东 北 大 学 文 件

东大信网字〔2022〕7号

关于进一步加强网络安全防护工作的通知

各部门:

近期网络安全形势十分严峻，为贯彻落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》和教育部、公安部有关工作要求，全力防风险保安全护稳定，保障重要时期校园网络安全，为党的二十大胜利召开营造良好环境，现就进一步加强网络安全防护工作通知如下。

一、落实网络安全责任制

根据《东北大学网络安全管理办法（试行）》的规定，各部门主要负责人是本部门网络安全第一责任人；各部门主管网络安全的领导班子成员是直接责任人。各部门要在党的二十大召开前

召开一次网络安全专题会议，研究完善部门内部网络安全管理制度，建立数据安全管理与个人信息保护管理机制，梳理本部门信息资产清单，明确人员分工及责任划分，制定应急预案与值守方案，增强师生员工网络安全意识，切实做到领导到位、责任到位、人员到位和措施到位。

各部门请于9月27日前领取纸质《东北大学网络安全承诺书》一式两份，在9月30日前完成签订并返回一份。南湖校区领取返回地点为计算中心403室，浑南校区领取返回地点为图书馆D105室。无法领取纸质承诺书的，可自行打印电子版承诺书（详见附件），在9月30日前完成签订后报信网办网络安全部。

二、开展网络安全自查

各部门要在9月30日前完成网络安全自查工作，及时发现并消除安全风险。《网络安全自查情况表》将通过学校“一号通”平台下达到各部门网络安全联系人，请在9月30日17:00前按要求完成填报工作。

（一）开展信息资产审查备案

信网办将向各部门网络安全联系人发送“已备案的网络安全负责人和分管领导信息”“已备案网站和信息系统信息”“已备案LED电子显示屏信息”“已备案网络打印机信息”，各部门应及时确认备案信息资产是否有变化，如有新增或撤销信息资产，请于9月30日前报信网办网络安全部更新。

（二）清理“僵尸”信息系统

“僵尸”信息系统网络安全风险极高，容易被不法分子攻击利用甚至作为跳板攻击校内其他信息资产，请各部门认真研判识别并进行清理。按照教育部文件要求，符合以下条件之一的信息系统即为“僵尸”信息系统:

1.业务应用脱节，承载业务已停止或变更，不再通过该信息系统办理;

2.资源长期闲置，页面内容或者数据长期未更新，最近1年内访问量低;

3.运维停止，无专人运维或运维缺乏基本保障，安全问题长期不能修复。

（三）清理“双非”信息系统

“双非”信息系统指未经立项、未按校内信息化项目建设流程建设，使用非学校域名、非学校IP地址建设的信息系统（包括信息系统、移动APP等）。按照《东北大学网络安全管理办法（试行）》，“双非”信息系统不属于学校官方行为，一切网络安全责任由系统建设、使用部门和建设、使用人员承担。在校外部署的各类测试、演示系统不得使用学校标识及学校数据，测试、演示任务完成后应及时撤销删除。

请各部门开展“双非”信息系统排查，对于排查出的此类系统，如不再使用应注销和关闭；如仍需使用，请按照学校信息化建设管理规定进行建设或迁移至校内。

（四）加强校内各类办公账号密码安全

各类办公账号密码包括本部门主管的信息系统管理后台、数据库、办公邮箱、办公计算机、网络打印机、LED 电子显示屏、网络摄像头、网络设备等软硬件设备的密码。

各部门要加强办公密码安全管理，严禁使用简单密码、默认密码、通用密码，杜绝诸如密码长度不足、密码复杂度不足、使用生日和电话作为密码、使用设备或信息系统的默认密码、使用身份证号和学工号等有规律的密码等问题。

请各部门在 9 月 30 日前清除离职离岗人员办公账号权限，确认各信息系统分配高权限账号是否最小必要，排查所有办公密码强度，确保所有办公密码均已设置为强密码，密码长度应在 8 位以上，包含数字、大小写字母及特殊字符的三种及以上。

特别注意，将密码存放在各种互联网网盘或者将代码托管到 Github 等代码共享平台，存在严重的安全隐患。请各部门提醒师生不要将密码通过各种互联网网盘和代码托管平台共享。

（五）检查各服务器的安全配置状况

服务器配置是服务器安全的基础，配置不当会产生各类安全隐患，服务器应本着专用、最小化、合法合规等原则进行安全配置。请各部门组织运维人员对主管信息系统的服务器配置进行排查，包括:

1.是否安装与应用服务无关的软件;

2.是否安装远程控制软件，如 Teamviewer、向日葵、Todesk 等;

3.是否安装盗版软件或非官方渠道下载、更新的软件;

4.是否有非必要的服务、端口开启;

5.应用服务所用软件和中间件是否为安全版本;

6.访问控制范围是否为最小;

7.服务器中的代码和数据是否进行异地备份;

8.Web 应用系统访问日志是否至少保留 180 天。

（六）加强 LED 电子显示屏、网络摄像头等物联终端的管理

各部门应加强本部门主管的 LED 电子显示屏、网络摄像头等物联终端的管理，明确专人负责相关设备管理及信息发布，保障设备安全，避免出现不良信息发布或敏感信息泄露。

加强 LED 电子显示屏信息发布管理，原则上 LED 电子显示屏不得联网管理，如确需联网必须接入专网，不得与校园网、互联网连通。网络摄像头的部署应经过部门领导审批，明确用途且用途合理合法，严格控制访问权限，及时进行安全更新，加强设备使用监控，避免摄像头非授权、超范围使用，任何个人不得随意在校内公共场所部署网络摄像头，避免各类通过摄像头造成的敏感信息泄露等安全问题。

（七）加强专网的网络安全管理及运维

各部门如主管的信息系统使用专网，应建立专网网络安全管理运维机制，并在此次自查工作中对专网网络安全状况进行彻底检查，检查内容包括：严格执行专网设备和系统的补丁升级和漏洞修复，关闭不必要端口、共享访问及远程桌面连接，安装并及

时升级杀毒软件等。

（八）开展网站外链排查整改

过期或失效外链网站的域名容易被不法分子抢注而指向黑链、毒链、黄链等非法网站，存在严重安全隐患。请各部门在9月30日前对本部门的网站和具有信息发布功能的信息系统进行全面排查，检查确认各种外链是否必要、是否合法、是否有备案号，对无必要、无法确认合法性或已失效的链接进行删除。对于添加非gov.cn（政府类)和edu.cn(教育类）以外域名的网站链接，请登记造册，并至少每月自查一次。对于具有时效性的文章可在文章编辑时设置文章“发布时间”和“过期时间”，以降低“外链”风险。

（九）加强自建服务器集群安全管理

前期在学校安全检查中发现，校内某部门自建服务器集群存在严重安全隐患，管理人员安全意识较为薄弱，如被攻击利用将造成严重后果。各部门应引以为诫，加强自建服务器集群的安全管理，严格按照网络安全等级保护要求落实网络安全责任制，健全管理制度，制定重要时期网络安全保障方案，提高网络安全威胁应对能力，坚决遏制网络安全重大事故发生。应指定专人负责自建服务器集群的运维监测、数据安全及个人信息保护等工作，对于服务器使用者进行实名登记，对其操作进行审计，确保可管可控。

自建服务器集群的部门负责服务器集群网络安全工作的具

体落实，对出现的网络安全问题承担直接责任。请存在自建服务器集群的部门在9月30日前完成信息资产备案，确保应备尽备，学校将根据备案信息进行检查。备案地址：https://ehall.neu.edu.cn/db_portal/guide?id=16E7E900-BABB-4001-B337-C20C7D362206。

（十）自建信息服务排查

请各部门排查本部门及本部门师生员工是否有自建且未经信网办审核备案的校园网信息服务，此类信息服务不得接入校园网，不得使用学校资金、数据中心、域名、IP 地址建设，不得使用校名、校标等学校标识，一切网络安全责任由信息服务建设、使用部门和建设、使用人员承担。如实属必要，请向信网办申请备案，在学校完成审核备案和安全检查前应停止运行。

（十一）排查虚拟货币“挖矿”活动

日前，根据上级部门监测和学校网络设备分析发现，仍有师生因中“挖矿”木马而进行被动“挖矿”。请各部门组织师生在9月30日前对个人电脑和服务器开展一次安全检查，使用主流杀毒软件进行一次全盘病毒查杀。师生电脑和服务器应安装正版操作系统和应用软件，安装杀毒软件和主机防护类软件，定期检查CPU/GPU利用率和能耗情况，禁止安装各类破解版软件，并关停已停止服务或使用的电脑和服务器。如发现个人电脑或服务器被“挖矿”木马控制且无法自行处理的，可与信网办联系解决。

（十二）加强数据安全及个人信息保护工作

各部门需认真核查是否已落实数据安全保护措施、是否存在损害个人信息安全的情况。各业务系统应采取存储加密、限制数据访问授权、杜绝数据库违规外联、审计数据操作行为、开展重要数据备份等措施，严防类似国内某高校数据遭窃取事件。

各部门进行师生个人信息采集、使用、存储、共享、删除等处理活动时要严格按照国家法律法规进行，对在互联网中传播、存储的个人信息要展开清查，禁止在各类即时通讯软件、APP、公众号、网站等公开共享未经去标识化处理的师生个人信息。

通过外包服务方式进行服务运维的，应规范外包服务活动的数据安全责任，签订《数据保密协议》，要求外包服务单位不得以任何方式在任何时间、地点对第三方泄露项目数据和个人信息等。

（十三）开展高危漏洞动态清零

前期信网办已组织技术人员对学校备案信息系统进行拉网式的安全检查，对发现的疑似高危漏洞已通过邮件通报至各部门网络安全联系人。目前部分部门已完成整改和反馈，请尚未完成整改的部门高度重视此项工作，实现高危漏洞动态清零。请各部门在 9 月 30 日前完成整改工作，并将整改加固报告发送至 security@mail.neu.edu.cn。

三、工作要求

党的二十大即将召开，网络安全责任重大，各部门要从政治的高度深刻认识网络安全保障工作的紧迫性和重要性，突出问题

导向，全面从严管理，狠抓责任落实，着力发现和防范网络安全风险，认真完成各项检查整改任务，及时报送工作进展材料，切实提升本部门网络安全防护的能力和水平。

附件：东北大学网络安全承诺书

东北大学

2022 年 9 月 23 日

东北大学校长办公室　　2022年9月23日印发