校园网络安全综合治理方案

近年来，按照国家网络安全的总体部署，在全校各单位的共同努力下，网络安全形势明显好转，工作机制基本建立，防护能力不断加强。与此同时，我校机构多、系统多，网络安全工作仍存在许多问题，主要表现在：安全责任不落实、管理不规范、安全隐患修复不及时、监测预警和应急响应能力不足、网络安全事件时有发生等。这些问题给学校声誉造成了不良影响，同时危害到师生的切身利益。

为全面贯彻党中央、国务院、教育部关于网络安全的统筹部署，落实《网络安全法》，迎接党的十九大胜利召开，按照学校网络安全工作委员会统一部署，自2017年6月至10月，网络与信息中心（以下简称信息中心）将在全校开展网络安全综合治理行动，综合治理行动方案如下：

一、工作目标

各单位应落实网络安全责任制，加强组织管理，加强对网站乱象的治理、堵塞安全漏洞、规范安全管理，从而全面提升教育行业网络安全水平，增强信息系统防护能力，有效防范和抵御安全风险隐患，切实保障信息系统（网站）稳定运行和数据安全。

二、工作内容

**（一）落实安全责任制，加强组织管理。**

各单位应充分认识开展综合治理行动的重要性和紧迫性，将工作纳入重要议事日程予以部署，明确主管责任人，提供必要的工作保障，确保各项工作落到实处。同时，各单位需填报《网络安全联络通讯录》（附件1），主要负责人需签订《中国矿业大学网络安全承诺书》(附件2)和《中国矿业大学虚拟机服务协议书》（附件3），并于9月20日前将纸质材料连同电子版报送信息中心。

**（二）治理网站乱象，强化主体责任。**

**1.开展网站域名、虚拟机清理工作。**信息中心将信息系统登记表（附件4）下发给各单位，各单位根据实际情况对网站的域名、虚拟机进行清理和补充，网站安全责任人如有变更，需更新人员相关信息，并于9月20日前将纸质材料连同电子版报送信息中心。

1. **进一步落实网站统一管理工作。**各单位及单位下属部门的网站应统一纳入学校站点群平台，集中规范管理，提高安全保障。（2017年9月底前完成）
2. **加强网站信息发布管理。**各单位应定期全面检查网站信息发布情况，如有发布的信息中存在法律和行政法规禁止发布或传输的信息、涉及个人隐私和单位秘密的信息，应采取删除或更正等措施立即整改。
3. **规范虚拟机申请、管理工作。**

信息中心从即日起，仅对各单位用于教学、科研、管理用途的信息系统分配虚拟机，不再对新闻网站或个人分配虚拟机。各单位所属虚拟机的重启、开机、关机操作，由各单位的网络安全管理员统一负责，信息中心依据单位上报的《网络安全联络通讯录》为网络安全管理员分配账号。

**（三）堵塞安全漏洞，增强防护能力。**

**1.加固系统安全。**各单位应对本单位主管的服务器（虚拟机），开展常态化维护，定期更新操作系统补丁，定期进行病毒、木马扫描。操作系统及网站管理后台如存在弱密码问题，应及时更换密码。

**2.全面监测网络安全威胁。**各单位应对本单位主管的信息系统（网站），利用360等免费在线监测平台或采取其他措施，开展常态化监测，发现存在漏洞、后门、暗链、弱口令等安全威胁的信息系统（网站），应及时修复、跟踪复测整改结果，尽快消除安全隐患。

**3.有序推进通报整改。**信息中心接收来自教育部、公安机关等部门通报的安全事件通报，及时通知相关单位，为避免事态恶化，信息中心将采取断开WEB服务等措施，相关单位应深入查找薄弱环节，及时整改修复，并将整改报告报送信息中心，信息中心确定安全隐患消除后恢复WEB服务。

**（四）规范安全管理，提升治理水平。**

**1.加强和规范数据管理。**各单位应规范数据采集、存储、使用和开放共享，对重要数据进行加密存储和加密传输，对应用程序及数据进行异地备份。

**2.健全网络安全事件应急响应机制。**各单位应组织学习学校网络安全应急预案，建立安全事件分级响应、跨部门协同处置的工作机制，重大安全事件需上报信息中心。

**3.开展宣传教育，提升安全意识。**各单位应组织开展网络安全宣传教育，面向网络安全管理人员和上网人员开展专题培训，切实提高网络安全意识、管理水平和防护能力。

网络安全联系人：网络与信息中心王老师

办公电话：83592122

办公地址：南湖校区图书馆大楼822室

附件报送邮箱：security@cumt.edu.cn

网络安全QQ群：32470702（中国矿大网管群）

站点群联系人：网络与信息中心赵老师

办公电话：83590047

办公地址：办公楼C603

邮箱：zd530520@cumt.edu.cn

附件：1. 网络安全联络通讯录

1. 中国矿业大学网络安全承诺书
2. 中国矿业大学虚拟机服务协议书
3. 各单位信息系统登记表

网络安全工作委员会

2017年6月29日

附件1

**网络安全联络通讯录**

单位：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网络安全负责人 | 姓 名 |  | 职务 |  |
| 办公电话 |  | 移动电话 |  |
| 邮箱地址 |  | | |
| 网络安全管理员 | 姓 名 |  | 职务 |  |
| 办公电话 |  | 移动电话 |  |
| 邮箱地址 |  | QQ |  |
| 工号 |  | 身份证号 |  |

**附件2**

**中国矿业大学网络安全承诺书**

网络安全工作委员会：

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。

1. 本单位承诺遵守《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》和《信息安全等级保护管理办法》、《网络安全法》及其他国家有关法律、法规和行政规章制度。
2. 本单位已知悉并承诺执行学校《中国矿业大学网络信息安全管理办法（试行）》的文件规定。
3. 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。
4. 本单位承诺建立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。
5. 本单位承诺加强终端计算机安全，落实软件正版化，推进具有自主知识产权的软硬件应用，规范工作人员的使用行为。
6. 本单位承诺规范本单位数据采集和使用，不采集超越职能范围的数据，保障数据安全。
7. 本单位承诺提升应急响应能力，制定本单位应急预案，组织开展应急演练。
8. 本单位承诺对本单位的信息系统进行安全监测，并对监测发现和通报的安全问题进行限时整改。
9. 本单位承诺加强信息技术安全教育，组织工作人员参加培训，提高管理人员的安全意识和技术人员的防护能力。
10. 本单位承诺当信息系统发生信息技术安全事件，迅速进行报告与处置，将损害和影响降到最小范围，并按照要求及时进行整改。
11. 若违反本承诺书有关条款和国家相关法律法规的，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。
12. 本承诺书自签署之日起生效。

主要负责人（签字）：

单位盖章：

年月日

**附件3**

**中国矿业大学虚拟机服务协议书**

甲方：网络与信息中心

乙方：\_\_\_\_\_\_\_\_\_\_\_\_\_\_

为了方便学校各二级单位建立用于公共教学、管理、科研用途的业务系统，节省购买服务器与存储的费用以及后续能耗费，甲方为乙方（不包括个人）免费提供虚拟机租用服务。为明确甲、乙双方的责任、义务，特签定本协议。

1. 乙方申请的虚拟机限定用于存放信息系统，新闻性质的网站需通过站点群平台建站。
2. 甲方数据中心机房提供高速可靠的网络接入和标准动力环境，所有虚拟机由于网络安全设备提供集中安全防护。
3. 甲方在乙方提交虚拟机服务申请表和协议书后一周内为乙方开通虚拟机。
4. 甲方为乙方开通虚拟机后，向乙方提供虚拟机的IP地址和管理员账号及初始密码，乙方自行妥善保管，后期可更换账号和密码，甲方不提供恢复密码服务。如乙方遗忘、外泄密码而造成的损失，由乙方自行承担责任。
5. 甲方为乙方提供初次操作系统的安装，应用软件乙方可通过远程桌面自行安装。
6. 乙方利用虚拟机存储和发布的信息必须遵守国家相关的法律法规，未经有关部门同意，严禁在服务器上私设代理、论坛、邮件、DNS等类似的服务。若发生以上现象经查明后，甲方有权关闭虚拟机，情节严重的上报学校或移交公安机关处理。
7. 乙方负责虚拟机上操作系统和应用程序的安全防护和补丁更新，自行备份网站数据，如虚拟机因乙方维护不当或被黑客攻击，导致虚拟机崩溃、网站数据被篡改或丢失，乙方自行承担损失。
8. 甲方如发现乙方虚拟机因存在中病毒、木马、主动或被动攻击等安全问题影响校园网络正常运行，及时向乙方反馈，甲方有权暂时关闭服务器直到乙方解决为止。
9. 如因线路故障、停电、自然灾害等不可抗力因素造成的虚拟机服务中断，甲方不承担责任；如甲方因工作需要，对网络重新调整造成的服务中断，甲方会提前通知乙方，乙方必须无条件配合，不得追究甲方责任。
10. 乙方自行解决虚拟机上所安装的软件版权，乙方对使用虚拟机所引起的任何经济、政治、法律等纠纷负完全责任，与甲方没有任何关系，甲方也不应对此或对第三方承担任何责任或者义务。
11. 本协议一式两份，甲乙双方各执一份，自签字之日起生效.两份具有同等法律效力。

主要负责人（签字）：

单位盖章：

年月日

**附件4**

**各单位信息系统登记表**

格式如下，电子版将通过邮件方式发送给各单位网络安全管理员。

