华南理工大学信息化办公室

信息化〔2020〕01号

关于印发《华南理工大学网络安全监测与处置办法》的通知

校内各单位:

为增强学校网络安全风险防范能力， 进一步规范校内网络安全通报工作，根据《教育系统网络安全事件应急预案》和《华南理工大学网络安全事件应急预案》要求，制定《华南理工大学网络安全监测与处置办法》，经2019年第16次校长办公会议讨论通过，自2020年1月8日起实施，请遵照执行。

信息化办公室

2020年1月8日

华南理工大学网络安全监测与处置办法

第一条 为增强学校网络安全风险防范能力，进一步规范校内网络安全通报工作，根据《教育系统网络安全事件应急预案》和《华南理工大学网络安全事件应急预案》要求，制定本办法。

第二条 本办法适用于对学校计算机网络及信息安全威胁的监测发现和处置流程。网络安全威胁是指校园网或互联网上存在或传播的、可能或已经对校内单位和用户造成危害的网络资源、恶意程序、安全隐患或安全事件，包括：

1. 被用于实施网络攻击的恶意 IP 地址、恶意域名、恶意 URL、恶意电子信息，包括木马和僵尸网络控制端，钓鱼网站，钓鱼电子邮件等；

2. 被用于实施网络攻击的恶意程序，包括木马、病毒、僵尸程序、移动恶意程序等；

3. 网络服务和产品中存在的安全隐患，包括硬件漏洞、代码漏洞、业务逻辑漏洞、弱口令、后门等；

4. 网络服务和产品已被非法入侵、非法控制的网络安全事件，包括主机受控、数据泄露、网页篡改等；

5. 其他威胁网络安全或存在安全隐患的情形。

第三条 依据“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，学校网络安全和信息化领导小组办公室（下文简称“网信领导小组办公室”）主管全校网络安全监测与处置工作，日常工作由信息网络工程研究中心（下文简称“网络中心”）负责，校内各单位明确网络安全责任人、联络员、信息系统管理员。

第四条 网信领导小组办公室承担以下职责：

1. 监督、检查校内网络安全检测与处置工作。

2. 制定并修订学校网络安全监测与处置办法；

3. 接收上级主管部门、权威机构的预警和通报，建立校内监测预警系统，及时核实情况，发起校内处置流程；

4. 汇总学校网络安全情况、动态，发生的网络安全事件等信息，对学校网络安全事件进行通报，按要求向上级主管部门报送。

第五条 网络中心承担以下职责：

1. 建立校园网络安全联络体系和建立信息系统校内登记体系，登记单位责任人和联络员、系统责任人和管理员；

2. 登记和梳理学校信息系统资产信息；

3. 指导学校相关部门制定网络安全问题整改方案，完成网络安全事件的处置，验证整改结果；

4. 采取措施防范安全威胁进一步发展；

5. 在重大活动和重要专项工作期间，实施网络安全防范和监测预警，建立 24 小时应急联络渠道，执行每日零事件报告制度。

第六条 校内各单位承担以下职责：

1. 信息系统放置在校内，可以购买符合国家安全要求的校外应用平台服务，向网络中心完成信息系统校内登记备案，系统发生变更应在 5 个工作日内更新登记信息；

2. 单位责任人和联络员、系统责任人和管理员发生变更，应在 5 个工作日内向网络中心更新登记信息；

3. 为每个信息系统指定信息系统管理员，应定期开展日常巡检工作；

4. 在重大活动和重要专项工作期间，重要系统应安排专人 24 小时值班加强网络安全防范，执行每日零事件报告制度。

第七条 安全威胁预警处置过程

1. 处置对象：校内监测发现的或者上级主管部门和权威机构发布的，可能危害校内网络、主机、应用系统的安全威胁；

2. 预警范围：根据可能的影响范围，面向全校发布预警或向特定用户群定向发布预警；

3. 责任单位应积极开展自查，排除预警的安全威胁情况。

第八条 安全威胁通报处置过程

1. 处置对象：校内监测发现的或者上级主管部门和权威机构通报的，有确定危害对象的安全威胁；

2. 通报范围：对责任单位进行定向通报；

3. 责任单位在收到通报后，应及时落实整改措施，三个工作日内网络中心提交《华南理工大学安全威胁通报整改报告》；

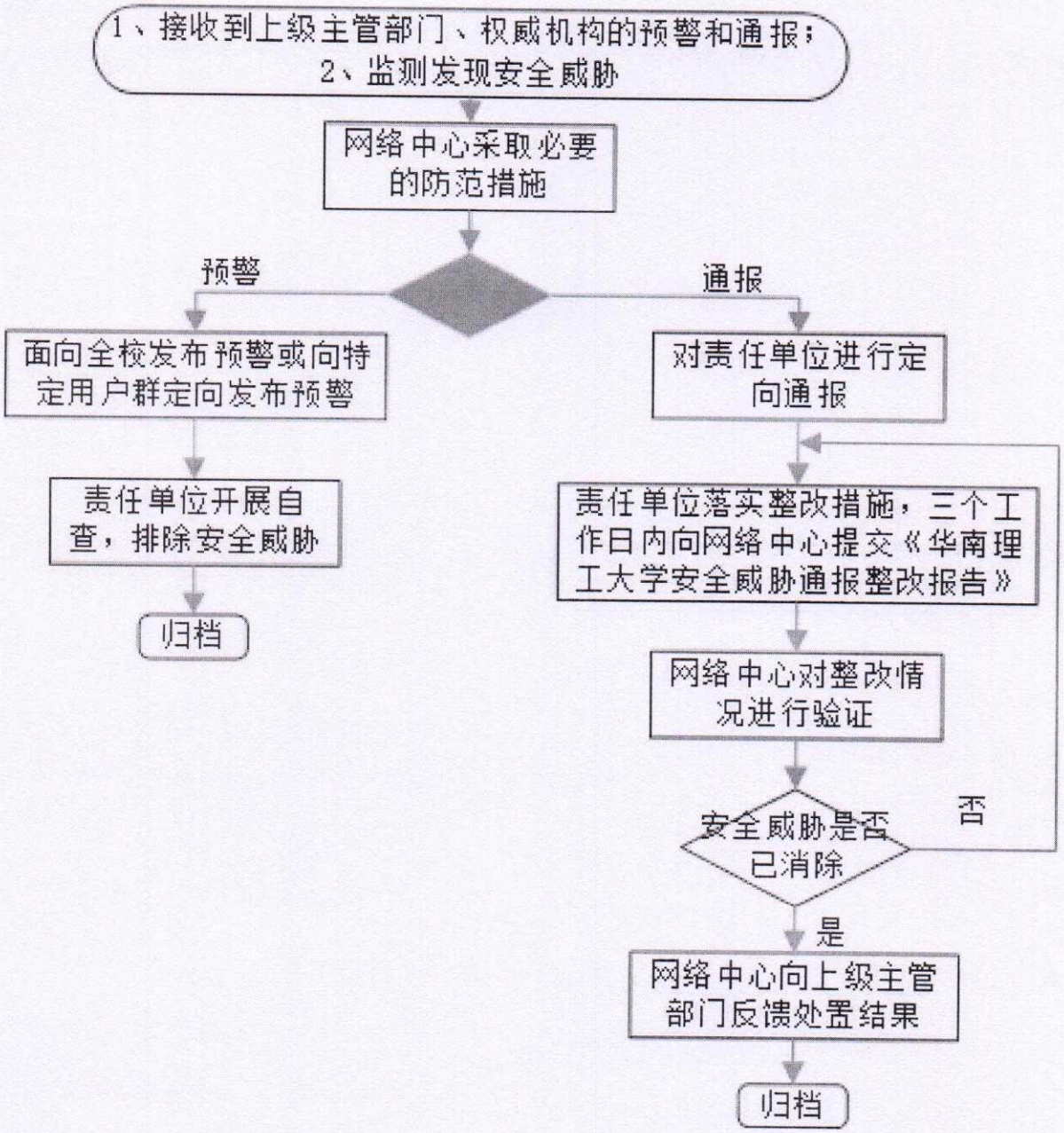
4. 网络中心对整改情况进行验证；

5. 针对反复整改都没有消除安全威胁、拖延或拒不整改的情况，网络中心应采取限制网络访问、收回服务资源等惩罚措施。

第九条 本办法由学校负责解释，具体工作由网络安全和信息化领导小组办公室承担。

第十条 本办法自 2020 年 1 月起施行。

附件 1: 网络安全威胁处置流程



附件 2

华南理工大学安全威胁通报整改报告

单位名称：（需加盖公章）　　报告时间：　　年　　月　　日

联系人姓名		手机		电子邮件	
通报描述	通报时间：　　年　　月　　日 安全威胁描述：				
系统、主机基本情况（如涉及请填写）	1. 系统名称：_____ 2. web 网址：_____ 3. IP 地址：_____ 4. 系统用途：_____				
安全威胁的判定原因（可加页附文字、图片以及其他文件）					
已采取整改措施					
希望得到的援助					
系统责任人意见（签字）					
单位安全责任人意见（签字）					