**关于全校开展网络与信息安全专项检查的工作要求**

各职能部门、各学院根据以下安全检查要求进行安全检查及检查结果反馈。请各单位积极配合检查工作，并对发现的问题及时整改。

### **一、对联网带屏设备的安全检查**

1. **资产台账梳理：**全面检查公共区域大屏系统的管理台账，包括设备清单、使用人员信息、维护记录等，确保其完整性和准确性。明确其数量、位置和管理责任人和使用责任人。信息资产（网站）资产名录、联网和内容投放终端台账信息有变更，需重新整理报图文信息中心存档；部门网信负责人、网信安全员、网站及系统的管理人员有变更，需重新签订安全承诺书。
2. **加强备案审核：**在建设、使用、承接联网带屏设备的，应在设备安装前，将设备名称、安装部位、生产运维负责人联系方式，联网方式(互联网、物联网、专网)，联网控制系统服务器、操控平台位置(含实体位置和虚拟空间位置)信息详细备案。
3. **管理责任人及使用责任人明确：**明确校内各单位、食堂及商铺所使用的LED电子显示屏、电视、会议室投影及大屏等设备的管理责任人及使用责任人，专人负责、专人值守、专人巡察，应急响应，避免无关人员非授权控制显示屏，确保管理权限的有效控制。
4. **强化日常管理：**联网带屏设备日常管理要做到“四个有”:有完整的摸排台帐、有固定的管理人员、有具体的管理制度、有可操作的应急处置预案。要将联网带屏设备“全域、全量、全时”纳入常态化监管。健全完善播出内容审核、常态化巡防、重要敏感节点管控等工作机制。
5. **关闭不使用的显示设备：**在重要网络安全保障期间对于非使用的显示屏、投屏设备等关闭有线，无线连接功能,确保处于断网状态。
6. **网络管控：**检查公共区域大屏的网络连接，确保其只连接到可信的网络，并防止未经授权的访问。对于可单机运行的显示屏,要求断网管理并关闭无线连接功能。
7. **加强服务端口安全防护：**对确需联网使用的显示设备加强服务端口安全防护，减少不必要的无线和远程管理功能，定时开关机，加强对维护计算机的安全防护。使用单位要切实落实防篡改、防入侵、防攻击等网络安全保护措施,加强内容更新权限管理和安全审核,切实消除安全隐患。
8. **播控系统及主机管控：**对播控系统及主机的安全性进行检查，包括是否有访问控制策略、是否存在已知的漏洞等。
9. **电子屏合规管控：**对公共区域大屏的电子屏进行管控，包括显示内容的审核、播放策略等，确保其符合相关规定。对公共区域大屏的显示内容进行检查，确保其符合相关规定，不含有不良信息。
10. **账户口令管控：**对公共区域大屏系统的账户口令进行管理，包括是否有强密码策略、是否存在弱密码情况等。
11. **应急预案及响应：**制定针对公共区域大屏可能出现的网络安全事件的应急预案，并定期进行演练，确保在出现安全事件时能够及时响应。应急预案根据部门工作环境及网络安全要求及时进行更新完善。
12. **立即响应安全事件：**对于发生显示屏控制系统被攻击或内容被篡改等事件的,要第一时间消除影响,收集证据,并立即向上报。
13. **安全培训：**定期对公共区域大屏的使用和维护人员进行网络安全培训，提高人员安全意识和技能。
14. **安全检查：**定期对公共区域大屏的网络安全进行检查，发现并修复可能存在的安全隐患。

### **对联网终端的安全检查**

1. **资产台账梳理：**全面检查联网终端的管理台账，包括设备清单、使用人员信息、维护记录等，确保其完整性和准确性。明确其数量、位置和管理责任人和使用责任人。信息资产（网站）资产名录、联网和内容投放终端台账信息有变更，需重新整理报图文信息中心存档；部门网信负责人、网信安全员、网站及系统的管理人员有变更，需重新签订安全承诺书。
2. **终端设备安全：**检查终端设备是否符合安全标准，是否存在硬件或软件故障，检查是否安装了防病毒软件、安全补丁是否及时更新、是否存在恶意软件等。
3. **网络安全：**检查网络传输是否加密，网络设备是否具备安全防护措施，如防火墙、入侵检测系统等。
4. **端口安全：**检查网络中是否有开放的端口，是否存在风险等。
5. **网络访问：**检查网络访问情况，包括是否存在异常的网络访问行为、是否访问了不安全的网站等。
6. **数据安全：**检查数据传输是否加密，数据存储是否安全，以及是否存在数据泄露的风险。
7. **应用程序安全：**检查应用程序是否符合安全标准，是否存在漏洞或恶意代码，以及是否进行了安全测试和认证。
8. **用户行为安全：**检查用户行为是否存在异常，如未经授权的访问、异常登录等，以及是否存在违规操作或恶意攻击。
9. **安全日志检查：**检查安全日志是否完整、准确，以及是否存在异常事件或攻击行为。

### **三、对网站及信息系统的安全检查**

1. **资产台账梳理：**梳理关键信息基础设施、门户网站、邮件系统、办公系统、重要业务系统、云平台、大数据平台、数据库系统等，更新信息系统（网站）资产名录。信息资产（网站）资产名录、联网和内容投放终端台账信息有变更，需重新整理报图文信息中心存档；部门网信负责人、网信安全员、网站及系统的管理人员有变更，需重新签订安全承诺书。
2. **调查摸底：**对所有系统进行排查，了解每个系统的使用情况，确定哪些系统长期未被使用。明确哪些系统属于“僵尸”系统，以及它们未被使用的时间和原因。如果“僵尸”系统无法再被使用，需要考虑注销或删除这些系统。在注销或删除前，需要确保所有相关数据已经备份并彻底清除，以防止数据泄露或遗留问题。
3. **等保测评：**加强信息系统(网站)等保工作落实情况，对于新增信息系统（网站），开展等保测评工作。对于未进行定级备案和定级测评的信息系统（网站）不得在互联网上线使用。对等保测评信息进行上报。
4. **检查口令设置：**对于每个账户，检查其口令是否符合要求，包括长度、复杂度、使用时间等。对于短口令、简单口令、常见单词或短语，以及与个人信息相关的口令，都应视为弱口令。杜绝使用admin、password、root、123456等或键盘相邻按键组成的弱密码。
5. **后台管理设置：**各单位须对所负责和使用的以上资产进行排查，尤其是系统后台管理员密码，要严防弱口令、默认口令、通用口令，一经发现必须立即更改。
6. **口令的更新:**口令长期未变更的及时变更。检查账户的口令历史记录，看是否有重复使用或简单的口令。如果发现有这种情况，应及时更改口令。
7. **防止暴力破解：**检查系统的安全设置，看是否设置了防止暴力破解的措施，如IP地址限制、登录失败次数限制等。如果没有设置，建议添加这些措施以保护系统免受攻击。