27001.CN 信息安全管理体系适用性声明(ISO/IEC 27001：2022)

版本：1.0　　发布日期:

控制项			是否适用	删减理由	控制文件
5	**组织控制**				
5.1	信息安全策略	信息安全策略和特定主题的策略应被定义，由管理者批准，发布、传达给所有员工和外部相关方，并按策划的时间间隔或当重大变化发生时进行信息安全策略评审。	是	N/A	《信息安全策略管理程序》
5.2	信息安全角色和职责	应依据组织需求定义信息安全职责和角色。	是	N/A	《人力资源安全管理程序》
5.3	职责分离	应分离冲突的职责及其责任范围。	是	N/A	
5.4	管理职责	管理者应要求所有员工按照组织已建立的策略、特定主题的策略和规程应用信息安全。	是	N/A	
5.5	与职能机构的联系	组织应建立和维护与相关职能机构的联系。	是	N/A	《沟通管理程序》
5.6	与特殊利益团的联系	组织应建立和维护与特殊利益团，或其他专业安全论坛和专业协会的联系。	是	N/A	
5.7	威胁情报	与信息安全威胁相关的信息应被收集和被分析，以获得威胁情报。	是	N/A	《威胁情报管理规范》
5.8	项目管理中的信息安全	信息安全应被整合到项目管理中。	是	N/A	《项目信息安全管理规范》
5.9	信息和其他关联资产清单	应编制和维护信息和其他关联资产清单，包含其所有者。	是	N/A	《信息资产管理程序》
5.1	信息和其他关联资产的可接受使用	应识别信息和其他关联资产的可接受使用规则，以及其处理规程，形成文件并加以实施。	是	N/A	
5.11	资产归还	员工和其他相关方在任用、合同或协议变更或终止时，应归还其占用的所有组织资产。	是	N/A	
5.12	信息的分级	信息应按照基于保密性、完整性、可用性以及相关方要求的组织的信息安全需求进行分级。	是	N/A	
5.13	信息的标记	应按照组织采用的信息分级方案，制定并实施一组适当的信息标记规程。	是	N/A	
5.14	信息传输	应为组织内部以及组织与其他方之间的所有类型的传输设施制定信息传输规则、规程或协议。	是	N/A	
5.15	访问控制	应根据业务和信息安全需求，建立对信息和其他关联资产的物理和逻辑访问的控制规则，并予以实施。	是	N/A	《账户与口令安全管理规范》
5.16	身份管理	应管理身份的整个生命周期。	是	N/A	
5.17	鉴别信息	应通过正式的管理过程控制鉴别信息的分配和管理，包括建议人员适当处理鉴别信息。	是	N/A	
5.18	访问权	应根据组织特定主题的访问控制策略和规则对信息和其他关联资产的访问权进行分配、评审、修改和删除。	是	N/A	
5.19	供应商关系中的信息安全	为管理使用供应商提供的产品或服务所带来的信息安全风险，相关过程和规程应被定义，并予以实施。	是	N/A	《供应商信息安全管理程序》
5.2	在供应商协议中强调信息安全	应基于供应商关系类型，建立相关信息安全要求，并与各供应商就信息安全要求达成一致。	是	N/A	

5.21	信息与通信技术(ICT)供应链的信息安全管理	为管理信息与通信技术(ICT)产品和服务供应链相关的信息安全风险，相关过程和规程应被定义，并予以实施。	是	N/A	《供应商信息安全管理程序》
5.22	供应商服务的监视、评审和变更管理	组织应定期监视、评审、评价供应商信息安全实践和服务交付，并应管理过程中的变更。	是	N/A	
5.23	使用云服务的信息安全	应根据组织信息安全要求，为获取、使用、管理和退出云服务建立流程。	否	体系覆盖范围未使用云服务	N/A
5.24	信息安全事件管理的策划和准备	组织应定义、建立和沟通信息安全事件管理过程、角色和职责，以策划和准备信息安全事件的管理。	是	N/A	《信息安全事件管理程序》
5.25	信息安全事态的评估和决策	组织应评估信息安全事态并决定其是否属于信息安全事件。	是	N/A	
5.26	信息安全事件的响应	组织应按照文件化的规程响应信息安全事件。	是	N/A	
5.27	从信息安全事件中学习	应利用在信息安全事件中得到的知识来增强和提升信息安全控制。	是	N/A	
5.28	证据的收集	组织应建立识别、收集、获取和保存信息安全事件的相关证据的规程，并予以实施。	是	N/A	
5.29	中断时的信息安全	组织应策划如何在中断期间将信息安全维持在适当的水平。	是	N/A	《信息安全连续性管理程序》
5.3	业务连续性的信息与通信技术（ICT）的准备	应基于业务连续性目标和信息与通信技术（ICT）连续性要求，策划信息与通信技术（ICT）的准备，并予以实施，保持和测试。	是	N/A	
5.31	法律、法规、规章和合同要求	应识别信息安全相关的法律、法规、规章和合同要求，以及组织满足这些要求的方法，并形成文件和保持更新。	是	N/A	《相关方需求和期望管理程序》
5.32	知识产权	组织应实施适当的规程，以保护知识产权。	是	N/A	
5.33	记录的保护	记录应进行保护以防其丢失、毁坏、伪造、未授权访问和未授权发布。	是	N/A	《记录控制程序》
5.34	隐私和个人身份信息的保护	识别并满足关于隐私保护和个人身份信息(PII)保护的要求。	是	N/A	《相关方需求和期望管理程序》
5.35	信息安全的独立评审	应按策划的时间间隔或在重大变化发生时，对组织的信息安全管理方法及其实施包括人员、过程和技术应进行独立评审。	是	N/A	《内部审核管理程序》
5.36	策略、规则和信息安全标准的符合性	应定期评审组织信息安全策略、特定主题的策略、规则和标准的符合性。	是	N/A	《文件控制程序》
5.37	文件化的操作规程	信息处理设施的操作规程应形成文件，并提供给有需要的人员使用。	是	N/A	《信息处理设施安全管理规范》
6	**人员控制**				
6.1	审查	在其加入组织之前，应对所有任用候选者的背景进行验证核查，并在其基础之上，考虑适用的法律、法规和道德规范，以及与业务要求、访问信息的等级和察觉的风险相适宜。	是	N/A	《人力资源安全管理程序》 《信息安全奖惩挂你程序》 《信息安全奖惩实施细则》
6.2	任用条款及条件	雇佣合同协议应声明员工和组织对信息 安全的职责。	是	N/A	
6.3	信息安全意识、教育和培训	组织和相关方的员工，应按其工作职能，接受适当的意识、教育和培训，以及定期更新的组织信息安全策略、特定主题策略及规程。	是	N/A	
6.4	违规处理过程	应有正式的、且已被传达的违规处理过程以对信息安全违规的员工和其他相关方采取措施。	是	N/A	

6.5	任用终止或变更的职责	应确定任用终止或变更后仍有效的信息安全职责和义务，传达至相关员工和其他相关方并执行。	是	N/A	
6.6	保密或不泄露协议	应识别、文件化和定期评审反映组织信息保护需要的保密性或不泄露协议，并由员工和其他相关方签署。	是	N/A	
6.7	远程工作	当员工远程工作时，应实施安全措施，以保护在组织场所以外所访问的、处理的或存储的信息。	是	N/A	
6.8	信息安全事态报告	组织应提供一种机制，使人员能够通过适当的渠道及时报告观察到的或可疑的信息安全事态。	是	N/A	
7	**物理控制**				
7.1	物理安全边界	应定义和使用安全边界来保护包信息和其他相关资产的区域。	是	N/A	《物理和环境安全管理规范》
7.2	物理入口	安全区域应由适合的入口控制和访问点所保护。	是	N/A	
7.3	办公室、房间和设施的安全	应为办公室、房间和设施设计并采取物理安全措施。	是	N/A	
7.4	物理安全监视	边界应被持续监视，以防止未授权的物理访问。	是	N/A	
7.5	物理和环境威胁的防护	应设计和实施针对物理和环境威胁（例如，自然灾害和对基础设施的其他有意或无意的物理威胁）的保护措施。	是	N/A	
7.6	在安全区域工作	在安全区域工作的安全措施应被设计和被实施。	是	N/A	
7.7	清空桌面和屏幕	针对纸质和可移动存储介质的清理桌面策略，以及针对信息处理设施的清理屏幕策略，应被定义和适当执行。	是	N/A	《信息资产管理程序》 《信息处理设施安全管理规范》
7.8	设备安置和保护	设备应安全的安置和保护。	是	N/A	《IT设备安全管理规范》
7.9	组织场所外的资产安全	组织场所外的资产应被保护。	是	N/A	
7.1	存储介质	存储介质应按照组织的分类方案和处理要求，对其获取、使用、运输和处置的生命周期进行管理。	是	N/A	《介质安全管理规范》
7.11	支持性设施	应保护信息处理设备使其免于由支持性设施的失效而引起的电源故障和其他中断。	是	N/A	《物理和环境安全管理规范》
7.12	布缆安全	应保护传输电力、数据或支持信息服务的电缆不受拦截、干扰或损坏。	是	N/A	
7.13	设备维护	设备应予以正确地维护,以确保其持续的可用性、完整性和信息的保密性。	是	N/A	《IT设备安全管理规范》
7.14	设备的安全处置或再利用	包含储存介质的设备的所有部分应进行核查，以确保在处置或再利用之前，任何敏感信息和注册软件已被删除或安全的重写。	是	N/A	
8	**技术控制**				
8.1	用户终端设备	存储在、由用户终端设备处理或通过用户终端设备访问的信息应受到保护。	是	N/A	《信息处理设施安全管理规范》
8.2	特许访问权	应限制和管理特许访问权的分配和使用。	是	N/A	
8.3	信息访问限制	应按照建立的访问控制的特定主题策略限制信息和其他关联的资产的访问。	是	N/A	
8.4	源代码的访问	对源代码、开发工具和软件库的读写访问应得到适当的管理。	是	N/A	《信息系统开发安全管理规范》

8.5	安全鉴别	应基于信息安全访问限制和访问控制的特定主题策略，实施安全鉴别技术和规程。	是	N/A	《信息系统开发安全管理规范》
8.6	容量管理	应根据当前和预期的容量需求，对资源的使用进行监视和调整。	是	N/A	《信息处理设施安全管理规范》
8.7	恶意软件防范	恶意软件的防范应被实施，并通过适当的用户意识来支持该过程。	是	N/A	
8.8	技术方面脆弱性的管理	应及时获取在用的信息系统的技术方面的脆弱性信息，评价组织对这些脆弱性的暴露状况并采取适当的措施。	是	N/A	《信息系统开发安全管理规范》
8.9	配置管理	硬件、软件、服务和网络的配置(包括安全配置)应被建立文件化的清单，并予以实施、监视和评审。	是	N/A	《配置管理规范》
8.1	信息删除	存储在信息系统、设备或任何其他存储介质中的信息，当不再需要时应予以删除。	是	N/A	《数据防护管理规范》
8.11	数据脱敏	应根据组织访问控制的特定主题策略和其他相关特定主题的策略，以及业务需求，并考虑适用的法律，使用数据脱敏。	是	N/A	
8.12	数据泄露防护	数据泄露防护措施应应用于处理、存储或传输敏感信息的系统、网络和任何其他设备。	是	N/A	
8.13	信息备份	应按照备份的特定主题策略，对信息、软件和系统镜像进行维护，并定期测试。	是	N/A	《信息处理设施安全管理规范》
8.14	信息处理设施的冗余	信息处理设施应被实施，并有足够的冗余，以满足可用性要求。	是	N/A	
8.15	日志	记录活动、异常、故障和其他相关事件的日志应产生、存储、保护和分析。	是	N/A	
8.16	监视活动	应监控网络、系统和应用程序的异常行为，并采取适当行动评估潜在的信息安全事件。	是	N/A	
8.17	时钟同步	本机构所使用之资讯处理系统之时钟应与经批准的时间源同步。	是	N/A	
8.18	特权实用程序的使用	对于可能超越系统和应用控制的实用程序的使用应予以限制并严格控制。	是	N/A	
8.19	运行系统的软件安装	应实施规程和措施，以安全地管理运行系统上的软件安装。	是	N/A	
8.20	网络安全	应防护、管理和控制网络和网络设备以保护系统和应用中的信息。	是	N/A	《网络安全管理规范》
8.21	网络服务的安全	网络服务的安全机制、服务级别和管理要求应予以识别、实施和监视。	是	N/A	
8.22	网络隔离	应在组织网络中隔离信息服务、用户及信息系统所使用的网络。	是	N/A	
8.23	网页过滤	应对外部网站的访问进行管理，以减少暴露于恶意内容。	是	N/A	
8.24	密码学的使用	有效使用密码学的规则，包括密钥的管理，应被定义，并予以实施。	是	N/A	《信息系统开发安全管理规范》
8.25	安全的开发生命周期	软件和系统的安全开发规则应被建立，并予以应用。	是	N/A	
8.26	应用安全要求	当开发或获取应用时，信息安全要求应被识别、规定和批准。	是	N/A	
8.27	安全系统架构和工程原则	应建立和维护文件化的工程安全系统原则，并应用于任何的信息系统开发活动。	是	N/A	

8.28	安全编码	安全编码原则应被应用于软件开发。	是	N/A	《信息系统开发安全管理规范》
8.29	开发和验收中的安全测试	在开发生命周期中，安全测试过程应被定义，并予以实施。	是	N/A	
8.3	外包的开发	组织应指导、监视和评审外包的系统开发的相关活动。	是	N/A	
8.31	开发、测试和生产环境的分离	开发、测试和生产环境应被分离，并予以保护。	是	N/A	
8.32	变更管理	信息处理设施和信息系统的变更应遵循于变更管理规程。	是	N/A	《信息处理设施安全管理规范》
8.33	测试信息	测试信息应被适当帅选、保护和管理。	是	N/A	
8.34	审计测试时的信息系统的保护	涉及运行系统验证的审计测试和其他保证活动应由测试人员和适当的管理人员策划和商定。	是	N/A	