

# 广东工贸职业技术学院

## 关于印发《广东工贸职业技术学院网络与信息 安全漏洞处理流程》的通知

各部门、各二级学院：

经校长办公会批准通过《广东工贸职业技术学院网络与信息安全漏洞处理流程》（制度编号：GDGM-WI-IT-03-08），现印发给你们，请认真贯彻执行。

广东工贸职业技术学院  
2025年3月25日

密级	主动公开	制度编号	GDGM-WI-IT-03-08			
管理模块	信息系统管理	制度级别	三级			
<div>广东工贸职业技术学院</div> <div>网络与信息安全漏洞处理流程</div>						
修 订 记 录						
日期	版本	修订内容概要	拟订	审核	通过形式	批准
2025 年 2 月	V1.0	新增	苏安伦	卢志海 詹东霖	经 2025 年第 2 次 校长办公 会审定	何汉武

# 广东工贸职业技术学院

## 网络与信息安全漏洞处理流程

### 1.目的和依据

目的：为保障网络与信息系统安全，确保网络与信息安全漏洞不会被利用，对学校网络与信息系统造成危害。

依据：《中华人民共和国网络安全法》《广东工贸职业技术学院网络与信息安全管理制制度》

### 2.范围

2.1 本流程文件适用于网络与信息安全漏洞处理业务。

2.2 流程的输入：《网络与信息安全漏洞通报》

2.3 流程的输出：《网络安全漏洞处置结果反馈表》

### 3.定义

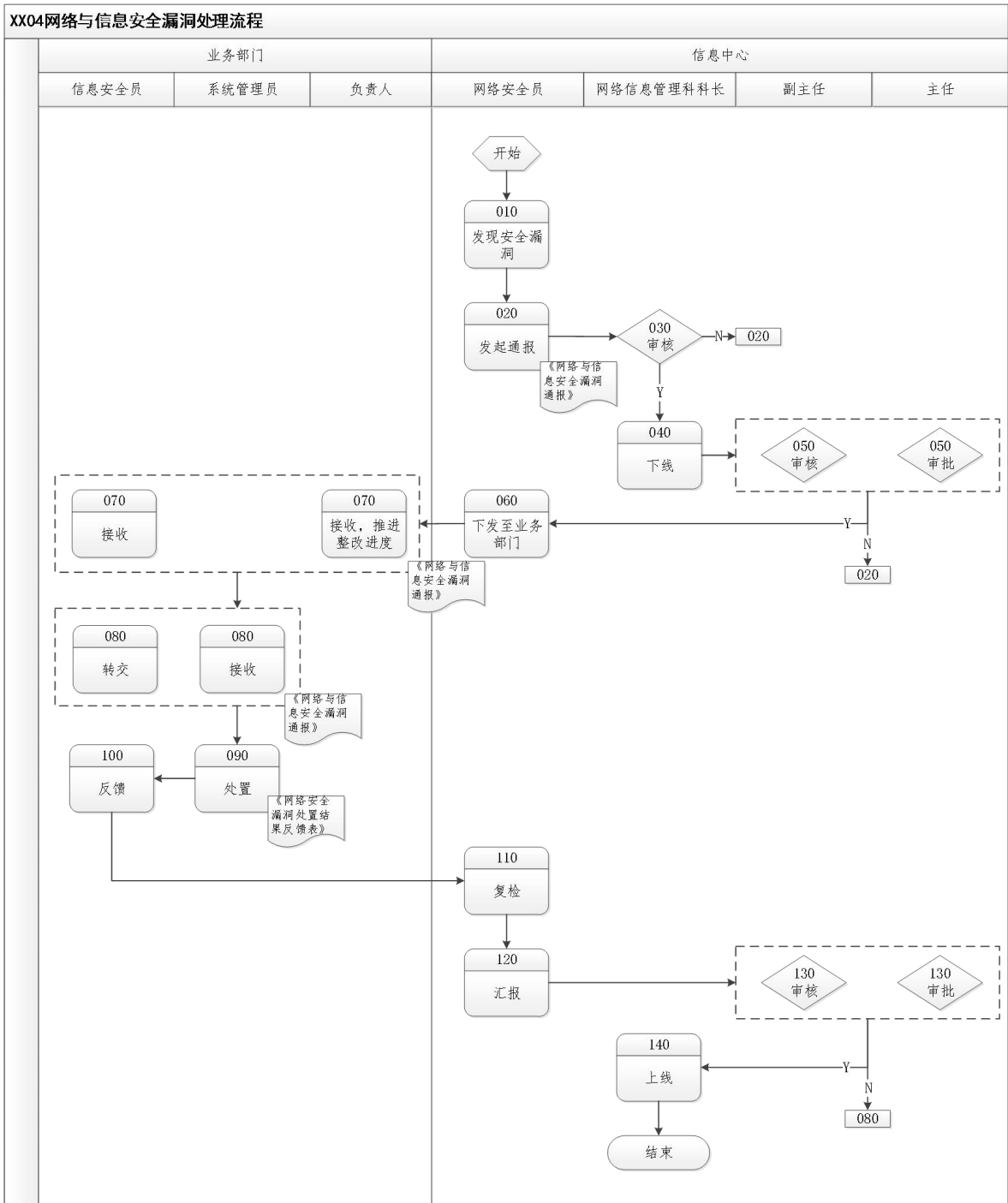
本文所指的网络与信息安全漏洞，是指网络与信息系统因策略配置不当或者操作系统、提供服务的中间件、应用程序本身存在的，可以使攻击者能够在未授权的情况下访问或破坏系统的缺陷。

### 4.部门/岗位与责任

序号	部门/岗位	责任
1	信息中心/网络安全员	发现安全漏洞，发起《网络与信息安全漏洞通报》，复核安全漏洞处理结果
2	信息中心/网络信息管理科科长	审核《网络与信息安全漏洞通报》，确认通报内容是否有误，对存在漏洞的信息系统做下线操作，令复检通过的系统重新上线

序号	部门/岗位	责任
3	信息中心/主任、副主任	同时审批《网络与信息安全漏洞通报》，确认是否同意发给相关部门，确认系统是否给予重新上线
4	业务部门/部门负责人	接收《网络与信息安全漏洞通报》推进安全漏洞处理进度
5	业务部门/信息安全员	接收《网络与信息安全漏洞通报》，通知系统管理员处置安全漏洞，转发《网络安全漏洞处置结果反馈表》发给网络安全员
6	业务部门/系统管理员	处置安全漏洞，填写《网络安全漏洞处置结果反馈表》

## 5.流程图



## 6.流程图说明

编号	活动名称	部门/岗位	活动描述
01	发现安全漏洞	信息中心/网络安全员	发现安全漏洞

编号	活动名称	部门/岗位	活动描述
02	发起	信息中心/网络安全员	发起《网络与信息安全隐患通报》
03	审核	信息中心/网络信息管理科科长	审核《网络与信息安全隐患通报》内容
04	下线	信息中心/网络信息管理科科长	将存在高危、中危安全隐患的业务系统下线
05	审批	信息中心/主任、副主任	同时审批《网络与信息安全隐患通报》内容，确认是否发给业务部门
06	下发	信息中心/网络安全员	根据信息中心主任、副主任审批，下发《网络与信息安全隐患通报》给业务部门
07	接收	业务部门/部门负责人、信息安全员	同时接收《网络与信息安全隐患通报》，部门负责人推进漏洞整改进度
08	转交	业务部门/信息安全员、系统管理员	信息安全员将《网络与信息安全隐患通报》转交系统管理员处理
09	处置	业务部门/系统管理员	处置安全隐患，填写《网络安全漏洞处置结果反馈表》转交信息安全员
10	反馈	业务部门/信息安全员	提交《网络安全漏洞处置结果反馈表》给网络安全员
11	复检	信息中心/网络安全员	根据《网络安全漏洞处置结果反馈表》进行安全隐患复检
12	汇报	信息中心/网络安全员	向信息中心主任、副主任汇报漏洞修复情况
13	审批	信息中心/主任、副主任	同时审批业务系统是否可以重新上线
14	上线	信息中心/网络信息管理科科长	根据信息中心主任、副主任审批恢复业务系统上线

## 7.其他说明

本流程管理者为信息中心负责人，由其负责本文件的拟订与

优化、使用培训与解释，以及牵头落地执行。党委会批准生效，自发布之日起施行。此前文件与本制度不符的，按本制度执行。本流程由党委会授权信息中心负责解释。

## **8.相关文件**

《网络与信息安全管理办法》

## **9.附件**

附件：《网络安全漏洞处置结果反馈表》空表

附件：

## 网络安全漏洞处置结果反馈表

部门名称*		通报日期*	
系统名称*		系统 ip*	
管理员*		管理员电话*	
运维服务商*		系统上线时间*	
处置记录/ 问题原因* 备注：（高、中危漏洞需逐条写明漏洞处置方式、步骤、结果以及截图等；如特殊操作，需在此备注，譬如限制端口访问等）	例： 服务器 ip:1.1.1.1 漏洞名称 1: SQL 注入漏洞（高危） 处置方式：过程和步骤 处置结果：最终处置完成结果及截图  <div style="text-align: right;">（盖章） 日期：</div>		
信息中心审核	<div style="text-align: right;">（盖章） 日期：</div>		
恶意文件样本	不涉及/附件随后送至信息中心	入侵日志	不涉及/附件随后送至信息中心

说明：1.如涉及木马、病毒等恶意文件，将恶意文件样本和入侵日志交至信息中心。