**附件**

2019年网络安全检查自查表

表二：信息系统运营使用单位填写（各市教育行政部门、各高校、厅直属事业单位（学校）填写）

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 一、信息系统运营使用单位基本情况 | | | | | | | | | | | | | |
| 单位名称 | | 厦门兴才职业技术学院 | | | | | | | | | | | |
| 单位地址 | | 厦门市集美区后溪镇兴溪路879-889号 | | | | | | | | | | | |
| 网络安全分管领导 | | 姓名 | 郝超 | | | 职务/职称 | | | | 校长 | | | |
| 网络安全责任部门 | | 教学辅助中心 | | | | | | | | | | | |
| 责任部门负责人 | | 姓 名 | 胡银涛 | | | 职务/职称 | | | | 网络信息中心主任 | | | |
| 办公电话 | 0592-3153340 | | | 移动电话 | | | | 18959276922 | | | |
| 责任部门联系人 | | 姓 名 | 陈承毅 | | | 职务/职称 | | | | 网络信息干事 | | | |
| 办公电话 | 0592-3153340 | | | 移动电话 | | | | 13063081965 | | | |
| 单位信息系统  总数 | | 2 | 第四级系统数 | | |  | | 第三级系统数 | | |  | | |
| 第二级系统数 | | | 1 | | 未定级系统数 | | | 1 | | |
| 单位信息系统  等级测评总数 | | 2 | 第四级系统数 | | |  | | 第三级系统数 | | |  | | |
| 第二级系统数 | | |  | | 未测评系统数 | | | 2 | | |
| 单位信息系统  安全建设整改总数 | | 2 | 第四级系统数 | | |  | | 第三级系统数 | | |  | | |
| 第二级系统数 | | | 1 | | 未整改系统数 | | | 1 | | |
| 单位信息系统  安全自查总数 | | 2 | 第四级系统数 | | |  | | 第三级系统数 | | |  | | |
| 第二级系统数 | | | 2 | | 未自查系统数 | | |  | | |
| 二、信息系统运营使用单位网络安全工作情况 | | | | | | | | | | | | | |
| 1、单位网络安全等级保护工作的组织领导情况 | | | | | | | | | | | | | |
| （重点包括：单位网络安全领导机构或网络安全等级保护工作领导机构成立情况；单位网络安全或网络安全等级保护工作的职责部门和具体职能情况；单位网络安全等级保护工作部署情况等。）  **“校园网络宣传及安全管理工作领导小组”，组成如下：**  （一） 组 长：陈毅勇  （二） 副组长：刘文体、张宝胜  （二）领导小组下设办公室  主 任：秦正友  副主任：何岳华、成员：胡银涛、高敏、唐伟键、陈承毅、付蒙蒙、吴飞燕、纪凤媚，各二级学院（部）行政秘书、教学秘书，校大学生通讯社及学生网络宣传队伍。  职责要求：  （一）办公室负责监督、检查校园网络宣传及安全管理的日常工作，尤其是做好“两会”、大型赛会、重要庆典、招生敏感期等特殊时期的校园网络宣传及安全管理工作。  （二）办公室负责对大学生通讯社及各二级学院推选的网络宣传学生队伍进行培训。  （三）党政办负责做好学校网站首页的更新、管理以及学校各网站的网页设计、后台管理；各部门做好各自网站的更新、管理，部门领导负责所发布内容的审核并签名，各行政秘书、教学秘书负责审核后材料的上传工作；教学辅助负责做好校园网的功能维护及安全管理工作。 | | | | | | | | | | | | | |
| 2、单位对网络安全等级保护工作的保障情况 | | | | | | | | | | | | | |
| （重点包括：单位网络安全等级保护工作年度考核情况；单位组织开展网络安全自查情况；单位网络安全工作经费是否纳入年度预算?单位网络安全工作的经费约占单位信息化建设经费的百分比情况等。）  **网络安全等级保护工作部署情况：**已参照第二级系统参数配备相应网络安全设备，同时对网站系统也参照二级系统参数进行改版。  **校园网络与信息安全责任书**  为明确校园网络与信息安全管理职责，进一步优化学校网络环境，确保我校无网络与信息安全事故发生，根据上级相关文件精神，特拟定厦门兴才职业技术学院校园网络与信息安全责任书，具体内容如下：  一、各二级学院院长、各处室处长、各中心主任为该二级单位所属网络安全和信息安全的第一责任人，负责建立和完善本二级单位网络安全和信息安全组织，指定二级信息安全管理员，具体负责本单位网络安全和信息安全工作。  二、坚持“谁主管，谁负责；谁主办，谁负责”原则，加强对本部门上网信息及内容的审查，确保上网信息和保密信息安全。实行实时网络监控制度，切实做到“看好自己的门，管好自己的人，做好自己的事”。严禁本部门所属人员（教工及学生）利用网络制作、传播、查阅和复制下列信息内容：  1、损害国家及学校荣誉、利益、形象；  2、散布谣言、扰乱社会秩序、破坏社会稳定等言论；  3、散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪等内容；  4、含有法律、法规禁止的其他内容。  三、对本部门人员利用网络建立的网站、微博、微信、QQ群、飞信群等与学校主体相关的公共交流平台实时监控；教学单位要摸清学生群体建立的内部交流群，学生管理人员应参与学生交流群并加强监控与引导，严禁交流群中出现不当言论，对可能引发严重后果的情况要及时上报。  四、严格实行网络安全和信息安全责任追究制度。如因管理不善致使本部门内发生重、特大信息安全事故或严重违纪违法事件的，按有关规定对部门和相关责任人进行处理，情节特别严重的依法追究相关责任人的法律责任。  五、在责任期内，责任书各条款不因负责人变化而变更或解除，接任负责人应相应履行职责。  本责任书一式三份，学校宣传与网络安全管理工作领导小组与责任书签订部门各执一份，校党政办公室存档一份。  本责任书自签字之日起生效。 | | | | | | | | | | | | | |
| 3、单位网络安全责任追究制度执行情况 | | | | | | | | | | | | | |
| （重点包括：是否建立了单位网络安全责任追究制度？是否依据责任追究制度对单位发生的网络安全事件（事故）进行追责等情况。）  **网络安全事故发生后有关行动**  1、领导小组得悉消防紧急情况后立即赶赴本级指挥所，各种网络安全事故处理小组迅速集结待命。  2、应急小组成员听从组织指挥，迅速组织本级抢险防护。  （1）确保WEB网站信息安全为首要任务,迅速发出紧急警报，所有相关成员集中进行事故分析，确定处理方案。  （2）确保校内其它接入设备的信息安全：经过分析，可以迅速关闭、切断其他接入设备的所有网络连接，防止滋生其他接入设备的安全事故。  （3）分析网络，确定事故源：使用各种网络管理工具，迅速确定事故源，按相关程序进行处理。  （4）事故源处理完成后，逐步恢复网络运行，监控事故源是否仍然存在。  （5）针对此次事故，进一步确定相关安全措施、总结经验，加强防范。  （6）从事故一发生到处理的整个过程，必须及时向领导小组组长以及教务处以及校长汇报，听从安排，注意做好保密工作。  3、积极做好广大师生的思想宣传教育工作，迅速恢复正常秩序，全力维护校园网安全稳定。  4、迅速了解和掌握事故情况，及时汇总上报。  5、事后迅速查清事件发生原因，查明责任人，并报领导小组根据责任情况进行处理。  从事其他危害计算机信息网络安全的活动。做好记录并立即向当地公安机关报告。  6、在信息发布的审核过程中，如发现有以下行为的，将一律不予以发布，并保留有关原始记录，在二十四小时内向当地公安机关报告。  （一）煽动抗拒、破坏宪法和法律、行政法规实施  （二）煽动颠覆国家政权，推翻社会主义制度  （三）煽动分裂国家、破坏国家统一  （四）煽动民族仇恨、民族歧视、破坏民族团结  （五）捏造或者歪曲事实、散布谣言，扰乱社会秩序  （六）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪  （七）公然侮辱他人或者捏造事实诽谤他人  （八）损害国家机关信誉  （九）其他违反宪法和法律、行政法规  7、接受并配合公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为. | | | | | | | | | | | | | |
| 4、单位信息系统定级备案工作情况 | | | | | | | | | | | | | |
| （重点包括：单位信息系统是否全部定级备案？单位系统调整是否及时进行备案变更？单位新建信息系统是否落实定级备案等工作。）  **已参照第二级系统参数配备相应网络安全设备，同时对网站系统也参照二级系统参数进行改版，目前已确定由中信网安开展等级保护测评工作，新建系统也已在着手准备相应定级备案工作。** | | | | | | | | | | | | | |
| 5、单位信息系统安全测评和安全建设整改工作情况 | | | | | | | | | | | | | |
| （重点包括：单位信息系统安全检测和整改经费落实情况；单位信息系统恶意代码扫描、渗透性测试、等级测评和风险评估的安全检测情况；信息系统安全建设整改方案制定和实施情况；单位网络安全保护状况的了解掌握等情况。）  **一、投入费用：**  目前“智慧校园系统”一期工程已完成，参照市场报价，投入费用约为180万元。  “智慧校园系统”二期和三期工程将会根据学校发展的实际需要继续建设。  **二、系统实施和维护**  1.配合业务部门进行系统培训（业务部门负责业务方面解释，软件公司提供系统操作方面解释）  2.协助业务部门进行原始数据处理工作，确保上线后的数据基本完整。  3.阶段性回访业务部门，收集使用情况和汇总的有效建议，评估后进行系统优化升级。  4.定期和锐捷、国微等软件硬件提供商进行协调，对学校信息系统的安全进行升级与维护。 | | | | | | | | | | | | | |
| 6、单位网络安全管理制度的制定和实施情况 | | | | | | | | | | | | | |
| （重点包括：单位信息系统建设和网络安全“同步规划、同步建设、同步运行”措施的落实情况；单位人员管理，信息系统机房管理、设备管理、介质管理、网络安全建设管理、运维管理、服务外包等管理制度的建设情况；管理制度的监督保障和运行情况等。）  **一、网络信息安全管理制度**  1. 组织工作人员认真学习《计算机信息网络国际互联网安全保护管理办法》，提高工作人员的维护网络安全的警惕性和自觉性。  2. 负责对本网络用户进行安全教育和培训，使用户自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，使他们具备基本的网络安全知识。  3. 加强对单位的信息发布和BBS公告系统的信息发布的审核管理工作，杜绝违犯《计算机信息网络国际互联网安全保护管理办法》的内容出现。  4. 一旦发现从事下列危害计算机信息网络安全的活动的：  （一）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；  （二）未经允许对计算机信息网络功能进行删除、修改或者增加；  （三）未经允许对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、 修改或者增加；  （四）故意制作、传播计算机病毒等破坏性程序的；  （五）从事其他危害计算机信息网络安全的活动。做好记录并立即向当地公安机关报告。  5. 在信息发布的审核过程中，如发现有以下行为的，将一律不予以发布，并保留有关原始记录，在二十四小时内向当地公安机关报告。  （一）煽动抗拒、破坏宪法和法律、行政法规实施  （二）煽动颠覆国家政权，推翻社会主义制度  （三）煽动分裂国家、破坏国家统一  （四）煽动民族仇恨、民族歧视、破坏民族团结  （五）捏造或者歪曲事实、散布谣言，扰乱社会秩序  （六）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪  （七）公然侮辱他人或者捏造事实诽谤他人  （八）损害国家机关信誉  （九）其他违反宪法和法律、行政法规  6. 接受并配合公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为.  **二、信息发布登记制度**  1. 在信源接入时要落实安全保护技术措施，保障本网络的运行安全和信息安全；  2. 对以虚拟主机方式接入的单位，系统要做好用户权限设定工作，不能开放 其信息目录以外的其他目录的操作权限。  3. 对委托发布信息的单位和个人进行登记并存档。  4. 对信息源单位提供的信息进行审核，不得有违犯《计算机信息网络国际联网安全保护管理办法》的内容出现。  5. 发现有违犯《计算机信息网络国际联网安全保护管理办法》情形的，应当保留有关原始记录，并在二十四小时内向当地公安机关报告。  **三、信息内容审核制度**  一、必须认真执行信息发布审核管理工作，杜绝违犯《计算机信息网络国际联网安全保护 管理办法》的情形出现。  二、对在本网站发布信息的信源单位提供的信息进行认真检查，不得有危害国家安全、泄露国家秘密，侵犯国家的、社会的、集体的利益和公民的合法权益的内容出现。  三、对在百度贴吧等公告板等发布公共言论的栏目建立完善的审核检查制度，并定时检查，防止违犯《计算机信息网络国际联网安全保护管理办法》的言论出现。  四、一旦在本信息港发现用户制作、复制、查阅和传播下列信息的，按照国家有关规定，删除本网络中含有上述内容的地址、目录或者关闭服务器。并保留原始记录，在二十四小时之内向当地公安机关报告。  1. 煽动抗拒、破坏宪法和法律、行政法规实施  2. 煽动颠覆国家政权，推翻社会主义制度  3. 煽动分裂国家、破坏国家统一  4. 煽动民族仇恨、民族歧视、破坏民族团结  5. 捏造或者歪曲事实、散布谣言，扰乱社会秩序  6. 宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪  7. 公然侮辱他人或者捏造事实诽谤他人  8. 损害国家机关信誉  9. 其他违反宪法和法律、行政法规  **四、安全教育培训制度：**  一、定期组织管理员认真学习《计算机信息网络国际互联网安全保护管理办法》、《网络安全管理制度》及《信息审核管理制度》，提高工作人员的维护网络安全的警惕性和自觉性。  二、负责对本网络用户进行安全教育和培训，使用户自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，使他们具备基本的网络安全知识。  三、对信息源接入单位进行安全教育和培训，使他们自觉遵守和维护《计算机信息网络国际 互联网安全保护管理办法》，杜绝发布违犯《计算机信息网络国际互联网安全保护管理办法》的信息内容。 | | | | | | | | | | | | | |
| 7、单位重要数据的保护情况 | | | | | | | | | | | | | |
| （重点包括：单位数据中心建设情况；数据加密保护情况；单位重要数据备份恢复情况等）  **中心机房是校园信息化系统工程建设的“心脏”，它与智慧校园建设息息相关。建设标准化数据中心机房是信息化基础建设的一个重要任务，也是关键工作。2018年4月我们开始建设前期准备，组织协调涉事办公室的搬迁和场地基础建设；2018年5月启动建设工程，目前已完成数据中心机房的建设和测试，并已正式开始应用。** | | | | | | | | | | | | | |
| 8、单位网络安全监测和预警情况 | | | | | | | | | | | | | |
| （重点包括：单位开展日常网络安全监测情况；单位网络安全监测技术手段建设情况；单位网络安全预警工作情况等。）  **已和锐捷网络有限公司开展合作，配备相应安全设备解决网络安全监测问题，同时也和高校招生网站安全服务平台、安全狗等相关平台开展网络安全监测和安全预警功能。** | | | | | | | | | | | | | |
| 9、单位网络安全应急预案和演练情况 | | | | | | | | | | | | | |
| （重点包括：是否制定了单位网络安全预案？单位网络安全预案是否进行了演练？是否根据演练情况对预案进行了修改完善等情况。）  网络信息安全应急预案  为确保学校在发生网络安全问题时各项应急工作高效、有序地进行，最大限度地减少损失，根据互联网网络安全相关条例及上级相关部门文件精神，结合我校校园网工作实际，特制定本预案。  一、成立安全应急小组  网络信息中心全体成员及学校各部门网络管理员组成网络安全应急小组成员，并在学校宣传与网络安全管理工作领导小组（以下称领导小组）指导下开展工作，网络安全应急小组主要职责：  （1）协调各二级学院院长、各处室处长、各中心主任为该二级单位所属网络安全和信息安全的第一责任人并签定校园网络与信息安全责任书。。  （2）充分利用各种渠道进行网络安全知识的宣传教育，组织、指导全校网络安全常识的普及教育，广泛开展网络安全和有关技能训练，不断提高广大师生的防范意识和基本技能。  （3）认真搞好各项物资保障，严格按照预案要求积极配备网络安全设施设备，落实网络线路、交换设备、网络安全设备等物资，强化管理，使之保持良好工作状态。  （4）采取一切必要手段，组织各方面力量全面进行网络安全事故处理工作，把不良影响与损失降到最低点。  （5）调动一切积极因素，全面保证和促进学校网络安全稳定地运行。  二、各级处理预案  1、网站不良信息事故处理预案  （1）一旦发现学校网站上出现不良信息（或者被黑客攻击修改了网页），立刻关闭网站。  （2）备份不良信息出现的目录、备份不良信息出现时间前后一个星期内的HTTP连接日志、备份防火墙中不良信息出现时间前后一个星期内的网络连接日志。  （3）打印不良信息页面留存。  （4）完全隔离出现不良信息的目录，使其不能再被访问。  （5）删除不良信息，并清查整个网站所有内容，确保没有任何不良信息，重新开通网站服务，并测试网站运行。  （6）修改该目录名，对该目录进行安全性检测，升级安全级别，升级程序，去除不安全隐患，关闭不安全栏目，重新开放该目录的网络连接，并进行测试，正常后，重新修改该目录的上级链接。  （7）全面查对HTTP日志，防火墙网络连接日志，确定该不良信息的源IP地址，如果来自校内，则立刻全面升级此次事件为最高紧急事件，立刻向领导小组组长汇报，视情节严重程度领导小组可决定是否向公安机关报案。  （8）从事故一发生到处理事件的整个过程，必须保持向领导小组组长汇报、解释此次事故的发生情况、发生原因、处理过程。  2、网络恶意攻击事故处理预案  （1）发现出现网络恶意攻击，立刻确定该攻击来自校内还是校外；受攻击的设备有哪些；影响范围有多大。并迅速推断出此次攻击的最坏结果，判断是否需要紧急切断校园网的服务器及公网的网络连接，以保护重要数据及信息；  （2）如果攻击来自校外，立刻从防火墙中查出对方IP地址并过滤，同时对防火墙设置对此类攻击的过滤，并视情况严重程度决定是否报警。  （3）如果攻击来自校内，立刻确定攻击源，查出该攻击出自哪台交换机，出自哪台电脑，出自哪位教师或学生。接着立刻赶到现场，关闭该计算机网络连接，并立刻对该计算机进行分析处理，确定攻击出于无意、有意还是被利用。暂时扣留该电脑。  （4）重新启动该电脑所连接的网络设备，直至完全恢复网络通信。  （5）对该电脑进行分析，清除所有病毒、恶意程序、木马程序以及垃圾文件，测试运行该电脑5小时以上，并同时进行监控，无问题后归还该电脑。  （6）从事故一发生到处理事件的整个过程，必须保持向领导小组组长汇报、解释此次事故的发生情况、发生原因、处理过程。  3、学校重大网络事件处理预案  （1）对学校重大事件（如校庆、评估、重大活动等对网络安全有特别要求的事件）进行评估、确定所需的网络设备及环境。  （2）关闭其它与该网络相连，有可能对该网络造成不利影响的一切网络设备及计算机设备，保障该网络的畅通。  （3）对重要网络设备提供备份，出现问题需尽快更换设备。  （4）对外网连接进行监控，清除非法连接，出现重大问题立刻向上级部门求救。  （5）事先应向领导小组汇报本次事件中所需用到的设备、环境，以及可能出现的事故及影响，在事件过程中出现任何问题应立刻向领导小组组长汇报。  三、日常管理  1、领导小组依法发布有关消息和警报，全面组织各项网络安全防御、处理工作。各有关组员随时准备执行应急任务。  2、网络管理员对校园内外所属网络硬件软件设备及接入网络的计算机设备定期进行全面检查，封堵、更新有安全隐患的设备及网络环境。  3、加强对校园网内计算机设备的管理，加强对学校网络的使用者（学生和教师）的网络安全教育。加强对重要网络设备的软件防护以及硬件防护，确保正常的运行软件硬件环境。  4、加强各类值班值勤，保持通讯畅通，及时掌握学校情况，全力维护正常教学、工作和生活秩序。  5、按预案落实各项物资准备。  四、网络安全事故发生后有关行动  1、领导小组得悉消防紧急情况后立即赶赴本级指挥所，各种网络安全事故处理小组迅速集结待命。  2、应急小组成员听从组织指挥，迅速组织本级抢险防护。  （1）确保WEB网站信息安全为首要任务,迅速发出紧急警报，所有相关成员集中进行事故分析，确定处理方案。  （2）确保校内其它接入设备的信息安全：经过分析，可以迅速关闭、切断其他接入设备的所有网络连接，防止滋生其他接入设备的安全事故。  （3）分析网络，确定事故源：使用各种网络管理工具，迅速确定事故源，按相关程序进行处理。  （4）事故源处理完成后，逐步恢复网络运行，监控事故源是否仍然存在。  （5）针对此次事故，进一步确定相关安全措施、总结经验，加强防范。  （6）从事故一发生到处理的整个过程，必须及时向领导小组组长以及教务处以及校长汇报，听从安排，注意做好保密工作。  3、积极做好广大师生的思想宣传教育工作，迅速恢复正常秩序，全力维护校园网安全稳定。  4、迅速了解和掌握事故情况，及时汇总上报。  5、事后迅速查清事件发生原因，查明责任人，并报领导小组根据责任情况进行处理。  五、其他  1、在应急行动中，学校各部门要密切配合，服从指挥，确保政令畅通和各项工作的落实。  2、各部门应根据本预案，结合本部门实际情况，认真制定本部门的应急预案，并切实落实各项组织措施。 | | | | | | | | | | | | | |
| 10、单位网络安全事件（事故）的处置情况 | | | | | | | | | | | | | |
| （重点包括：是否明确了单位网络安全事件（事故）发现、报告和处置流程？年内是否发生重大网络安全事件（事故）？是否与相关部门建立了网络安全应急处置机制等情况。）  一、成立安全应急小组  网络信息中心全体成员及学校各部门网络管理员组成网络安全应急小组成员，并在学校宣传与网络安全管理工作领导小组（以下称领导小组）指导下开展工作，网络安全应急小组主要职责：  （1）协调各二级学院院长、各处室处长、各中心主任为该二级单位所属网络安全和信息安全的第一责任人并签定校园网络与信息安全责任书。。  （2）充分利用各种渠道进行网络安全知识的宣传教育，组织、指导全校网络安全常识的普及教育，广泛开展网络安全和有关技能训练，不断提高广大师生的防范意识和基本技能。  （3）认真搞好各项物资保障，严格按照预案要求积极配备网络安全设施设备，落实网络线路、交换设备、网络安全设备等物资，强化管理，使之保持良好工作状态。  （4）采取一切必要手段，组织各方面力量全面进行网络安全事故处理工作，把不良影响与损失降到最低点。  （5）调动一切积极因素，全面保证和促进学校网络安全稳定地运行。  我们重点从设备安全、系统安全、制度安全、防御及备份恢复系统等四大方面建立网络安全长效机制，确立专人专岗负责网络安全日常巡逻，从而确保网络数据的可用性、完整性和保密性！在多次重大活动（如厦门金砖会晤、十九大、两会等）期间都能高质量的完成上级各部门的网络安全检查；在勒索病毒、境外反中黑客流行期间，第一时间启动网络安全应急预案，组织技术人员对全校办公电脑逐一进行安全修复，保障学校网络安全，保持网络安全 “零事故” 。 | | | | | | | | | | | | | |
| 11、单位信息技术产品、服务国产化情况 | | | | | | | | | | | | | |
| （重点包括：单位操作系统、服务器、数据库、交换机等核心信息技术产品的国产化比率情况；单位网络安全设备的国产化比率情况；单位信息技术产品国产化替换工作计划情况；单位新建信息系统是否采用国产化设备；单位信息安全服务情况等。）  1、官网站群系统建设：厦门兴才职业技术学院官网站群系统采用的是国微CMS，国微CMS是国内四大主流平台提供商之一，也是中国南方PHP领域最大的系统提供商，属于行业著名品牌；产品主要面向政府、部队、高校以及企业集团，为其提供中高端信息化应用；耕耘九年，国微软件累积注册人数23万、产品下载超90万余次。国内很多重要的互联网平台技术来自国微。国内唯一可以提供双站群模式的厂商；两种站群模式可以完美配合  ◆ 分站站群模式：后台可以快速复制或建立新站点，平均只需2分钟即可创建一个站点，并包括数据设置；每个分站可以设置独立域名、管理员、模板等。  ◆ 独立站群模式：将两个或多个完全独立的系统，通过一个站群插件连接起来，实现数据相互推送，主站统一管理分站；每个站点都是独立数据库，可放置在不同服务器；每个分站又可以根据需求创建子站群。  2、宽带网络校校通：除继续使用电信宽带网络进入校园并进行长期合作外，学校于2017年12月和中国移动签订协议，为学校的宽带网络提供更好人服务。学校在精技楼、教学楼三、图书馆布置多间多媒体教室，用于教学使用；为老师提供一套基本的软件工具和教学资源；各办公室基本配置计算机用于备课授课，并根据不同专业需要建立相应的实训室，目前已经和福建国科信息科技有限公司签订“智慧校园”校企战略合作协议，针对学校的信息化建设和网络安全开展全方位合作。 | | | | | | | | | | | | | |
| 12、单位网络安全宣传培训情况 | | | | | | | | | | | | | |
| （重点包括：单位组织开展网络安全宣传教育情况；单位组织开展网络安全岗位培训和网络安全员培训等情况。）  四、安全教育培训制度：  一、定期组织管理员认真学习《计算机信息网络国际互联网安全保护管理办法》、《网络安全管理制度》及《信息审核管理制度》，提高工作人员的维护网络安全的警惕性和自觉性。  二、负责对本网络用户进行安全教育和培训，使用户自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，使他们具备基本的网络安全知识。  三、对信息源接入单位进行安全教育和培训，使他们自觉遵守和维护《计算机信息网络国际 互联网安全保护管理办法》，杜绝发布违犯《计算机信息网络国际互联网安全保护管理办法》的信息内容。 | | | | | | | | | | | | | |
| 三、单位信息系统基本情况 | | | | | | | | | | | | | |
| 序号 | | 信息系统名称 | | | 是否定级 | 是否备案 | | 是否为关键信息基础设施 | | 备案编号 | | | 安全保护等级 |
| 1 | | 厦门兴才职业技术学院官网 | | | 是 | 否 | | 否 | |  | | | 二级 |
| 2 | | 智慧校园系统（研发测试中） | | | 否 | 否 | | 是 | |  | | | 二级 |
| 3 | |  | | |  |  | |  | |  | | |  |
| 4 | |  | | |  |  | |  | |  | | |  |
| ....... | |  | | |  |  | |  | |  | | |  |
|  | |  | | |  |  | |  | |  | | |  |
|  | |  | | |  |  | |  | |  | | |  |
|  | |  | | |  |  | |  | |  | | |  |
|  | |  | | |  |  | |  | |  | | |  |
|  | |  | | |  |  | |  | |  | | |  |
|  | |  | | |  |  | |  | |  | | |  |
|  | |  | | |  |  | |  | |  | | |  |
|  | |  | | |  |  | |  | |  | | |  |
|  | |  | | |  |  | |  | |  | | |  |
|  | |  | | |  |  | |  | |  | | |  |
|  | |  | | |  |  | |  | |  | | |  |
|  | |  | | |  |  | |  | |  | | |  |
|  | |  | | |  |  | |  | |  | | |  |
|  | |  | | |  |  | |  | |  | | |  |
|  | |  | | |  |  | |  | |  | | |  |

表三：网站安全情况自查表（各市教育行政部门、各高校、厅直属事业单位（学校）填写）

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 一、网站的基本情况 | | | | | | |
| 网站中文名 | | 厦门兴才职业技术学院官网 | IP地址 | | 210.34.129.100 218.85.139.13  222.76.204.157  222.76.204.158 | |
| 网址 | | Xmxc.com | | | | |
| 网站责任单位 | | 教学辅助中心 | 网站运行单位 | | 教学辅助中心 | |
| 网站责任单位负责  人及职务 | | 胡银涛（教学辅助中心主任） | 联系电话 | | 18959276922 | |
| 网站运行安全责任人及职务 | | 陈承毅（网络信息干事） | 联系电话 | | 13063081965 | |
| 网站责任单位  所在地 | | 厦门市集美区后溪镇兴溪路879-889号 | | | | |
| 工信部ICP备案号 | | 闽ICP备05019609号-1 | | | | |
| 国际联网备案号 | |  | | | | |
| 隶属关系 | | □中央 □省(自治区、直辖市) ■地(区、市、州、盟)  □县（区、市、旗） □其他\_\_\_\_\_ | | | | |
| 单位类型 | | □政府机关 □事业单位 □国企  □互联网 □其他 民办高校 | | | | |
| 行业类别 | | 教育 | | | | |
| 等级保护定级备案 | | ■二级 □三级 □四级 □未定级 | | | | |
| 等级测评 | | ■已开展 □未开展 | | | | |
| 网站安全责任书 | | ■已签订 □未签订 | | | | |
| 网站服务栏目 | | ■新闻发布 ■政策宣传 □事项办理 □论 坛 □即时通信  □电子邮件 □留言版 □政务公开 □其他\_\_\_\_\_ | | | | |
| 二、网站的联网信息 | | | | | | |
| 域名注册服务机构和联系方式 | 北京新网互联软件服务有限公司  地址：北京市海淀区后屯路28号1号楼KPHZ国际技术转移中心210室  电话：010-62915202 | | | | | |
| .cn域名的NS记录 |  | | | | | |
| .cn域名的A记录 |  | | | | | |
| 主站IP地址范围 | 210.34.129.100 218.85.139.13  222.76.204.157  222.76.204.158 | | | | | |
| 主要协议/端口 |  | | | 操作系统版本 | | linux |
| 接入运营商及联系方式 | 厦门中国电信: 厦门市软件园二期望海路53号楼 | | | | | |
| 物理接入位置 | 软件园二期厦门电信 | | | | | |
| 接入带宽 |  | | | | | |
| CDN IP地址范围 | 218.85.139.13 | | | | | |
| CDN 服务提供商 | 厦门中国电信 | | | | | |
| CDN 联系人姓名 | 陈陪帆 | | | 陈陪帆 | | 陈陪帆 |
| 域名服务联系人  姓名 | 客服中心 | | | 客服中心 | | 客服中心 |

表四：重要数据和公民个人信息集中的企业网络安全自查表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 单位名称 | 厦门兴才职业技术学院 | | | |
| 单位地址 | 厦门市集美区后溪镇兴溪路879-889号 | | | |
| 网络安全责任部门 | 教学辅助中心 | | | |
| 责任部门联系人 | 姓 名 | 陈承毅 | 职务/职称 | 网络信息干事 |
| 办公电话 | 0592-3153340 | 移动电话 | 13063081965 |
| 数据保护责任部门 | 教学辅助中心 | | | |
| 责任部门联系人 | 姓 名 | 蔡海定 | 职务/职称 | 网络信息干事 |
| 办公电话 | 0592-3153322 | 移动电话 | 13950077865 |
| 单位数据总量（TB/PB） | 4T | | | |
| 数据存储位置 | □互联网 ■业务专网 □互联网和业务专网 □其他 | | | |
| 数据内容描述 | 学校教务系统和人事系统主要存储：   1. 学生基础信息主要包括：学号、姓名、身份证号、联系电话、家庭地址、课程成绩、实习单位信息等。   教师基础信息主要包括：工号、姓名、身份证号、联系电话、家庭地址、学历信息等。 | | | |

**企业存储（含缓存）的重要数据和公民个人信息统计表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 单位名称 | 信息系统名称 | 包含的数据类型 | 数据量  （TB/PB） | 数据存储位置 | 数据库IP地址 | 数据库维护单位、联系人及联系方式 |
| 企业总部 | 教务系统 | 无 | 学号、姓名、身份证号、联系电话、家庭地址、课程成绩、实习单位信息等 | 1.7G | 校内服务器 | 222.76.204.154 |
| 人事系统 | 无 | 工号、姓名、身份证号、联系电话、家庭地址、学历信息等 | 0.1G | 校内服务器 | 222.76.204.154 |
| 分公司1 |  |  |  |  |  |  |
|  |  |  |  |  |  |
| 分公司2 |  |  |  |  |  |  |
|  |  |  |  |  |  |

注：包含的数据类型：业务数据/公民个人信息；数据存储位置：互联网/互联网和业务专用网/托管单位。