防灾科技学院信息化管理中心

信息中心〔2021〕02 号

关于印发《防灾科技学院第三方和外包人员信息安全管理规定》的通知

学校各部门、各单位：

为加强学校对第三方和外包人员行为和规范的管理，特制定《防灾科技学院第三方和外包人员信息安全管理规定》，现予印发，请遵照执行。

防灾科技学院信息化管理中心

2021 年 10 月 7 日

防灾科技学院第三方和外包人员信息安全管理规定

第一章　总则

第一条　为规范防灾科技学院（以下简称“学院”）第三方和外包人员行为和规范，特制定本管理办法。

第二条　第三方和外包人员安全管理包括：外部人员分类及管理责任、基本安全、账户管理、计算机设备接入管理、远程访问管理、IT 外部人员规定以及违规处罚。

第二章　准则

第三条　外部人员须签订外部人员信息安全承诺书，以承诺对所接触到的关于学院的相关信息及数据具有保密责任。

第四条　外部人员分类及管理责任

（一）外部人员分类：外部人员分为如下四类：

①贵宾外部人员：指由上级领导或学院领导直接陪同或委派专人陪同，在学院信息中心安全区域内进行活动的外部人员；

②临时外部人员：指由于业务关系、行政关系或其他特殊原因，在学院信息中心安全区域内进行活动，且活动时间不超过一天的外部人员；

③短期外部人员：指由于业务关系、行政关系或其他特殊原因，在学院信息中心安全区域内进行活动，且活动时间在三天以上、三个月以内的外部人员；

④长期外部人员：指由于业务关系、行政关系或其他特殊原因，在学院安全区域内进行活动，且活动时间在三个月以上的外部人员。

（二）外部人员的信息安全管理实行“谁接待，谁负责；谁引入，谁负责”的原则。对口部门或对口人员负责监督、管理外部人员在学院工作或访问期间的一切行为，并对其所对口的外部人员的行为、影响和后果负有全部责任。

（三）信息中心指派专门人员对进入安全区域的外部人员进行身份确认与登记。

（四）对于在安全区域内活动的长期外部人员，如需对其进行考勤，则由对口部门向信息中心提出申请，由信息中心统一进行考勤工作。

第三章　基本安全

第五条　所有外部人员必须遵守学院发布的与信息中心风险管理和信息安全相关的方针策略、实施规范、管理办法等。

第六条　贵宾外部人员由对口部门或对口人员确定其能访问的物理安全区域；临时外部人员仅允许访问一级物理安全区域（办公区）；短期外部和长期外部人员经过审批后，可以允许其访问二级及以上安全区域（运维间、机房）；所有外部人员进入三级及以上安全区域（机房、配电室）须学院信息中心员工全程陪同。

第七条　外部人员在学院工作期间，必须遵守学院的相关规章制度，未经许可，外部人员不允许访问学院信息处理设施；外

部人员因工作需要使用学院相关文档资料，需根据文档的敏感性级别由相关责任部门进行审批并登记备案，所借文档资料未经许可不得复印。

第八条 短期外部人员和长期外部人员，以及工作中涉及到学院专有和保密信息的其它外部人员，需与学院签署保密协议后才能开始工作。信息中心和人事科负责外部人员保密协议的签署与保管。

第九条 学院保留随时对外部人员的信息安全状况进行检查的权利，外部人员必须给予配合和协助。

第四章 账户管理

第十条 贵宾外部人员由对口部门或对口人员确定是否为其开通OA账号和登录内网；临时外部人员不允许开通OA账号和登录内网；短期和长期外部人员如需开通OA账号和登录内网，需要单独申请，并报信息中心负责人审批。

第十一条 外部人员为完成其工作，需要对学院信息系统进行临时访问（访问时间不超过一天），由信息中心员工在学院管理的设备上，输入满足其工作需要的最小权限用户的用户登录信息，来获得临时性登录权限，并全程负责检查监督其对该账户的使用情况。

第十二条 外部人员为完成其工作，需要对学院信息系统进行短期访问（访问时间超过一天，不超过三个月），由信息中心员工为其申请相应环境和相应时间的短期账户，并全程负责检查监

督其对该账户的使用情况。

第十三条 外部人员为完成其工作，需要对学院信息系统进行长期访问（访问时间超过三个月），由信息中心员工为其申请相应环境和相应时间的长期账户，并定期检查监督其对该账户的使用情况。

第十四条 外部人员在使用完账户后，需通知信息中心。信息中心相应岗位人员须立即断开该外部人员的全部系统连接，并确认删除该外部人员所属的全部账户。

第五章 计算机设备接入管理

第十五条 临时外部人员的计算机设备不允许接入学院网络，不允许通过本网络设备登录互联网；贵宾外部人员、短期外部人员和长期外部人员的计算机设备如需接入学院网络，或通过学院网络设备登录互联网，须由信息中心负责人审批。

第十六条 在没有得到授权的情况下，外部人员的计算机设备不得接入学院任何安全域的网络端口。外部人员的计算机设备如果需要接入学院网络，须向信息中心提出申请，经批准后使用专门的网段进行接入。

第十七条 外部人员的计算机设备接入前，必须安装学院规定的安全控制软件、系统安全补丁和防病毒软件，及时升级病毒库，并进行病毒扫描。

第六章 远程访问管理

第十八条 外部人员为完成其工作，需要通过远程方式访问

到学院网络系统或设备，必须事先制定工作计划与工作方案，报对口部门和信息中心负责人审批通过后,才能允许进行远程访问。

第十九条 外部人员进行远程访问时，必须严格按照审批通过后的工作计划与工作方案进行工作，对口部门或对口人员负责检查监督其工作。

第七章 IT 外部人员特别规定

第二十条 IT 外部人员是指从事 IT 相关工作的学院外部人员，进入学院工作的 IT 外部人员除了要遵守以上所有规定外，还应当符合下列规定：

（一）当 IT 外部人员进入生产系统进行系统安装、测试时，必须信息中心相关人员全程陪同并进行监督。其使用过的账号，必须在安装、测试工作完成后进行删除或进行口令变更；

（二）当 IT 外部人员所涉及的系统含有敏感数据时，需要由信息中心相关人员进行脱敏，并采取必要的控制措施；

（三）开发、测试和检查过程中产生或获取的数据与资料，未经授权不得带出现场；

（四）进入机房及其他生产测试环境的 IT 外部人员，应遵守学院有关机房管理及办公场所的有关规定，禁止吸烟，符合用电及消防要求。

第二十一条 未经授权，IT 外部人员不得使用学院的信息资产，不得对学院的网络进行漏洞扫描和渗透测试，不得把移动介质带入机房及其他生产测试环境；

第二十二条 IT 外部人员不得利用工作之便，私自搜集、复制、传播、泄露学院敏感信息。

第八章 违规处罚

第二十三条 外部人员如违反学院信息安全有关规定，须对其进行处罚，相关处罚方法遵照学院人力资源部的有关规定执行。

第二十四条 对于违规情节特别严重的外部人员，外部人员对口部门应中止与外部人员所属单位的合作关系，并要求对方根据情况赔偿学院损失。

第二十五条 对于违反国家法律法规的外部人员，学院将会同违规人员所属单位将违规人员移交司法机关，并根据违规人员学院造成的具体损失情况，由其所属单位负责赔偿。

第九章 附则

第二十六条 本规定由信息化管理中心负责解释。

第二十七条 本规定自颁布之日起施行。

附表 1

项目运行与维护工作保密协议书

在防灾科技学院信息系统安全运行与维护工作过程中，因工作需要，为保护项目资料和商业秘密，在平等、自愿、协商一致的基础上，参与各方达成如下协议：

甲方：_____

乙方：_____

本协议于_____年_____月_____日（“生效日”）由_____（甲方公司名）和_____签订。

本协议各方有必要向对方提供某些专有信息（“保密信息”）。披露此类保密信息的一方应为“甲方”，接受此类保密信息的一方应为“乙方”，但任何一方都可以是“公司”。作为本协议各方接收对方保密信息的对价，各方同意，通过下面各自的签名，根据本协议规定使用保密信息，除非双方书面签署文件同意以其他方式使用保密信息。特此，双方协商如下：

1、乙方不得将甲方的保密信息透露给任何第三方，而应尽力避免由于疏忽将保密信息披露给任何第三方。

2、乙方不应使用甲方的保密信息也不应在自己的组织内流通，除非是为与甲方人员或授权代表商谈、讨论和协商之需或在本协议签署后经甲方书面授权的任何目的。

3、乙方不应为除本协议规定的目的以外的自身利益或任何其他方的利益而使用任何甲方的保密信息。

4、乙方对以下方面的信息没有保密义务：（a）在甲方向乙方告知信息时，该信息已处于公众领域中；（b）在甲方向乙方告知信息后，该信息非因乙方过错而进入公众领域；（c）在甲方向乙方告知信息时，该信息

系乙方拥有且无任何保密义务的信息；（d）该信息被法院或政府命令要求披露，且已将规定或命令通知甲方从而使其可申请保护令或其他合适的救济。

5、本保密协议，保密信息的披露和双方之间其后的商讨并不产生除本协议规定以外的义务。本协议或向乙方披露的保密信息均不得视为向乙方授予任何知识产权或与之有关的任何性质的权利。

6、所有保密信息都是基于“可能是”而提供。任何一方都不通过明示、暗示或其他方式对其准确性、完整性或性能作出保证。

7、所有由甲方提供给乙方的材料，包括但不限于文件、设计和清单应仍为甲方的财产，且甲方要求时应立即归还原件和所有据此制作的副本。

8、所有由甲方提供给乙方的材料和所有乙方在服务期间由于操作需要（如扫描报告、渗透测试报告、运维服务等）对甲方信息系统产生的数据材料，包括但不限于文件、设计和清单应仍为甲方的财产，且甲方要求时应立即归还原件和所有据此制作的副本。

9、本协议自生效日起三（3）年内一直保有完全的效力。本协议有效期内任何时间双方可通过相互同意或向另一方发出书面通知六十（60）天后终止协议；但提前终止本协议不应豁免乙方在本协议下就终止生效日前提供给乙方保密信息所应履行的义务。

10、 乙方人员服务结束之后仍对其在甲方服务期间接触、知悉的甲方或者虽属于乙方但甲方承诺有保密义务的商业秘密，承担如同服务期间一样的保密义务和不擅自使用有关秘密信息的义务，而无论乙方人员因何种原因离职。

11、 本协议应根据中华人民共和国宪法进行解释。

本协议包括其条款和条件，是双方对协议完整并具有排他性的陈

述，其将取代双方就题述事项先前或同步达成的所有书面或口头的提议、谅解录和其它所有通讯。本协议及其任何修改、附件、变更或补充经公司签署并经 _____（甲方公司名）主管或最高责任人接受和签署方才生效。

经签署，签字人保证其系经正式授权代表签署本协议。

--正文完，以下为签字栏--

双方签字盖章

甲方： **（盖章）** 负责人： 联系电话： 日　　期：	**乙方：** **保密人（单位）签字（盖章）** 保密人： 联系电话： 日　　期：

附表 2

第 三 方 服 务 评 审 表

合同名称：	
服务单位：	
服务期限：	×××年××月××日－××××年××月××日
评审意见：	
备注：	
审核人：	审核时间：

附表 3

第三方入网申请表

申请人		所在部门
申　请 原　因		
部　门 意　见		
信息中心 意　见		

注意：1、非涉密计算机申请接入内部办公网应严格按照《防灾科技学院网络和系统安全管理办法》及《防灾科技学院存储介质管理规定》等要求执行。接入内部办公网之后，如出现泄密事件，由申请人负个人责任。

2、此表一式两份，申请人一份，信息中心留一份备案。

附表 4

第三方调查表

部门/人员		（注解：第三方接口管理部门或人员）		
第三方单位名称				
调查项目		调查内容	调查结果	备注
1	公司（例）	公司相关资质、营业执照等		
2	人员（例）	项目主要人员背景调查情况		
3	..			
4				
5				
6				
7				
8				
9				
10				

附表 5

第三方信息安全管理检查列表

第三方名称		第三方联系人		联系邮件	
				联系电话	
接待部门		部门联系人		联系邮件	
				联系电话	
驻场时间		提供服务内容			
编号	检查内容			检查结果	备注
进入防灾科技学院前					
1	是否有对第三方驻场人员进行工作背景等信息进行调查？				
2	是否与第三方人员签署保密合同或保密协议？				
驻场过程中					
1	是否有清单记录目前常驻的第三方人员的基本信息？				
2	是否有记录记载第三方人员进入防灾科技学院行后使用的设备清单？				
3	是否有清单记录第三方人员在防灾科技学院拥有的各信息系统的逻辑访问权限？				
4	是否对第三方人员进行安全培训，并对培训效果进行考核？				
5	是否对第三方的服务质量和交付物进行管理、监督和评审，并对发现的问题及时进行整改？				
6	是否对第三方进行周期性的安全检查，并对检查中发现的问题及时进行整改？				
离场时					
1	第三方人员是否有归还所有的防灾科技学院各类资产？				
2	是否及时清除第三方人员的各类物理和逻辑访问权限？				