**关于做好网络安全自查和防护工作的通知**

为贯彻落实上级关于做好党的二十大网络安全保障工作的要求，切实提高各单位应对网络安全风险能力和水平，现将有关事项通知如下：

1. **落实网络安全责任**

各单位主要负责人为网络安全第一责任人，应指定本单位教师担任网络信息安全管理员和上网行为管理员，网络信息安全管理员负责信息系统网络安全自查，上网行为管理员负责上网行为安全自查。

上网行为管理员负责统计本单位师生、实验室、机房电脑的数量，确保联网电脑安装开启杀毒软件和防火墙，接到协查的通知后，负责监督相关人员完成整改工作。网络信息安全管理员在二十大重要保障期间（至10月29日），负责每天的网络安全“零报告”工作，按要求回复信息化中心公众号推送的消息，发现异常第一时间与信息化中心取得联系。

1. **信息系统网络安全自查内容**

**1.站群中的网站**

|  |  |  |
| --- | --- | --- |
| 项目 | 内容 | 措施 |
| 自查 | 管理员账号 | 修改网站后台管理的弱密码，删除停用的账号。 |
| 值守巡检 | 网站篡改信息审查 | 1. 仅在工作时间更新网站；
2. 核查微信中收到的网站文件变化预警信息；
3. 每天检查网站是否被篡改；
4. 审查发布的信息，确保信息的真实性和准确性;
5. 不在网站上发布个人感信息和工作秘密;
6. 检查网站外部链接的有效性和合法性。
 |

**2.信息系统（自建网站、业务系统、移动APP、公众号应用、微信小程序）**

|  |  |  |
| --- | --- | --- |
| 项目 | 内容 | 措施 |
| 自查 | 弱口令 | 未对接学校统一身份认证的信息系统暂停服务。 |
| 合规性 | 1.相关日志留存至少6个月，对重要文件和数据库进行备份；2.关闭非学校IP地址和域名的信息系统；3.关停长期闲置、停止运维更新的“僵尸”系统；4.未做备案的系统关停。 |
| 个人敏感信息存储 | 1.严禁存储师生非必要个人敏感信息，如确有需要，应加密存储，未加密前应关停；2.严禁将师生个人敏感信息存储到校外。 |
| 安全漏洞 | 修复业务系统程序漏洞前关停服务。 |
| 值守巡检 | 信息系统篡改信息审查 | 1. 仅在工作时间更新网站；
2. 每天检查信息系统是否被篡改；
3. 确保信息的真实性和准确性;
4. 检查系统外部链接的有效性和合法性。
 |

**3.托管到信息化中心的设备（服务器、虚拟机、存储）**

|  |  |  |
| --- | --- | --- |
| 项目 | 内容 | 措施 |
| 自查 | 弱口令及口令泄露 | 1. 更新各托管服务器或虚拟主机负责人的口令，确保口令强度，严禁使用默认密码；
2. 操作系统管理权限只能在校内访问；
3. 重保时期只能在工作时间更新。
 |
| 巡检 | 合规性 | 1. 确保杀毒软件和防火墙等防护措施有效；
2. 备份设备配置文件并妥善保管；
3. 更新操作系统的安全补丁；
4. 确认日志留存至少6个月。
 |

**4.接入校园网的终端设备（个人电脑、服务器、打印机、打印服务器、路由器、自助设备、摄像头、LED公共区域显示屏）**

|  |  |  |
| --- | --- | --- |
| 项目 | 内容 | 措施 |
| 自查 | 弱口令 | 定期更新管理账号的密码，确保口令强度，严禁使用默认密码。 |
| 巡检 | 合规性 | 1. 更新病毒库，开启防火墙；
2. 安装最新的操作系统安全补丁；
3. 下班时关闭非必要开机的联网设备。
4. 断开LED显示屏的物理网络连接
 |

1. **上网行为安全自查**

|  |  |  |
| --- | --- | --- |
| 自查项目 | 范围 | 防范措施 |
| 自查 | 电脑、邮箱、社交媒体的账号密码 | 1. 不使用弱密码、默认密码；
2. 密码至少8位字符，同时包括大小写字母、数字和特殊符号；
3. 不同类别账号使用不同的密码；
4. 办公邮箱严禁使用办公电话做密码
5. 安装杀毒软件，开启防火墙
6. 定期更新操作系统、病毒库和软件的升级补丁。
7. 开展防钓鱼邮件教育培训
 |

1. **报送要求**

请各单位高度重视，于10月14日下班前将自查表电子版和签字盖章扫描件以电子邮件形式发送至ic@cust.edu.cn如有疑问请与信息化中心联系，联系电话：85582445。

**附件： 一、信息系统安全自查表**

**二、上网行为安全自查表**

**三、关于加强上网行为安全的建议**

**四、吉林省教育厅关于进一步做好重要时期网络安全保障工作的通知**

信息化中心

2022年10月13日

**附件一：**

**信息系统安全自查表**

|  |  |
| --- | --- |
| 部门名称 |  |
| 网络信息安全管理员 | 姓名 |  | 职务/职称 |  |
| 办公电话 |  | 移动电话 |  |
| 需要自查的信息系统包括：站群网站、自建业务系统、自建网站、移动应用 |
| 序号 | 自查项目 | 落实情况 |
| 已落实 | 落实中 | 未落实 |
| 1 | 管理员口令保证密码强度（8位以上，包含大小写字母、数字和特殊符号） | 🞎 | 🞎 | 🞎 |
| 2 | 重保时期网站只在工作时间更新 | 🞎 | 🞎 | 🞎 |
| 3 | 发布的信息确保真实、准确且不包含个人敏感信息和工作秘密 | 🞎 | 🞎 | 🞎 |
| 4 | 网站外部链接合法且有效 | 🞎 | 🞎 | 🞎 |
| 5 | 关闭校外自建系统 | 🞎 | 🞎 | 🞎 |
| 6 | 数据、程序和配置完成备份 | 🞎 | 🞎 | 🞎 |
| 7 | 日志留存6个月 | 🞎 | 🞎 | 🞎 |
| 8 | 更新服务器操作系统的补丁 | 🞎 | 🞎 | 🞎 |
| 9 | 修复以发现的程序高危漏洞 | 🞎 | 🞎 | 🞎 |
| 10 | 已安装杀毒软件并保持病毒库最新、开启防火墙 | 🞎 | 🞎 | 🞎 |
| 11 | 物理断开LED屏的网络连接 | 🞎 | 🞎 | 🞎 |
| 主 要 负 责 人：网络信息安全管理员： 公章： 年 月 日 |

**附件二：**

**上网行为安全自查表**

|  |  |
| --- | --- |
| 部门名称 |  |
| 上网行为管理员 | 姓名 |  | 职务/职称 |  |
| 办公电话 |  | 移动电话 |  |
| 教师电脑数量 |  |
| 教师邮箱数量 |  |
| 机房和实验室电脑数量 |  |
| 学生电脑数量 |  |
| 序号 | 自查项目 | 落实情况 |
| 已落实数量 | 落实中数量 | 未落实数量 |
| 1 | 电脑设置复杂登录口令 |  |  |  |
| 2 | 安装并开启杀毒软件和防火墙 |  |  |  |
| 3 | 教师邮箱修改为复杂口令 |  |  |  |
| 4 | 部门邮箱修改为复杂口令 |  |  |  |
| 序号 | 自查项目 | 落实情况 |
| 已落实 | 落实中 | 未落实 |
| 1 | 开展防范钓鱼邮件教育 | 🞎 | 🞎 | 🞎 |
| 2 | 开展安全使用个人电脑教育 | 🞎 | 🞎 | 🞎 |
| 主 要 负 责 人：上网行为管理员： 公章： 年 月 日 |

**附件三：**

### 关于加强上网行为安全的建议

1. 保护个人的网络信息隐私，不将本人的网络账号、邮箱账号、身份证号码、手机号码、微信或QQ账号、银行卡号等泄露给他人非法使用；

2. 防范钓鱼邮件攻击，注意检查核实邮件来源，不轻信更新专家信息、填写获奖信息等邮件内容，如果无法确认来源，不打开邮件中的链接，不下载邮件中的附件，发现来历不明的邮件请直接删除；

3. 防范木马及病毒攻击，安装杀毒软件（例如360，下载地址：https://sd.360.cn/,火绒，下载地址：https://www.huorong.cn/）并开启实时防护，经常对个人电脑进行病毒扫描。开启防火墙，定期更新系统补丁，不随意打开非法的网站及来历不明的网页链接，不下载安装来源不明的软件和程序；

4. 对电脑操作系统及常用软件进行定期升级，避免安全漏洞造成的病毒感染。请选择正规网站下载安装；

5. 使用本人的校园网帐号联网，不代理、不共享，以免发生网络安全事件时影响终端定位和责任追究。