遵守安全审查制度、密码管理不善、应急处置不及时、整改不力、瞒报缓报等行为，由学校纪检监察部门依据规定对相关责任部门第一责任人和直接责任人进行约谈或通报问责；对发生重大信息泄露事件或极端事件，情节严重、违反法律法规，除承担法律后果外，将依法依规严肃追责问责。对师生健康网络与信息安全工作成果突出的部门和个人要适时总结，通报表扬。