迁西职教中心

网络与信息安全管理规范及工作职责

迁西职教中心
网络与信息安全管理规范及工作职责

为了加强数字校园信息化安全保障工作，全面提高信息安全防护能力，加强对我校校园网的运行和使用管理，防止有害信息侵害，促进我校校园网的健康发展，学校决定健全和完善学校统一领导、分级负责、各司其责的信息安全管理体系，完善各项规章制度，建立校园网络信息管理和运行安全防范监控机制，切实做好我校网络与信息安全保障工作。学校特成立网络与信息安全管理机构（领导小组），工作人员按要求履行相关职责。

1、安全管理机构和人员管理要求

（1）岗位设置要求

1）应成立和信息化工作领导小组，统筹推进或组织本单位的和信息化工作，并作为单位信息化建设和管理的决策机构。一般情况下单位的主要负责人担任本单位和信息化领导小组组长。

2）应设立和信息化工作领导小组办公室，跨部门统筹协调与信息化工作。

3）应设立网络安全管理员、系统平台管理员、网络管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。

（2）人员配备要求

1）应配备一定数量的系统管理员、网络管理员、安全管理员等。

2）应配备专职安全管理员，不可兼任。

（3）授权和审批要求

1）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批

准人等。

2）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。

3）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

（4）沟通和合作要求

1）应加强各类管理人员之间、组织内部机构之间以及职能部门内部的合作与沟通，定期召开协调会议，共同协作处理问题。

2）应加强与兄弟单位、公安机关、各类供应服务商、业界专家及安全组织的合作与沟通。

3）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

（5）审核和检查要求

1）应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

2）应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

3）应制定、实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

（6）人员录用要求

1）对被录用人员的身份、能力、素质等进行审查，对其所具有的技术、技能进行培训。

2）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。

（7）人员离岗要求

1）应及时终止或修改离岗人员的所有访问权限、密码等，取回各种身份证件、门禁、密钥等以及单位提供的软硬件设备。

2）应办理严格的调离交接手续，并承诺调离后的保密义务后方可离开。

（8）安全意识教育和培训要求

1）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

2）应针对不同岗位制定不同的培训计划，对网络安全基础知识、岗位操作规程等进行培训。

（9）外部人员访问管理要求

1）应确保在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案。

2）应确保在外部人员接入网络访问系统前先提出书面申请，批准后由专人开设账号、分配权限，并登记备案。

3）外部人员离场后应及时清除其所有的访问权限。

4）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

2、安全管理机构和人员管理措施

（1）岗位设置

为有效实施管理，应建立管理组织架构。岗位设置需要考虑的元素包括：职责分离、工作职责和岗位轮换。

职责分离：职责分离属于安全概念，是指把关键的、重要的和敏感的工作任务分配给若干的管理员或高级执行者，这样能阻止任何一个人具备

破坏或削弱重要安全机制的能力，可以将职责分离视为对管理员的最小特权原则的应用。

工作职责：工作职责是要求工作人员在常规的基础上执行的特定工作任务。根据工作职责，工作人员需要访问各种不同的对象、资源和服务。在安全的网络中，用户必须被授予访问与其工作任务有关的权限。

网络与信息化领导小组是本单位网络安全和信息化工作的最高领导决策机构，它不隶属于任何部门，其组长一般由本单位主要负责人担任，成员一般由本单位业务和网络安全相关的若干管理部门主要负责人组成。网络与信息安全领导小组是一个常设机构，负责定期研究并对本单位网络安全与信息化工作进行指导、监督检查和管理，可以根据实际情况随时进行调整。

网络与信息安全领导小组下设领导小组办公室（以下简称网信办，内设信息中心），承担具体网络安全管理和保障任务。网信办一般下设网络安全管理工作小组及具体的网络安全管理岗位，一般由学校领导、行政及相关部门领导、信息中心主要技术人员、运维人员等组成，主要承担规划、协调、技术、管理、维护、信息发布与安全、安全培训等具体工作。

（2）人员配备

1）网络安全管理员

网络安全管理员的职责如下：

① 负责组织建立、实施和维护网络安全策略、标准、规章制度和各项操作流程。

② 负责对安全产品购置提供建议，负责组织制定各种安全产品策略与配置规则，负责跟踪安全产品投产后的使用情况。

③ 负责指导并监督系统管理员（包括系统管理员、网络管理员、等）

及普通用户与安全相关的工作。

④ 负责组织信息系统的安全风险评估工作，并定期进行系统漏洞扫描，形成安全评估报告。

⑤ 根据本单位的需求，定期提出改进意见，并上报管理部门。

⑥ 定期查看网络安全站点的安全公告，跟踪和研究各种网络安全和攻击手段，在发现可能影响网络安全的安全漏洞和攻击手段时，及时做出相应的对策，通知并指导主机系统管理员进行安全防范。

⑦ 负责组织审议各种安全方案、安全审计报告、应急计划以及整体安全管理制度。

⑧ 负责并参与安全事故调查。

2）网络管理员

网络管理员的职责如下：

① 负责网络的部署以及网络产品、产品的配置、管理与监控，并对关键配置文件进行备份，及时修补网络设备的。

② 协助安全管理员制定网络设备安全配置规则，并落实执行。

③ 为网络安全管理员提供完整、准确地记录重要网络设备和网站运行活动的运行日志。

④ 在网络及设备异常或故障发生时，详细记录发生异常时的现象、时间和处理方式，并及时上报。

⑤ 编制网络设备的维修、报损、报废等计划，报主管领导审核。

3）系统平台管理员

系统平台管理员的职责如下：

① 对系统、系统进行安全配置，修补已发现的。

② 负责系统、系统的用户账号管理，对系统中所有的用户进行登记

备案；对系统、系统的用户、口令的安全性进行管理；对系统、系统登录用户进行监测和分析。

③ 负责业务数据及系统其他重要数据的备份与备份数据管理工作。

④ 负责应用程序及中间件系统其他重要数据的备份与备份数据管理工作。

⑤ 为安全审计员提供完整、准确的系统、系统运行活动的日志记录，详细记载发生异常时的现象、时间和处理方式，并及时上报。

⑥ 在发生安全问题导致数据或应用程序损坏或丢失时，进行数据或应用程序的恢复。

⑦ 根据业务发展的需求，提交数据存储介质购买或存储系统扩容计划。

① 对业务应用系统进行安全配置，督促软件开发商提供补丁修补已发现的漏洞。

② 对业务应用系统的用户、口令的安全性进行管理，对业务应用系统的登录用户进行监测和分析。

③ 负责提出数据的备份要求，制定数据备份策略，督促数据库管理员按照备份方案按时完成，并恢复所需数据。

④ 实施系统软件版本管理、应用软件备份和恢复管理。

5）网络安全员

网络员的职责如下：

① 负责定期对主机系统、网络产品、应用系统的日志文件进行分析审计，发现问题及时上报。

②负责对保障管理活动进行独立的监督，提供内部独立的审计和评估工作，并根据需要可以协同外部审计评估机构进行评估和认证，为决策领

导提供信息系统和保障执行状况的客观评价。

③负责安防系统的安全，确保师生校园信息的安全

6）信息安全管理员

①负责执行和监督整个系统全面的信息安全工作。

②制定病毒防范操作规程。

③定时升级网络杀毒软件的病毒库，监督个人杀毒软件的升级工作。

④实时监控重要业务系统和数据的安全，杜绝非法开放的入侵途径，降低侵害的影响。

⑤及时报告上级部门病毒和感染情况，提供感染频率高和严重性强的病毒的有效解决方案。

⑥负责系统交易、传输、认证密钥的管理以及加密机的操作。

7）资产管理员

资产管理员的职责如下：

负责信息技术部门全部资产的采购、登记、分发、回收、废弃等管理。

8）信息审核员

信息审核员的职责如下：

①全面负责网络信息审核、监管；负责校园网站新闻、图片、资源的上传及审核工作

②主要负责非技术性的、常规的安全工作，如信息处理场地的保卫、办公室的安全，验证出入信息中心的手续和多项规章制度的落实。

9）信息员

负责信息内容及材料的收集、组织、整理、发布、上传。

10）安全培训员

安全法律顾问的职责如下：

①负责师生文明上网的安全教育和网络道德教育。

②负责本单位与外单位签署安全服务合同的法律咨询工作。

11）信息技术员

外聘技术专家的职责如下：

①根据实际工作需要和本单位特点，可以选择长期或临时性聘请行业内有关技术专家提供网络安全规划、建设、实施、应急处置、故障研判等方面的咨询建议。

②根据学校教育信息化发展规划制订本教研组教育信息发展计划；负责本教研组计算机日常维护，确保运行安全。

③配合其他岗位开展相关工作。

（3）授权和审批

应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度，分别详细记录在系统变更、重要操作、物理访问等管理体系中不同的授权和审批流程。

授权和审批的基本原则：

1）坚持根据单位及上级部门的管理变化情况适时调整授权的原则，兼顾相对稳定和持续化。

2）坚持授权与授责相结合、授权与监督相结合、有权必有责、有责要担当、失责必追究的原则。

（4）沟通和合作

加强各类管理人员、组织内部机构之间以及职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理问题。

（5）审核和检查

1）网信办负责组织审核和安全检查管理，并严格规范安全审核和安全检查工作，按规定开展审核和安全检查活动。

2）上级单位应牵头组织对下级单位或部门进行检查，各下级单位或部门负责组织本单位内部的自查工作。

3）定期（至少每半年一次）或根据需要组织对信息系统的全面安全审核和检查，包括现有安全技术和管理措施的有效性、安全配置与安全策略的一致性、安全管理制度及执行情况等。

4）定期（至少每半年一次）或根据需要进行常规的安全审核和检查，包括系统日常运行安全、系统漏洞、备份与恢复、应急响应等情况。

5）在审核和安全检查中发现的安全隐患，要及时向网信办提交检查报告，网信办应及时制定隐患整改计划，提出改进意见，指导、督促相关部门限期整改，消除安全隐患。

（6）人员录用

由单位人力部门负责人员录用相关事宜，对被录用人员的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核，并签署保密协议。

（7）人员离岗

工作人员离岗，应按照信息系统安全管理的要求，办理相关交接和责任变更手续，管理部门应及时更换系统口令，注销其所有账号，撤销其出入安全区域、接触敏感信息的权限，删除有关文件和信息，交接有关设备和文件，确保密码、设备、技术资料及相关敏感信息的安全。关键岗位人员离岗须承诺调离后的保密义务后方可离开。

（8）安全意识教育和培训

为了确保管理制度在单位内部得到有效的运行，督促各部门对体系进

行持续有效的改进。网信办要负责制定意识教育和培训计划，开展管理制度、保密教育、技术防护措施等教育培训。单位全体工作人员每年应接受不少于两次的保密教育，关键岗位（部门）涉密人员，每年度必须接受不少于两次的保密岗位技能培训。保密教育采取授课、观看警示教育片等形式进行，如有可能组织一次保密知识测试。对涉及国家秘密、单位重要秘密的重大活动、重要项目，采取对有关人员进行有针对性的保密教育。开展教育培训的所有活动记录，应按规定归档保存。

安全意识教育和培训的基本内容：

1）网络安全保密工作指导思想和方针政策的宣传教育。

2）国家保密、法规和规章的宣传教育。

3）等级保护法规教育。

4）网络安全保密形势的宣传教育。

5）网络安全保护技术和技能的宣传教育。

6）新入岗人员的网络安全保密教育；

7）涉密人员的网络安全保密教育；

8）关键岗位、部门人员的网络安全保密教育；

9）各级主管领导的网络安全保密培训教育。

10）新入岗必须接受的保密法规的内容。

（9）外部人员访问管理

通过对外部人员的访问管理，减少安全风险，确保本单位计算机信息系统安全。外部人员包括临时工作人员、实习人员、参观检查人员、外来技术人员。

信息中心负责外部人员安全服务管理制度制定和技术防护措施；确定外部人员是否符合访问要求，与外部人员签订服务合同和保密协议，对外

部人员的访问进行审批。外部人员如需访问重要区域，由外部人员向信息中心提出书面申请，经信息中心审核后报主管领导审批，主管领导签字并指派信息中心相关人员陪同进入重要区域；对于外部人员访问重要区域情况须由运维人员填写《外部人员访问重要区域记录表》，记录进入时间、离开时间、访问区域及陪同人员等。

访问服务结束后，本单位责任人员必须对信息系统和设备进行安全检查，确认对信息系统和设备没有造成安全影响后，双方签字方可离开现场。

信息中心及各业务部门负责各项管理制度和技术措施的具体落实；对外部人员进行网络安全控制和监督。对因工作需要提供给第三方安全服务人员的信息系统技术资料、管理制度等相关资料，要详细记录所提交的文档编号、内容简要、页码数、附件等相关内容，并要求服务方对检查结果的所有权、委托方的专利权、验证结果等进行保密。

信息中心负责对服务方各项保密措施的实施进行监督检查，并就发现的问题及时向对方通报。

迁西职教中心