附件

网络安全检查工作方案

**一、时间安排**

**（一）自查整改阶段（即日起至4月7日）。**各单位梳理本单位及下属单位所属网站和信息系统，填写关键信息基础设施、重要信息系统和网站情况表和自查表（附后），认真查摆问题，并针对梳理出的所属重要信息系统、工控系统、重点网站进行技术检测，全面查找发现各类潜在安全漏洞和突出问题。

**（二）现场检查阶段（4月8日－4月22日）。**我办会同相关主管部门对各单位开展现场抽查。对落实网络安全工作责任制存在问题、系统存在安全隐患的运营使用单位，将责令限期整改。

**二、检查内容**

按照“谁主管、谁负责，谁运行、谁负责”原则，此次检查重点检查各单位落实网络安全工作责任制，落实安全技术措施同步规划、同步建设、同步使用等情况，检查将委托技术支撑单位通过技术手段查找关键信息基础设施、重要信息系统（含工业控制系统）以及党政机关和企事业单位网站的风险隐患，检验网络攻击应对能力，对发现的突出问题、隐患限期整改。

**三、工作要求**

**（一）高度重视，加强领导。**各单位要从维护国家安全和社会稳定的大局出发，严格落实党委（党组）网络安全工作责任，充分认识此次网络安全检查工作的重要性和紧迫性，自觉抓好关键信息基础设施、重要信息系统和重点网站的安全防范工作。

**（二）强化督导，严格落实。**各单位要加强对检查工作的督导，及时总结检查经验，推动检查工作深入开展。对安全工作不落实、措施不到位，或在检查工作中弄虚作假对抗检查的，我办将会同相关部门严肃追究责任。

**（三）认真总结，狠抓整改。**各单位要将各阶段的检查工作情况认真梳理总结，及时掌握网络安全工作薄弱环节，并系统性予以督促整改，力争从源头上遏制和消除网络安全风险。

附表：

1. 关键信息基础设施、重要信息系统和网站情况表

2. 关键信息基础设施、重要信息系统和网站安全自查表

表1

## 关键信息基础设施、重要信息系统和网站情况表

**填表单位（盖章）：**

|  |  |  |
| --- | --- | --- |
| **关键信息基础设施、重要信息系统和网站名称（全称）： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_** | | |
| **主**  **管**  **单**  **位**  **信**  **息** | **单位全称** | 厦门兴才职业技术学院 |
| **单位地址** | 地（区、市、州、盟）县（县、市、旗）  厦门市集美区后溪镇兴溪路879-889号  邮政编码：361024 |
| **单位类型** | □党政机关 □事业单位  □社会团体 □国有及国有控股企业  ■其它：民办非企业 |
| **法人代表/单位主要负责人** | 姓 名：林亚姜 职 务：董事长  固定电话：18959268688 |
| **网络安全分管领导** | 姓 名： 郝超 职 务：校长  固定电话：13801507608 |
| **上一级**  **主管单位** | ■无  □有 主管单位全称： |
| **联**  **系**  **方**  **式** | **网络安全管理部门及负责人** | 是否已明确网络安全管理部门：■是 口否  网络安全管理部门名称：教学辅助中心  负责人：胡银涛 职 务：副主任  手 机： 18959276922 固定电话：0592-3153340 |
| **安全**  **管理员** | 姓名： 陈承毅 职 务：干事  手机： 13063081965 固定电话：0592-3153340 |
| **基**  **本**  **信**  **息** | **系统类别** | 日均访问量：0.1万次  □党政机关网站 □新闻信息网站  □事业单位网站 □社会团体网站  □国有企业网站 ■其他：民办非企业 |
| **功能描述** | 为上级部门、社会各界、全校师生传递学校信息和新闻动态。 |
| **联网信息** | 域名：xmxc.com  IP地址：222.76.204.157  公安机关互联网安全备案：■是 □否 备案号：35021102000003  信息安全等级保护备案：□是 ■否 备案号：s  ICP备案：■是 □否 备案号：闽ICP备05019609号-1 |
| **系统特征** | 是否24小时运行：■是 □否  是否面向社会公众提供服务：■是 □否 |
| **信息技术**  **产品** | 服务器数量:台存储设备数量:1台  路由器数量:台交换机数量:1台  服务器操作系统数量:1套 数据库管理系统数量:1套 |
| **数**  **据**  **存**  **储** | **存储位置** | ■全部境内存储 □有数据境外存储，主要存储地：校内机房 |
| **数据集中** | □全国数据集中 □省级数据集中 ■无数据集中 |
| **与境外信息系统数据交换** | □存在 ■不存在 |
| **数据加密** | ■数据存储与传输均加密 □数据存储与传输均未加密  □仅数据存储加密 □仅数据传输加密 |
| **运**  **行**  **环**  **境** | **托管情况** | ■未托管  □托 管  主要托管地：  托管单位（全称）：  托管方式：□主机托管 □虚拟主机/云计算 □其它 |
| **运**  **行**  **维**  **护** | **运维模式** | ■自行运维  □外包运维  主要运维厂商全称：境内厂商  境外厂商  运维方式：□现场运维 □远程运维  运维联系人：手 机： |
| **网**  **络**  **安**  **全**  **状**  **况** | **灾备情况** | (可多选）□数据灾备 RP0**1**:  □系统灾备 RTO**2**:  □无灾备措施 |
| **漏洞管理** | 定期对系统漏洞进行检查分析：■是 □否 |
| **网络安全**  **监测** | □无□自主监测  □ ■委托第三方监测，监测机构全称：锐捷网络科技有限公司 |
| **云防护**  **措施** | □采用云防护服务，服务商全称：  □未采用云防护服务 |
| **应急措施** | 网络安全应急预案：■已制定 □未制定  网络安全应急演练：□本年度已开展 ■本年度未开展 |
| **网络安全**  **事件** | 2019年发生的网络安全事件次数：0次  其中由于软硬件故障导致的事件次数： 0次  20 2019年检测发现的高危漏洞数：0个 |

填表说明：

●若单位含有下属机构且下属机构有互联网信息系统的，由主管单位统一收集上报。

●若单位有多个系统，请根据实际情况自行扩展，每个系统对应一张表。

**1**RPO (Recovery Point Objective)是指灾难发生后，容灾系统能把数据恢复到灾难发生前时间点的数据，是衡量灾难发生后会丢失多少生产数据的指标。可简单的描述为设施能容忍的最大数据丢失量。

**2**RTO (Recovery Time Objective)则是指灾难发生后，从关键信息基础设施宕机导致业务停顿之刻开始，到业务恢复运营所需要的时间间隔。可简单的描述为设施能容忍的恢复时间。

表2

关键信息基础设施、重要信息系统和网站安全自查表

**填表单位（盖章）：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **一、单位关键信息基础设施、重要信息系统和网站安全保护工作的相关情况** | | | | |
| **序号** | **检查项** | **结果记录** | **检查记录** | |
| **1、网络安全工作协调（领导）机制建立运行情况** | | | | |
| 1-1 | 是否通过正式文件或会议纪要明确本单位党委（党组）领导班子成员中网络安全直接责任人（主管网络安全的负责同志） | ■是□否 | |  |
| 1-2 | 是否明确了负责本单位网络安全工作的处级机构 | ■是□否 | |  |
| 1-3 | 是否通过制度文件明确了该机构负责此项工作的职责，明确了负责处室 | ■是□否 | |  |
| **2、网络安全人员配备和责任制落实情况** | | | | |
| 2-1 | 网络安全工作机构是否按照岗位实际配备了网络安全工作人员 | ■是□否 | | 兼岗性质 |
| 2-2 | 是否书面规定了网络安全工作人员的安全责任和惩戒措施 | □是■否 | |  |
| **3、网络安全规划制定落实情况** | | | | |
| 3-1 | 是否制定了本单位网络安全规划、实施计划或工作方案等文件 | ■是□否 | |  |
| 3-2 | 是否提出了本单位的网络安全主要目标、基本要求、工作任务和保护措施 | ■是□否 | |  |
| 3-3 | 是否制定相关工作规范，确保本单位的信息系统建设与安全建设同步规划、同步建设、同步使用 | ■是□否 | |  |
| **4、对网络安全工作的重视情况、网络安全经费保障情况以及关键信息基础设施、重要信息系统和网站安全防护工作的组织部署情况** | | | | |
| 4-1 | 单位主要负责同志是否对网络安全工作有重要批示和指示 | ■是□否 | |  |
| 4-2 | 是否定期组织召开本单位信息安全会议，研究关键信息基础设施、重要信息系统和网站安全防护等重点工作，制定工作计划，落实关键信息基础设施、重要信息系统和网站安全防护各项任务要求，并建立相关的考核制度 | ■是□否 | |  |
| 4-3 | 是否能够保障网络安全所需的费用 | ■是□否 | |  |
| **5、有关网络安全管理制度的建立和执行情况** | | | | |
| 5-1 | 是否制订了包括人员录用、安全培训、技术考核、安全保密、人员离岗等方面在内的网络安全人员管理制度 | □是■否 | | 由于网络安全人员采用兼岗性质，部份安全管理制度仍不够完善。 |
| 5-2 | 是否针对信息系统建设过程中的产品采购、服务外包、系统投入使用前进行安全测试等方面建立了相应的管理制度 | ■是□否 | |  |
| 5-3 | 是否与服务外包中标企业签订了安全保密责任书 | ■是□否 | |  |
| **6、信息系统定级备案工作开展情况** | | | | |
| 6-1 | 本单位所有信息系统是否都确定了安全保护等级 | □是■否 | | 系统总数2个，三级系统数量个，  二级系统数量个。 |
| 6-2 | 信息系统定级结果是否经过专家评审和上级主管部门审批 | □是■否 | | 目前联系等保公司做方案。 |
| 6-3 | 安全保护等级为第二级（含）以上的信息系统，是否已经到所在地设区的市级以上公安机关办理了备案手续 | □是 ■否 | | 目前联系等保公司做方案。 |
| 6-4 | 信息系统所承载的业务、服务范围、安全需求等是否发生变化，信息系统安全保护等级是否变更 | □是■否 | |  |
| 6-5 | 新建信息系统是否在规划、设计阶段确定安全保护等级并备案 | □是■否 | | 新建信息系统数量个 |
| **7、****第三级（含）以上信息系统等级测评和安全建设整改工作开展情况** | | | | |
| 7-1 | 单位第三级（含）以上重要信息系统是否开展了等级测评 | □是■否 | | 无第三级（含）以上重要信息系统 |
| 7-2 | 是否根据等级测评结果，制定了信息系统安全建设整改方案，开展了安全建设整改工作 | □是■否 | | 无第三级（含）以上重要信息系统 |
| 7-3 | 所选择的测评机构是否具有相应资质 | □是□否 | | 等级测评机构名称 |
| **8、正版软件应用情况** | | | | |
| **8-1** | **单位重要信息系统服务器是否使用正版操作系统** | **□是□否** | | **已安装正版操作系统\_\_\_\_个**  **占所有服务器比例\_\_\_\_\_\_** |
| **8-2** | **单位计算机设备是否使用正版操作系统** | **□是□否** | | **已安装正版操作系统\_\_\_\_个**  **占所有计算机设备比例\_\_\_\_\_\_** |
| **8-3** | **单位是否使用正版软件** | **□是□否** | | **已安装使用正版化软件有：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **9、网络安全自查工作情况** | | | | |
| 9-1 | 是否对本单位网络安全检查工作制定了计划、明确了要求并部署实施 | ■是□否 | |  |
| 9-2 | 是否定期对信息系统安全状况、安全保护制度及措施的落实情况进行了自查 | ■是 □否 | |  |
| 9-3 | 是否对自查中发现的安全威胁和隐患进行了整改 | ■是□否 | |  |
| 9-4 | 是否对相关主管部门检查或通报的问题进行整改 | ■是□否 | |  |
| **10、关键信息基础设施、重要信息系统和网站安全监测预警、容灾备份等工作情况** | | | | |
| 10-1 | 是否对单位关键信息基础设施、重要信息系统和网站安全运行状况进行监测，对报警情况进行及时处置 | ■是□否 | |  |
| 10-2 | 是否建立了重要系统和数据的容灾备份安全管理制度和技术措施，并定期进行备份 | ■是□否 | |  |
| **11、安全事件应急处置工作情况** | | | | |
| 11-1 | 是否制定了安全事件应急预案 | ■是□否 | |  |
| 11-2 | 是否定期对应急预案进行演练 | ■是□否 | | 演练周期一年一次  演练记录 |
| 11-3 | 应急预案的执行是否有足够的资源保障 | ■是□否 | |  |
| **12、通报应急处置及协调机制** | | | | |
| 12-1 | 各单位是否制定通报应急联系机制以协调应急突发事件 | ■是□否 | |  |

记录人：陈承毅 记录时间：2019年4月5日