广西工业技师学院恶意代码防范管理制度

第一章 总　则

第一条　为了加强广西工业技师学院（以下简称“枢纽台”）对恶意代码的预防和治理，确保枢纽台远程监控系统网络和数据信息免遭恶意代码的入侵和破坏，保障枢纽台远程监控系统的安全、可靠运行，特制定本制度。

第二条　本管理规范适用于广西工业技师学院远程监控系统（包括未联网计算机）恶意代码的防治管理工作。

第三条　本规定所称的恶意代码，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制和传播的一组计算机指令或者程序代码。恶意代码疫情，是指某种恶意代码爆发、流行的时间、范围、破坏特点、破坏后果等情况的报告或者预报。信息介质，是指计算机软盘、硬盘、磁带、光盘等。

第二章 恶意代码管理措施

第四条　枢纽台各部门在从信息网络上下载软件、程序、数据和购置、维修、借入计算机设备时，必须先对其进行恶意代码检测，经确认无毒后方可使用。

第五条　信息网络中心应当对易受恶意代码攻击的信息系统，定期进行恶意代码检查；枢纽台各部门使用外来媒体交换的信息要按相关规定进行管理，并进行恶意代码检测，确认无毒后方可使用，防止恶意代码对系统和数据的破坏。

第六条　信息网络中心应采取加强访问控制机制，关闭不必要的共享服务与应用端口等措施，堵住漏洞，切断恶意代码的感染与传播途径，防范恶意代码入侵。

第七条　枢纽台各部门必须配备安装经枢纽台许可的企业版网络防病毒软

件，以便操作人员能够经常检测，及时发现和清除恶意代码，避免或尽可能减轻恶意代码造成的危害或损失。

第八条 信息网络中心恶意代码防治人员必须定期升级计算机防病毒服务端软件，及时更新有关病毒库，并督促使用人员定期升级本机上的计算机防病毒客户端软件，以确保计算机防病毒软件的功效。

第九条 枢纽台各部门应及时组织做好分行辖内所有计算机（包括终端和办公用机）相关安全补丁的安装工作。

第十条 所有终端和开发用机的操作系统、数据库、应用系统等软件的安装由信息网络中心专人负责，并做好计算机防病毒软件及相关安全补丁的安装工作。

第三章 计算机设备和网络恶意代码管理

第十一条 系统管理员应切实加强计算机与网络设备使用管理，严格管理信息系统终端的规范使用，避免恶意代码交叉感染。

第十二条 枢纽台各部门在业务终端上使用业务信息介质以及其他相关单位提供的信息介质前，必须先进行严格的恶意代码检测，确认无毒后方可使用。

第十三条 严禁在业务终端上运行、查看、拷贝与本业务无关、来历不明、未经确认无毒的软件。严禁在各种工作用计算机上玩游戏。

第十四条 信息网络中心对联入互联网、局域网的计算机和服务器，应当采取严格的计算机防病毒措施，认真审批传输内容，限定访问使用权限，以防止恶意代码与黑客的侵袭。

第十五条 安全管理员至少每周一次检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关上截获危险病毒或恶意代码进行及时分析，并形成书面的报表和总结报告，向枢纽台信息网络中心汇报。

第四章 恶意代码疫情监控上报与处理

第十六条 计算机使用人员严禁擅自任意修改查杀策略，删除防病毒软件。在

每日病毒库升级过程中，严禁擅自中止系统升级；系统定时扫描时，严禁用户擅自中止系统扫描。

第十七条 计算机使用人员每日必须及时查看恶意代码查杀情况。发现计算机感染了病毒，要立即停止使用疫情计算机，切断网络，隔离一切涉嫌感染病毒的信息介质和设备，同时报告信息网络中心。信息网络中心接到疫情报告后，应立即对疫情进行调查，查明病毒来源并及时清除病毒，避免病毒进一步传播。

第十八条 计算机信息系统发生恶意代码疫情，造成计算机信息系统瘫痪、程序和数据严重破坏等重大事故时，应立即上报信息网络中心并保护好现场。信息网络中心应立即派专人进行调查，查清病毒来源，分析病毒疫情，查杀恶意代码，并填写《恶意代码疫情报告表》。能力范围外无法及时查杀病毒的，应立即采取措施隔断染毒计算机，控制疫情，并联系计算机防病毒软件供应商请求协助。

第五章 恶意代码工作的落实与检查

第十九条 信息网络中心应定期对枢纽台各部门的计算机信息系统防病毒工作进行检查，发现影响计算机信息系统安全的隐患时，应及时通知该机构进行整改。

第二十条 违反本规定，并造成计算机系统重大安全事故的，枢纽台将按情况追究部门负责人和相关责任人的责任。

第六章 附 则

第二十一条 本管理规范由枢纽台信息网络中心负责解释。

第二十二条 本管理规范自发布之日起施行。