国际标准

ISO/IEC 27001:2022

第3版

2022-10

信息安全、网络安全和隐私保护

信息安全管理体系

要求

索引号
ISO/IEC 27001:2022

目　　次

前　　言 III
引　　言 IV
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 组织环境 1
4.1 理解组织及其环境 1
4.2 理解相关方的需求和期望 1
4.3 确定信息安全管理体系范围 2
4.4 信息安全管理体系 2
5 领导 2
5.1 领导和承诺 2
5.2 方针 2
5.3 组织的角色、责任和权限 3
6 规划 3
6.1 应对风险和机会的措施 3
6.2 信息安全目标及其实现规划 4
6.3 针对变更的规划 4
7 支持 4
7.1 资源 5
7.2 能力 5
7.3 意识 5
7.4 沟通 5
7.5 文件化信息 5
8 运行 6
8.1 运行规划和控制 6
8.2 信息安全风险评估 6
8.3 信息安全风险处置 6
9 绩效评价 6
9.1 监视、测量、分析和评价 6
9.2 内部审核 7
9.3 管理评审 7
10 改进 8

10.1 持续改进 8
10.2 不符合与纠正措施 8
附 录 A （规范性） 信息安全控制参考 9
参 考 文 献 16

国际标准

ISO/IEC 27017:2015

第 1 版

2015-07

信息技术 安全技术

基于 ISO/IEC27002 的云服务信息安全控制的实施规范

索引号

ISO/IEC 27017:2015

目 录

前言 4
前言（ITU-T 相关） 4
引言 7
1 范围 8
2 规范性引用文件 8
3 术语和缩略语 9
4 云领域特定概念 10
4.1 概述 10
4.2 云服务中的供应商关系 11
4.3 云服务客户与云服务提供商之间的关系 12
4.4 云服务客户与云服务提供商的关系 12
4.5 云服务类型 13
5 信息安全方针 14
5.1 信息安全的管理指导 14
6 信息安全组织 16
6.1 内部组织 16
6.2 移动设备与远程办公 18
7 人力资源安全 19
7.1 雇佣前 19
7.2 雇佣期间 19
7.3 雇佣终止与变更 20
8 资产管理 20
8.1 资产责任 21
8.2 信息分类 22
8.3 介质处理 23
9 访问控制 23
9.1 访问控制的业务需求 23
9.2 用户访问管理 24
9.3 用户责任 27
9.4 系统与应用访问控制 27
10 密码术 29
10.1 密码控制 29
11 物理与环境安全 30
11.1 安全区域 30
11.2 设备安全 31
12 运行安全 33
12.1 运行程序与责任 33
12.2 恶意软件防护 35
12.3 备份 35
12.4 日志记录与监控 36
12.5 运行软件控制 39
12.6 技术漏洞管理 39
12.7 信息系统审计考量 39

13 通信安全 40
13.1 网络安全管理 40
13.2 信息传输 41
14 系统获取、开发与维护 42
14.1 信息系统的安全需求 42
14.2 开发与支持过程中的安全 43
14.3 测试数据 44
15 供应商关系 45
15.1 供应商关系中的信息安全 45
15.2 供应商服务交付管理 46
16 信息安全事件管理 47
16.1 信息安全事件管理与改进 47
17 业务连续性管理中的信息安全方面 49
17.1 信息安全连续性 49
17.2 冗余 50
18 合规性 50
18.1 遵守法律与合同要求 50
18.2 信息安全审查 53
附录 **A** 云服务扩展控制集 55
CLD.6.3 云服务客户与云服务提供商的关系 55
CLD.8.1 资产责任 56
CLD.9.5 共享虚拟环境中云服务客户数据的访问控制 56
CLD.12.1 运行程序与责任 58
CLD.12.4 日志记录与监控 59
CLD.13.1 网络安全管理 60
附录 **B** 与云计算相关的信息安全风险参考文件 62
参考书目 65