哈尔滨商业大学文件

哈商大〔2017〕71号

关于进一步加强校园网络信息安全管理工作的通知

校直各单位:

近年来，国家对网络信息安全管理的要求越来越高，高校已成为信息安全的重点防范区，我校的信息安全事件也呈增长趋势。近期，我校一些部门的网站和业务系统被检测到存在严重的系统漏洞，极易受到黑客的攻击和入侵，存在极大的安全隐患。为加强校园网络信息的安全管理，本着“谁管理谁负责，谁使用谁负责，谁运维谁负责”的原则，明确信息安全责任，现将有关要求通知如下:

一、强化信息安全责任制。各单位负责人为本单位网络信息安全的第一责任人;各单位信息化分管领导协调负责本部门业务系统建设和网络信息安全工作;各单位的信息安全管理员，负责本单位信息系统和网站信息的具体更新、维护和安全管理工作。

根据《中华人民共和国保守国家秘密法》《计算机信息系统国际互联网保密管理规定》《中华人民共和国计算机信息系统安全保护条例》《计算机信息网络国际联网安全保护管理办法》《互联网安全保护技术措施规定》等有关法律法规的规定，各单位须

签订《网络信息安全承诺书》（附件1）及《互联网服务安全责任书》（附件2）。各级信息安全人员如有调整须及时向网络与教育技术中心报备。

二、**加强网站、业务系统安全检测。**新建网站、业务系统在上线使用前，必须按流程进行安全检测，以防范潜在的安全风险，安全检测合格后方可上线运行（附件3）。对于已上线运行的网站、业务系统，各单位要加强管理，网络与教育技术中心会定期进行检测，如果存在安全漏洞，网络教育技术中心将及时通知相关单位，并根据安全漏洞的风险等级，采取相应的措施，避免造成安全事件。

三、加强域名的使用和管理。校内各域名使用单位不得擅自变更域名用途，不得用于申请之外的用途，如域名不再使用应及时注销。由于域名使用不当造成的安全问题，由域名使用单位负责。

四、加强网站论坛、留言板等互动平台的管理。各单位新建的网站，不设置论坛、留言板等互动功能；已有的互动平台，应实行严格的信息后台审核发布制度，不允许用户直接在前台发布信息。对于互动平台引发的信息安全问题，由所属单位负责。

附件：1.哈尔滨商业大学网络信息安全承诺书

2.哈尔滨商业大学互联网服务安全责任书

3.新建网站、业务系统上线运行流程

哈尔滨商业大学

2017年8月31日

附件 1

哈尔滨商业大学网络信息安全承诺书

根据《中华人民共和国保守国家秘密法》《计算机信息系统国际互联网保密管理规定》《中华人民共和国计算机信息系统安全保护条例》《计算机信息网络国际联网安全保护管理办法》《互联网安全保护技术措施规定》等有关法律法规的规定，本单位郑重承诺遵守本承诺书的有关条款，如有违反本承诺书有关条款的行为，由本单位承担由此带来的一切民事、行政和刑事责任。

一、本单位保证不利用网络危害国家安全、泄露国家秘密，不侵犯国家的、社会的、集体的利益和第三方的合法权益，不从事违法犯罪活动。

二、本单位承诺严格按照国家相关法律法规做好本单位网站的信息安全管理工作、本单位承诺健全各项网络安全管理制度和落实各项安全保护技术措施。

三、本单位承诺接受国家有关单位的监督和检查，如实主动提供有关安全保护的信息、资料及数据文件，积极协助查处通过国际联网的计算机信息网络违法犯罪行为。

四、本单位承诺不通过互联网制作、复制、查阅和传播下列信息:

1.反对宪法所确定的基本原则的。

2.危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的。

3.损害国家荣誉和利益的。

4.煽动民族仇恨、民族歧视，破坏民族团结的。

5.破坏国家宗教政策，宣扬邪教和封建迷信的。

6.散布谣言，扰乱社会秩序，破坏社会稳定的。

7.散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的。

8.侮辱或者诽谤他人，侵害他人合法权益的。

9.含有法律、行政法规禁止的其他内容的。

五、本单位承诺不从事下列危害计算机信息网络安全的活动，包括但不限于:

1.未经允许，进入计算机信息网络或者使用计算机信息网络资源的。

2.未经允许，对计算机信息网络功能进行删除、修改或者增加的。

3.未经允许，对计算机信息网络中存储或者传输的数据和应用程序进行删除、修改或者增加的。

4.故意制作、传播计算机病毒等破坏性程序的。

5.其他危害计算机信息网络安全的。

六、本单位承诺，当计算机信息系统发生重大安全事故时，立即采取应急措施，保留有关原始记录，并在24小时内向政府监管部门报告，并书面告知网络与教育技术中心。

七、若违反本承诺书有关条款和国家相关法律法规，本单位直接承担相应法律责任，造成财产损失的，由本单位直接赔偿。同时，网络与教育技术中心有权暂停提供接入服务直至解除双方间租用协议。

八、本承诺书自签署之日起生效并遵行。

单　位　公　章:

负　责　人　签　字:

信息化分管领导签字:

信息安全管理员签字:

日　　期:

注：业务系统和网站如果由不同人员管理，可在信息安全管理员处增加签字人员

附件 2

哈尔滨商业大学互联网服务安全责任书

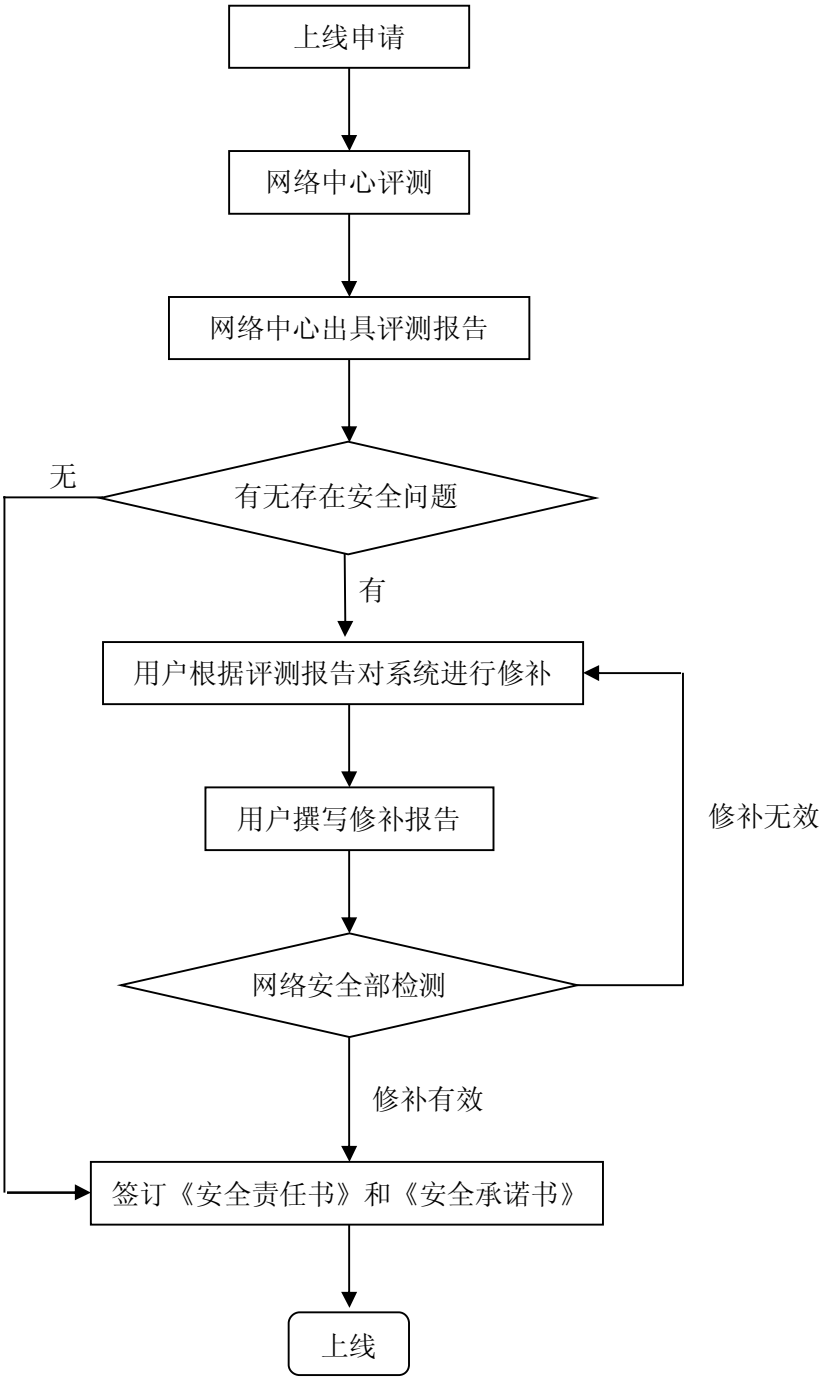
服务名称: **编号:**

<table>
<tr><td>单位名称（盖章）</td><td colspan="5"></td></tr>
<tr><td rowspan="2">单位负责人
（签字）</td><td rowspan="2"></td><td rowspan="2">职务</td><td rowspan="2"></td><td>手机</td><td></td></tr>
<tr><td>邮件</td><td></td></tr>
<tr><td rowspan="2">信息化分管领导
（签字）</td><td rowspan="2"></td><td rowspan="2">电话</td><td rowspan="2"></td><td>手机</td><td></td></tr>
<tr><td>邮件</td><td></td></tr>
<tr><td rowspan="2">信息安全管理员
（签字）</td><td rowspan="2"></td><td rowspan="2">电话</td><td rowspan="2"></td><td>手机</td><td></td></tr>
<tr><td>邮件</td><td></td></tr>
<tr><td colspan="6">为保证校园网络与信息安全，维护学校稳定和国家安全，保守国家秘密，按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则切实落实网络与信息安全责任，本单位在进行互联网服务期间，承担如下责任:
遵守国家法律法规和校内有关规章制度，建立信息安全保密制度和用户信息安全管理制度，依法提供网络信息服务。
在校外托管、校内自管的网站和系统及数据中心物理服务器托管须设置安全可靠的防火墙，web 防护，入侵检测、防病毒等安全技术措施并定期升级，定期进行安全风险分析与系统漏洞测试，适时对系统、软硬件进行升级，修补系统漏洞确保系统安全、可靠、稳定地运行。
校内虚拟服务器托管须定期进行安全风险分析与系统漏洞测试，适时升级系统、应用软件，修补漏洞，确保系统安全、可靠、稳定地运行。
不在网上制作、复制、发布、传播《互联网信息服务管理办法》第十五条规定的禁止事项。发现有害信息，按照法律法规有关规定及时报告和处理，并报告学校网络与信息中心。严格遵守国家《保密法》等有关法律法规，不得泄漏国家秘密，不得泄漏用户个人资料。
校内各系统各网站上线前必须报网络与教育技术中心进行安全检测，未通过安全检测的系统一律不得上线运行。系统运行后，网络与教育技术中心有权对各系统进行安全扫描、漏洞测试及渗透测试，对于有严重问题的有权进行停止网络服务，停止联网后由网络中心下达安全通报。使用单位须进行安全加固并提交整改报告，经检测合格后，方能重新开放。
建立紧急响应机制，落实网络信息安全责任人联系制度，保证学校管理部门可以通过电话随时与信息安全主管领导、技术负责人及联系人沟通联系。
对于设有电子公告栏、留言板等交互式信息栏目的网站，应加强内容审核，及时发现和删除各类有害信息，确保网站信息安全。加强监控，一旦发现网站有被篡改、植入木马、修改链接等情况，应立即采取紧急措施：关闭网站以消除不良影响；保存被修改内容及系统日志；及时向上级领导、网络与教育技术中心报告；认真查找网站安全漏洞，增加安全措施，恢复正常内容。经安全检测后网站才能重新上线。
对互联网管理部门及相关国家主管机关要求删除的违法、有害信息，必须立即执行。相关责任人和联系人发生变更时，须第一时间报告学校网络与教育技术中心。电话 84865124，邮件 security@hrbcu.edu.cn。</td></tr>
</table>

注：本表一式两份，学校与各部门各执一份；业务系统和网站如果由不同的人员管理，请根据服务名称另行填报责任书。

附件 3

新建网站、业务系统上线运行流程



哈尔滨商业大学党公室　　2017 年 8 月 31 日印发