广西工业技师学院信息安全总体策略

第一章 总　则

第一条　为确保广西工业技师学院（以下简称“枢纽台”）信息系统正常稳定运行，确保枢纽台内网、SDH 网和远程监控系统网络信息安全和广播电视安全播出得到保障，落实网络安全责任，提高网络安全防护能力，维护国家安全、社会稳定和用户合法权益，根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》、以及国家网络安全等级保护等有关规定，特制订本信息安全总体策略。

第二条　专业术语定义

（一）　人为的失误：计算机技术人员及业务人员在信息系统的设计、开发、安装、使用过程中，都有机会产生人为的错误或失误。

（二）　欺诈行为：来自于内部职工或外部人员，欺骗性地修改或产生信息系统的数据，进行犯罪。

（三）　内部人员破坏行为：由于对工作不满或其他原因，有意在程序中设置“后门”或程序炸弹，并对设备、数据、系统进行故意破坏的行为。

（四）　物理资源服务丧失：设备故障或物理环境发生意外灾难（电源断电、通讯中断、水灾、火灾、地震等）而产生系统宕机事件。

（五）　黑客攻击：黑客通过非法手段访问或破坏信息系统。

（六）　信息泄密：部分职工利用权限之便而造成信息系统数据的外泄。

（七）　病毒（恶意程序）侵袭：指编制或者在计算机程序中插入破坏计算机功能或者毁坏系统数据的计算机指令或者程序代码。

（八）　程序系统自身的缺陷：程序设计开发时，对系统的安全性考虑不足，

留下安全隐患，这是一种来自系统自身的威胁。

第三条 枢纽台信息系统网络安全工作遵循“以安全保发展，以发展促安全”的指导思想，坚持“谁主管谁负责、谁运行谁负责”的原则。

第四条 枢纽台在学院领导下负责指导监督管理直属各单位网络安全工作，配合网信、公安部门开展有关工作。

枢纽台信息网络中心是学院负责网络安全管理工作的职能部门，负责组织实施本单位网络安全各项工作，配合广播电视行政部门开展网络安全监督管理相关工作，包括建立健全体制机制、编制完善制度预案、落实网络安全责任制，提供人财物保障，定期汇报，解决重大问题等。

第五条 本信息安全总体策略适用于业务系统信息化建设、使用和维护整个生命周期相关的各项安全管理活动。

第二章 总体目标

第六条 保护枢纽台信息系统的硬件、软件、业务信息和数据、通信网络设备等资源的安全，有效防范各类安全事故，合法合规发展各类信息系统，确保为社会提供高效稳定的服务。

第三章 组织管理体系

第七条 枢纽台管理体系建立的目标是建立自上而下的信息安全工作管理体系，确立安全管理组织机构的职责，统筹规划、专家决策，以推动信息安全工作的开展。

第八条 安全领导小组定期组织会议，对近期网络安全形势进行通报分析，对重要工作进行部署。

第九条 重要保障期前，要组织技术力量，对所辖重要信息系统开展技术检测和风险评估，对发现问题要进行及时整改。

第十条 应建立网络安全信息报告制度，及时将发现的网络安全事件、风险、威胁等上报技术中心，对可能影响到行业内其他单位的安全信息，要及时提供给本级监测监管机构。

第十一条 可建立包含行业内外网络安全领域相关专家组成的专家组，必要时对网络安全趋势研判、事件处置、方案制定、专项规划、标准研究等进行技术支撑。

第四章 人员安全管理

第十二条 人员安全管理的目标是通过设立安全管理制度及岗位责任制，为保证最大程度地降低信息化建设过程中由于人为失误或错误所造成的风险。

第十三条 人员是信息系统安全的决定性因素。与信息安全相关的岗位职责分配的基本原则为：

（一） 职责分离原则：在人员岗位建立时，相关的信息系统访问的安全责任应该确定，不相容的职责应分离。接触信息系统的人员应承担与其工作性质相应的安全责任，各类人员不得从事超越自己职责以外的任何工作。

（二） 有限授权原则：任何人员对信息资源的访问权利应受到限制，应对超越职责的访问进行控制。

（三） 相互制约原则：安全环节的管理应采取相互制约原则，做到职责分明，各司其职，相互配合和制约。

（四） 任期审计原则：应记录并监控职工在任职期内的信息资源访问活动。

第十四条 信息系统关键岗位职工（是指计算机系统运行过程中直接从事生产系统或周围设施管理的人员）必须是枢纽台正式职工，上岗前要对其进行培训，并使其充分了解信息系统安全的至关重要性。对各类计算机系统的相关人员应实施有针对性、有计划的计算机信息安全教育和培训。职工通过培训应明确与本职工作有关的计算机信息安全知识和责任。

第十五条 定期考核职工的工作表现，调整与其岗位不符的安全职责权限或调离违反岗位安全规则的职工。

第十六条 职工离职前，应交还手中持有的与信息系统相关的文档、物品，应交接其负责的工作。一经离职，办公室要立即通知信息网络中心，

相应的信息系统合法身份账户及权限应立即注销，视调离保密岗位人员的重要程度，及时调整系统的安全保密措施。

第十七条 所有职工必须签订安全保密承诺书。相关安全教育由办公室统一组织，由信息网络中心统一确定培训教育的教材、课程。

第五章 标准化和规范化管理

第十八条 标准化和规范化安全的目标是通过建立内部业务处理、操作流程、信息系统管理和技术等一系列标准化和规范化的过程，奠定信息系统安全的基础。

第十九条 枢纽台信息网络中心应该根据各业务对资产保护的需要，确定应用系统的安全等级，建立枢纽台各项业务的标准、规范化处理流程和业务数据标准，以及确定各级职工对信息资源访问的权限标准。

第二十条 信息网络中心应该规范信息系统的工程建设，依照国家或本行业的安全管理政策和标准，逐步建立信息系统安全的各项管理规范和相关技术标准，规范基础设施建设、系统和网络平台建立、应用系统开发、运行管理等重要环节，创建信息系统安全的基础。

第六章 设备与物理环境安全

第二十一条 设备与物理环境安全的目标是保护计算机设备、设施（含网络）以及信息系统的物理环境免遭自然灾害和其他形式的破坏，保证信息系统的实体安全。

第二十二条 安全计划和安全管理必须实施于信息系统基础设施建设的需求计划、部署实现、安装启用、终止结束等完整工程生命周期的各个阶段。

第二十三条 信息系统有关物理环境的选址及建设应遵照国家计算机场地安全标准和有关主管部门的场地环境设施标准，配备防火、防雷、防水、防静电、防鼠等机房安全设施，有效防止数据泄密，维持系统不间断的运行能力，确保信息系统运行的安全可靠。

第二十四条 应对突发事故，实体安全建立应急计划，配备应急电源，实施系

统主机及重要设备的备份、冗余技术保护措施；对数据应做到异地备份或做到异地存放；应对灾难事故，实体安全建立灾难中心，实现物理实体的恢复机制。根据实际情况定期实施主备机的切换和应急方案的演练。

第二十五条 限制和规定枢纽台机房、重要信息设备所在地的人员进出活动。

第二十六条 对重要安全设备产品的选择，必须符合国家有关技术规范或经过专业测评机构检测不低于本行业计算机信息安全管理技术规范中的最低安全要求，并核实是否具备安全部门的设备准用证或国家有关部门的安全产品许可证书。

第二十七条 严格确定信息设备的合法使用人。建立详细的设备使用运行日志及故障维修记录，实施定期的设备维护、保养操作。

第七章 应用系统安全

第二十八条 应用系统安全的目标是保证各业务应用系统开发过程以及最终产品的安全性，安全建设必须与应用系统建设同步进行。

第二十九条 质量管理和安全监控必须实施于应用系统从计划到运行全周期的各阶段（即需求计划阶段、系统设计阶段、技术实现阶段、安装测试以及投产运行阶段）。

第三十条 应用系统的总体需求计划阶段，应全面评估系统的安全风险，分析系统的潜在威胁，根据信息资源的保护等级策略，确立系统的访问控制、身份认证、信息加密、审计跟踪、稽核检查等安全需求，并征求保卫科意见，确立应用系统的安全策略。

第三十一条 在应用系统的总体架构设计的过程中，应实施安全需求设计，并确立安全服务机制、项目开发人员安全技术要求和操作规程。

第三十二条 应用系统的实现阶段，应根据安全需求设计实施安全技术，对应用系统技术实现过程进行质量管理，防止技术开发人员故意保留“后门”，保证系统最终产品的安全性质量。

第三十三条 在应用系统建设的各阶段，必须保证应用软件的完整性，即确保软件的变更是经过授权及合法性的验证；必须形成各阶段相应的系

统功能设计及技术实施的规范性文档，以及重要的系统安全策略，安全规划、应急计划、风险分析、安全服务机制等安全性文档，并随着系统实现的进程应保持文档变更的同步及准确。

第三十四条 应用系统投产运行之前，必须充分进行局部功能、整体功能、压力测试，以及与安全需求目标一致的系统安全性能、操作流程、应急方案等重要安全性测试，测试的结果应记录文档。

第三十五条 只有正式经过管理、操作、技术控制等安全鉴定获准的应用项目，可以投入生产运行。

第三十六条 外包开发的应用系统须获得第三方权威机构的安全检测或认证，确保其不存在后门或恶意代码。

第八章 通信网络安全

第三十七条 网络安全的目标是有效防范网络体系的安全风险，为应用系统发展提供安全、可靠、稳定的网络管理和技术平台。

第三十八条 通信网络安全建设是业务发展的基础，通信网络安全管理和网络安全技术的配合是获得网络整体安全的基本保障。

第三十九条 通信网络架构的安全可靠性设计、网络建设的安全投入应依照国家或本行业制定的各项安全管理规定和安全产品技术标准，充分考虑应用系统的发展规划和安全保护等级。

第四十条 对于依赖网络架构安全性的业务和应用系统，必须视其安全级别，实施相应的访问控制、身份认证、抗抵赖、加密、审计等信息安全服务机制，以提高业务和应用系统的安全防护能力。

第四十一条 在内部网络与外部网络的接入口、内部区域网的接入口、重要业务系统的外联接入口，必须视信息资源的保护等级，实施相应安全级别的隔离防火墙、认证、审计、动态检测等安全技术措施，防范信息资源被非法访问、篡改和破坏。任何职工不得在未经安全管理认可的情况下，擅自从内部网络的计算机直接访问外部网络。

第九章 运行安全

第四十二条 运行安全的目标是保证信息系统日常运行的安全稳定，对信息系统的运行环境、技术支持、操作使用、病毒防范、备份措施、文档建立等方面实施安全性管理。

第四十三条 枢纽台主要负责人为第一责任人，应建立完善本单位网络安全运行机制，可设立专门的部门负责本单位网络安全工作的组织、协调、检查和对外联络，应明确各信息系统的网络安全责任主体，并与各主体责任人签订网络安全责任书。

第四十四条 枢纽台信息系统实行等级保护制度，设立信息系统的运行单位应按照国家和行业有关要求，进行信息系统定级，编写备案材料，经行政部门审核后，送公安机关备案，并将备案情况反馈行政部门。应按照等级保护有关要求开展安全测评和安全整改。

第四十五条 枢纽台应遵循“同步规划、同步建设、同步运行”的原则，网络安全防护体系与主体工程同时规划、建设、验收和使用。

第四十六条 信息系统应在安全测试（定级为三级以上的信息系统须进行网络安全等级测评）通过后方可上线运行。上线运行后，应对系统的安全性和可能存在的风险每年至少进行一次检测评估，发现问题及时整改。连通互联网的信息系统还应每年至少进行一次网络安全渗透测试。相关检测测试结果和整改情况，报所属行政部门备案。

第四十七条 应建立包括业务、产品、服务的立项、开发、测试、验收、上线、运行、检修、维护、合作、外包、下线等环节在内的安全管理制度，确保产品、数据、业务等安全。

第四十八条 重要保障期前，各运行单位应开展隐患排查，完善各项防范措施。重要保障期间，领导应靠前指挥，重点部门、重要岗位应建立 24 小时值班制度，加强监测。

第四十九条 应建立网络安全监测系统，实时监测信息系统的运行状态，对可能引发网络安全事件的信息进行收集、分析和判断，发现异常情况及时处置和报告。

第五十条 运行单位要与属地公安机关及相关的安全服务提供商、内容分发网

络（CDN）服务提供商、互联网接入服务提供商、网络服务提供商等建立联动机制，发生安全事件时，各负其责，快速处置。

第五十一条 发生网络安全事件时，相关单位应立即启动预案，采取有效措施，阻止有害信息传播，降低信息系统损害程度，尽快分析查找事件原因，对发现的问题及时进行整改。如涉及攻击、破坏等违法犯罪，应尽可能保护好相关数据、记录、资料和现场，于 24 小时内向当地公安机关报案，并配合调查取证。

第五十二条 发生网络安全事件，应立即上报技术中心，按照相关要求报告广播电视行政部门。

第五十三条 运行单位应根据行业的网络安全事件应急预案制定本单位的应急预案，并到所属行政部门备案。根据网络安全风险及业务变化及时修订，定期组织开展应急演练。

第五十四条 应配合广播电视行政部门建立完善相关工作机制，根据技术中心的统一部署，为监测提供必要的数据接口，为检查提供必要的资料、场地，按要求及时报送相关工作情况和数据报表。建立本单位信息通报机制，及时反馈行政部门通报网络安全威胁漏洞的整改情况。

第五十五条 应将网络安全建设、运维、培训、检测、应急处置等所需经费纳入年度预算。各单位应以专项形式按程序申报预算，财务管理部门应优先安排该类经费，保证各项工作顺利开展。

第五十六条 应定期对全体人员进行网络安全教育，对网络安全技术人员进行网络安全专业知识和技能培训，定期考核，考核合格后方可上岗。

第五十七条 对信息系统运行阶段的任何变化，数据、软件、物理设置等，都应实施技术监控和管理手段以确保其完整性，即防止信息被非法复制、非授权的修改及破坏，确保信息系统的任何查询和变更操作是经过授权及合法性验证。

第五十八条 软件是计算机系统运行的核心。软件的安全保护及正确运行至关重要，应严格控制计算机系统中软件的使用。软件的随意下载及运行，将使计算机网络系统容易产生病毒侵入，干扰系统正常运行及系统安全防护的失效。新版软件、版本升级过程要实施投产前必要

的软件检验和测试。应确保软件的版本合法。

第五十九条 技术支持人员、软硬件供应商、第三方技术提供商都有可能从事技术维护服务。必须实施严格的访问控制机制和制度，确保只有合法的人员才能进入系统从事维护活动。

第六十条 应建立多层次、立体式病毒防护体系，维持病毒采集、汇总、上报、升级的渠道顺畅，提高病毒检杀的响应能力，从网络、服务器、单机的各个环节有效防范病毒侵入。

第六十一条 信息系统的程序和数据备份至关重要。备份的周期取决于数据的变动频度及变动的重要程度，重要的系统和数据必须做到异地备份，确定备份的工作流程。要经常检测备份以保证其可用性。备份应安全存放。

第六十二条 对各种信息媒介应实施物理环境保护及其他各种控制措施，确保磁带、磁碟、光盘、打印数据等重要媒介不失密、不被破坏、不被篡改和不失效，维护其完整性和可用性，并授权专人负责介质的登记、存放、检验等维护工作。

第六十三条 计算机技术维护和操作都应有相应的文档，以确保支持的连续性和一致性。正确的操作描述文档有助于防止对安全的忽视、减少操作的失误。

第六十四条 当数据信息、硬件设备、软件程序结束运行使用时，视需求分别进行存档、废弃和销毁处理。

第十章 应急计划

第六十五条 信息系统应急计划的目标是分析信息系统可能出现的紧急事件或者灾难事故，技术支持和业务部门应建立一整套应急措施，以保障关键核心业务的连续服务。

第六十六条 一旦发生重大的或灾难性事故时，信息安全工作小组应迅速进行灾情分析，并上报信息安全领导小组，成立应急领导小组，负责指挥执行紧急应变计划，排除灾难事故。同时应急领导小组还要组织相关的部门做好对外的解释、宣传和公告以及保卫工作，防止事态

的扩大。

第六十七条 应急计划要充分考虑到信息系统可能面临的由于系统设备、软件、网络通讯而造成的紧急故障，地震、火灾等自然灾难事故，以及由计算机病毒、恶性程序代码和来自行内、外部人员非法侵入产生的安全事件。应建立对安全事件的快速反应机制，并使之成为应急计划的一部分。

第六十八条 根据业务服务的要求以及对事故的恢复能力，应确定应急措施所维持的核心业务及优先级别。

第六十九条 应急措施的建立将维持关键核心业务服务，应对构成核心业务的全部资源进行分析，明确相关的人员、设备处理能力、基础服务支持、数据和应用系统、文档及文件等资源。

第七十条 应急方案的设立应充分考虑可能发生的事故，同时应本着实用、灵活、低成本原则。根据各核心业务的资源，确定应急方案的人员指挥架构及工作流程。应急计划要明确描述紧急事故发生、核心业务的应急处理、正常业务的恢复等各环节的流程及操作步骤。

第七十一条 为确保应急计划的正确启用，应确保编写正确的应急手册及对人员的培训。

第七十二条 为保证应急计划的有效，应针对不同业务系统要求，定期进行应急方案的测试演练，并适应当前系统资源的变化，及时调整、完善应急计划。

第七十三条 针对恶性安全事件，信息系统应具备相应的技术措施，提供对安全事件的快速反应机制，并及时中断安全事件对其他系统的危害，迅速搞清本系统存在的漏洞，有效防范未来事故的再次出现。

第十一章 安全责任

第七十四条 任何人员只能访问其职责权限范围内的信息资源，如发现超越职责权限访问资源的行为，应立即停止其访问权利，并给予警告。

第七十五条 任何人员如有故意编造或发送恶意程序、输入计算机病毒，影响正常办公、业务信息处理秩序的行为，视情节严重情况，给予相应

的行政处分，构成犯罪的应送交公安部门处理。

第七十六条 枢纽台网络与信息安全领导小组对枢纽台计算机信息安全负领导责任，对制定枢纽台计算机信息安全的实施策略和原则负直接责任；并保障信息安全所需的人、财、物资源，仲裁有关计算机信息安全的重大事项。

第七十七条 信息网络中心：评估和鉴定枢纽台计算机信息安全技术体系；监督检查枢纽台各部门内部安全制度的执行情况，技术防范的实施情况，解决计算机信息安全问题；落实枢纽台信息安全策略，安全体系资源的配给和调度以及安全建设的规划组织、技术协调。对所建设的信息系统，负有安全设计、安全建造、安全稳定运行、安全变更维护，以及安全防范的责任；对安全合规地使用信息系统，审慎地进行电脑操作和业务管理负责。

第七十八条 办公室：对违反安全策略和安全操作并造成重大影响的人和事，按国家和枢纽台的相关规定严肃处理；办公室应遵照安全策略落实奖惩措施；负责人员录用过程中的人员资格、资质和背景调查；负责人员离职、离岗过程中的手续办理审查。

第十二章 附 则

第七十九条 本标准由枢纽台信息网络中心负责解释。

第八十条 本标准自颁布之日起实行。