
安全技术 – 针对ISO/IEC27001和ISO/
IEC 27002 在隐私信息管理的扩展 -
要求和指南



内容	页
前言	vii
0 引言	viii
0.1 总则	viii
0.2 与其他管理体系的兼容性	viii
1 范围	1
2 规范性引用文献	1
3 术语，定义和缩写	1
3.1 联合PII控制者	1
3.2 隐私信息管理体系PIMS	2
4 总则	2
4.1 本标准的结构	2
4.2 ISO/IEC 27001:2013要求的应用	2
4.3 ISO/IEC 27002:2013指南的应用	3
4.4 顾客	4
5 与ISO/IEC 27001相关的PIMS特定要求	4
5.1 总则	4
5.2 组织环境	4
5.2.1 理解组织及其环境	4
5.2.2 理解相关方的需求和期望	5
5.2.3 确定信息安全管理体的范围	5
5.2.4 信息安全管理体系	5
5.3 领导	5
5.3.1 领导和承诺	5
5.3.2 方针	5
5.3.3 组织角色，职责和权限	5
5.4 规划	6

ISO/IEC	
5.4.1 应对风险和机会的措施	6
5.4.2 信息安全目标和实现规划	7
5.5 支持	7
5.5.1 资源	7
5.5.2 能力	7
5.5.3 意识	7
5.5.4 沟通	7
5.5.5 文件记录信息	7
5.6 运行	7
5.6.1 运行的规划和控制	7
5.7 绩效评价	8
5.7.1 监测，测量，分析和评价	8
5.7.2 内部审核	8
5.7.3 管理评审	8
5.8 改进	8
5.8.1 不符合和纠正措施	8
5.8.2 持续改进	8
6 与ISO/IEC 27002相关的PIMS特定指南	8
6.1 总则	8
6.2 信息安全策略	8
6.2.1 信息安全管理指导	8
6.3 信息安全组织	9
6.3.1 内部组织	9
6.3.2 移动设备和远程工作	10
6.4 人力资源安全	10
6.4.1 任用前	10
6.4.2 任用中	10
6.4.3 任用的终止和变更	10
6.5 资产管理	11
6.5.1 有关资产的责任	11
6.5.2 信息分级	11
6.5.3 介质处理	11

6.6	访问控制	12
6.6.1	访问控制的业务要求	12
6.6.2	用户访问管理	12
6.6.3	用户责任	13
6.6.4	系统和应用程序访问控制	13
6.7	密码	14
6.7.1	密码控制	14
6.8	物理和环境安全	14
6.8.1	安全区域	14
6.8.2	设备	15
6.9	运行安全	16
6.9.1	运行规程和责任	16
6.9.2	恶意软件防范	16
6.9.3	备份	16
6.9.4	日志和监视	17
6.9.5	运行软件的控制	18
6.9.6	技术脆弱性管理	18
6.9.7	信息系统审计的考虑	18
6.10	通信安全	18
6.10.1	网络安全管理	18
6.10.2	信息传输	18
6.11	系统的获取，开发和维护	19
6.11.1	信息系统的安全要求	19
6.11.2	开发和支持过程中的安全	19
6.11.3	测试数据	21
6.12	供应商关系	21
6.12.1	供应商关系中的信息安全	21
6.12.2	供应商服务交付管理	22
6.13	信息安全事件管理	22
6.13.1	信息安全事件的管理和改进	22
6.14	业务连续性管理的信息安全方面	24
6.14.1	信息安全连续性	24
6.15	符合性	24

ISO/IEC

6.15.1	符合法律和合同要求	24
6.15.2	信息安全评审	25
7	针对PII控制者的补充ISO/IEC 27002指南	26
7.1	总论	26
7.2	收集和处理的条件	26
7.2.1	识别并记录目的	26
7.2.2	确定法律依据	26
7.2.3	确定何时以及如何获得准许	27
7.2.4	获得并记录准许	27
7.2.5	隐私影响评估	28
7.2.6	与PII处理者的合同	28
7.2.7	联合PII控制者	28
7.2.8	与处理PII控制有关的记录	29
7.3	对PII主体的义务	29
7.3.1	确定并履行对PII主体的义务	29
7.3.2	确定提供给PII主体的信息	30
7.3.3	向PII主体提供信息	30
7.3.4	提供修改或撤销准许的机制	31
7.3.5	提供反对PII处理的机制	31
7.3.6	访问，更正和/或擦除	31
7.3.7	PII控制者告知第三方的义务	32
7.3.8	提供PII处理者的副本	32
7.3.9	处理请求	33
7.3.10	自动决策的制定	33
7.4	设计的隐私和默认的隐私	33
7.4.1	限制收集	33
7.4.2	限制处理	34
7.4.3	准确性和质量	34
7.4.4	PII最小化目标	34
7.4.5	PII在处理结束时去识别化和删除	35
7.4.6	临时文件	35
7.4.7	保留	35
7.4.8	处置	36
7.4.9	PII传输	36

7.5	PII共享，传输和披露	36
7.5.1	识别司法管辖区之间PII传输的基础	36
7.5.2	PII可以传输至的国家和国际组织	36
7.5.3	PII传输的记录	37
7.5.4	向第三方披露PII的记录	37
8	针对PII处理者的补充ISO/IEC 27002指南	37
8.1	总则	37
8.2	收集和处理的条件	37
8.2.1	客户协议	37
8.2.2	组织的目的	38
8.2.3	营销和广告使用	38
8.2.4	侵权指令	38
8.2.5	客户义务	39
8.2.6	与处理PII有关的记录	39
8.3	对于PII主体的义务	39
8.3.1	对于PII主体的义务	39
8.4	默认的隐私，设计的隐私	39
8.4.1	临时文件	40
8.4.2	退回，传输或处置PII	40
8.4.3	PII传输控制	40
8.5	PII共享，传输和披露	41
8.5.1	管辖区之间PII传输的基础	41
8.5.2	PII可以传输至的国家和国际组织	41
8.5.3	向第三方披露PII的记录	41
8.5.4	PII披露请求的通知	42
8.5.5	具有法律约束力的PII披露	42
8.5.6	处理PII的分包商的披露	42
8.5.7	分包商处理PII的参与	42
8.5.8	分包商处理PII的变更	43
附录A		44
附录B		48
附录C		51

ISO/IEC	
附录D.	53
附录E.	56
附录F.	59
F.1 如何应用本标准	59
F.2 安全标准的改进示例	59
参考书目	61

注：本文件内容受到版权保护，未经恰当的授权禁止复制。本公司客户及相关单位，如需获取文件完整内容，请联系市场部门获取，电话：010-84720998。