人工智能学院
网站信息

安全管理制度

人工智能学院

2020 年 7 月

目　　录

.

网站安全管理责任人制度

1、网站实行使用责任人负责制，网站负责人负责网站整体安全、定期全面审核网站信息内容；各网站管理员全权负责本人网站模块下的信息、管理安全。

2、各管理员必须切实保障账号安全，不得随意将账号告知他人登录网站，修改内容。

3、不得随意将网站上的内部资料复制给他人使用。

4、网页编辑注重信息精确，不得附带与工作无关网页链接。

5、注重知识产权保护，不得上传有侵权可能性的信息资源。

6、出现网内突发互联网紧急事件，网站安全负责人应按相关法律法规和制度，先期开展工作，边处置，边报告，及时控制事态，防止扩大蔓延，尽可能减少和降低危害造成的损失。根据职责分工安排网站管理人员配合上级主管部门及公安部门保护现场，留存证据，及时恢复网站正常运行。

2020.7

.

信息发布、审核、登记制度

网站信息发布实行各信息发布模块负责人负责制，负责人审核批准，编辑人员具体实施的办法，在信息发布方面必须恪守如下规定：

1、发布申请应当确保发布信息准确、真实，符合国家有关的各项法律、法规制度；

2、信息发布人员应当对所发布的信息备案记录，以加强管理；

3、信息审核人员应在充分理解国家有关的各项法律、法规制度的基础上及时处理申请人员的请求，并将审核意见及时反馈给申请人员；

4、在审核人员同意的基础上应将信息及时转发给信息发布人员；

5、信息审核人员应当做好信息请求、处理、转发的备案工作；

6、信息发布人员对所收到的经过审核后的信息在确认审核意见后，应及时在网上发布，并确保发布信息的准确性；

7、信息发布人员对所发布的信息应当做好备案工作。

.

管理员账号登记和操作权限管理制度

为了保护我校校园网络系统的安全、促进人工智能学院网站的健康发展、信息的专业性、准确性、时效性，现制定本帐号使用登记和操作权限管理制度。

一、网站管理人员管理制度

1、根据具体分工，分模块安排网站管理人员；

2、网站管理人员需认真填写个人信息表，并保证其资料的真实性；

二、网络账户和操作权限管理制度

1、网站管理人员以外，其他任何人不得擅自操作、修改网站设置。

2、网站管理人员应当正确分配权限，并加口令予以保护，口令应定期修改，任何非网站管理人员严禁使用、猜测各模块管理员口令。

3、对于网站内容应做好备份工作，确保在系统发生故障时能及时恢复。

4、网站账户申请通过后将根据其日常工作要求设定固定的权限，严禁具有网络授权的管理人员私自提高个别用户的权限；

5、具有对网站内容进行添加、删除、修改等权限的用户需保护好自己的账户和密码，不得随意出借账户给其他用户。

.

安全管理人员岗位工作职责

为规范我院网站安全管理，现制定如下网站安全管理人员岗位工作职责。

一、 建立我院网站健全的安全管理组织：

1、学院院长为网站安全管理工作第一责任人，负责全面领导学院网站的防黄、防黑、防不良信息、防毒等网络安全工作；网站安全管理人员直接向院长负责；

2、学院信息发布明确到个人，网络安全管理人员须负责信息发布的信息安全审核；

二、 网站安全管理人员岗位日常管理职责：

1、网站安全管理人员应当保障网站信息安全，运行环境安全。保障网络系统的正常运行，保障信息系统的安全运行；

2、网站安全管理人员必须遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》；

3、网站安全管理人员必须接受并配合国家有关部门对本网站依法进行的监督检查；必须接受上级网络中心对其进行的网络系统及信息系统的安全检查；

4、网站安全管理人员负责网站安全和网上信息安全。如对网络安全和网上信息安全提出技术措施，须经上级网络中心批准后方可实施；

5、工作人员要树立安全第一的观念，遵纪守法认真贯彻执行《中

.

华人民共和国计算机信息网络国际联网管理暂行规定》和《计算机信息网络国际联网安全保护管理办法》,保护国家机密,净化网络环境;

三、网站安全管理人员岗位日常维护职责:

1、每日检查网站各模块,确保网站正常运行,内外网访问正常;

2、定期备份系统数据,仔细阅读记录文件,不放过任何异常现象;

3、规划、管理好各用户组,设定适当用户权限;

4、管理员密码和安全策略属网络中心核心机密,不得泄露;

.

应急处理——有害信息处理、上报制度

为规范对网内突发事件处理的方式，现制定如下制度：

一、互联网突发事件分类

互联网突发事件是指互联网络遭受破坏、损坏等意外因素导致重点网络系统瘫痪，大面积网络不能正常运行，大量用户数据丢失或修改，机密大量外泄等案件、事件或灾害。互联网突发事件可分为以下三类：

1、政治类突发事件：指境内外敌对势力、敌对分子和一些政治上别有用心的人利用互联网进行反动宣传渗透、造谣惑众，煽动制造政治动暴乱，以实现其破坏国家稳定、破坏社会主义制度、破坏经济建设、推翻党的领导的企图。

（1）社会发生局部动暴乱情况下，敌对分子利用互联网发布反动言论，甚至组织指挥对抗政府、危及国家安全的；

（2）制作、传播攻击党和国家领导人、损害国家声誉的政治谣言，大面积污染网络及用户的。

2、攻击类突发事件：指因计算机系统病毒感染、非法入侵计算机系统（黑客攻击）导致计算机网络大面积不能正常运行，重点网络系统瘫痪，机密大量外泄等情况。

（1）互联网遭受大规模病毒感染，导致网络不能正常运行的；

（2）非法侵入互联网，导致网络不能正常运行的；

（3）非法侵入国家事务、国防建设、尖端科学技术领域等重要

.

计算机信息系统，导致国家秘密、情报或军事秘密大量泄露，或不能正常运行的。

3、灾害类突发事件：指因爆炸、火灾、雷击等外力因素或自然因素导致机器设备损毁，系统瘫痪，网络无法运行。

（1）爆炸、火灾及其他破坏案件、事件导致网络不能正常运行的；

（2）遭受雷击等自然灾害，导致重要网络不能正常运行的；

4、其他因素导致重要网络不能正常运行，甚至瘫痪的案件、事件。

二、突发事件应急处置的职责分工

当遇有互联网突发事件，情况特别紧急，事态急剧恶化时，网站安全负责人应按相关法律法规和制度，先期开展工作，边处置，边报告，及时控制事态，防止扩大蔓延，尽可能减少和降低危害造成的损失。

1、网站安全管理人员必须做到及时发现、及时上报并配合学校网络中心安全管理人员对突发事件现场的保护措施实施以及对敏感地带的防控。

2、网站安全管理人员必须做到配合学校网络中心网络管理人员开展对网络的修复救援工作，加强对网络有害信息的封堵和过滤，通过多层次的网络安全和信息安全的技术防护体系，尽量确保突发事件期间网络正常运行。

三、突发事件应急处置流程

.

1、发现互联网信息安全和网络安全突发事件，应立即报告上级主管部门，同时保护现场，留存有关记录。

2、网站安全管理组织应立即按职责开展应急处置工作。

3、上级主管部门认为有必要时将组织相关部门人员立即赶赴现场，按照职责分工，与公安、安全等机关配合，对突发事件进行应急处理。

四、突发事件应急处置措施

1、政治类突发事件的应急处置：配合国家公安、安全机关迅速查明这类有害信息的来源，根据掌握的各种情报信息，分析判断敌对分子采用的技术手段，落实有效技术手段，切断其传播有害信息的渠道；同时要在取证后立即清除有害信息，必要时配合学校网络管理中心关闭、删除有关网页、节点内容，进行全面清理，并尽快恢复网站的正常秩序。

2、攻击类突发事件的应急处置：配合相关部门通过入侵检测和安全审计等方法确定病毒和黑客攻击使用的攻击技术方法，立即采取技术防范措施阻止攻击行为进一步造成危害，保护受攻击的网络现场，必要时应切断受攻击的网络链接；配合相关部门通过技术分析判断攻击者的来源，通过处置网络确定攻击者的地理位置，配合查找破案线索。

3、灾害类突发事件的应急处置：网站安全管理人员要立即上报单位、学校信息安全负责人，要立即赶赴现场处置，配合相关部门实行现场控制。在保护人员生命安全的前提下，控制对网络安全危害行

.

为的进一步发展，抢救的顺序依次是重要数据、重要设备、重要设施，尽快将它们转移到最安全的地方；启动网络安全应急设备和备份设备，组织技术人员和相关人员恢复网络工作环境，尽快使网络恢复正常秩序；配合相关部门查明灾难事故发生的原因，要尽快排除可能继续发生灾难事故的安全隐患，采取补救措施，保障网络安全。

.

网站安全管理机构设置

网站安全责任人：韦德泉、李中军

网站制作维护人：张家骏、胡修炎

网站信息发布人：张家骏、胡修炎、韩清华、裴霞、张强

网站信息审核人：李中军、杨振、张家骏

.