

# 聊城ISO27001信息安全管理体系认证，永盛认证服务

产品名称	聊城ISO27001信息安全管理体系认证，永盛认证服务
公司名称	山东永盛认证技术有限公司
价格	15000.00/张
规格参数	
公司地址	山东省聊城经济技术开发区东昌东路星美办公2号楼1602室（注册地址）
联系电话	13406396805

## 产品详情

### 信息安全管理体系认证原理和好处

标准化组织/IEC17799-2000包含127项安全控制措施，帮助组织识别运营期间影响信息安全的因素。组织可以根据适用的法律、法规和公司章程选择和使用它们，或者添加其他附加控制。化组织(标准化组织)于2005年修订了ISO 17799。修订后的标准是ISO27000标准系列的部分——化组织/IEC 27001。新标准去掉了9项控制措施，增加了17项控制措施，对部分控制措施进行了重组，增加了新的一章，更符合逻辑，更适合应用。并修改了一些控制措施措辞。修订后的标准包括11章:

- (1)安全策略。指定信息安全策略，为信息安全提供管理指导和支持，并定期审查。
- (2)信息安全组织。建立信息安全管理组织体系，在内部实施和控制信息安全的实施。
- (3)资产管理。检查所有信息资产，对信息进行良好分类，并确保信息资产得到适当保护。
- (4)人力资源保障。确保所有员工、承包商和第三方都了解信息安全威胁和相关事项以及各自的责任和义务，以减少人为错误、盗窃、欺诈或滥用设施的风险。
- (5)物理和环境安全。定义安全区域，防止未经授权的访问、损坏和干扰办公空间和信息；保护设备安全，防止信息资产丢失、损坏或被盗，干扰企业业务；同时，应进行全面控制，以防止信息和信息处理设施被损坏或被盗。
- (6)沟通和运营管理。制定操作规则和职责，确保信息处理设施的正确和安全运行；建立系统规划和验收标准，将系统故障风险降至低；防范恶意代码和移动代码，保护软件和信息的完整性；做好信息备份和网络安全管理，确保网络中信息的安全及其配套基础设施的保护；建立媒体处置和安全法规，防止资产损坏和业务中断；防止信息和软件在组织间交换时丢失、修改或滥用。

(7)访问控制。制定访问控制策略，避免未经授权访问信息系统，让用户知道自己的责任和义务，包括网络访问控制、操作系统访问控制、应用系统和信息访问控制，监控系统访问和使用，定期检测未经授权的活动；在使用移动办公和远程控制时，也要保证信息安全。

(8)系统获取、开发和维护。标记系统的安全需求，确保安全成为信息系统的内置部分，控制应用系统的安全性，防止应用系统中用户数据的丢失、修改或误用；通过加密手段保护信息的机密性、真实性和完整性；控制对系统文件的访问，确保系统文档和源代码的安全；严格控制开发和支持过程，维护应用系统软件和信息的安全。

(9)信息安全事故管理。报告信息安全事件和薄弱环节，及时采取纠正措施，确保信息安全事件得到持续有效的管理，并确保及时修复。

(10)业务连续性管理。目的是减少业务活动的中断，保护关键业务流程免受重大故障或自然灾害的影响，并确保及时恢复。

(11)合规性。信息系统的设计、运行、使用过程和管理应符合法律法规、组织安全政策和标准的要求，并对系统审计进行控制，使信息审计过程的有效性