



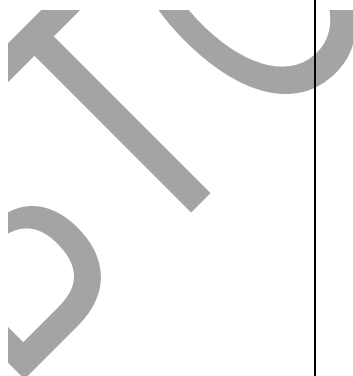
国际标准

ISO/IEC 27018

信息安全、网络安全和隐私保护
作为PII处理者在公有云中保护
个人可识别信息 (PII) 的指南

第三版

2025-08



目录

前言	vii
引言	viii
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
3.1 数据泄露 (data breach)	1
3.2 个人可识别信息 (personally identifiable information, PII)	1
3.3 个人可识别信息控制者 (PII controller)	2
3.4 个人可识别信息主体 (PII principal)	2
3.5 个人可识别信息处理者 (PII processor)	2
3.6 个人可识别信息处理 (PII processing)	2
3.7 公有云服务提供商 (public cloud service provider)	2
4 概述	2
4.1 本文件结构	2
4.2 控制措施框架	8
5 组织控制措施	9
5.1 信息安全政策	9
5.2 信息安全角色和职责	9
5.3 职责分离	9
5.4 管理职责	9
5.5 与主管部门的联系	9
5.6 与特殊利益群体的联系	9
5.7 威胁情报	10
5.8 项目管理中的信息安全	10
5.9 信息及其他相关资产清单	10
5.10 信息及其他相关资产的可接受使用	10
5.11 资产归还	10
5.12 信息分类	10
5.13 信息标记	10
5.14 信息传输	10
5.15 访问控制	10

5.16 身份管理	10
5.17 认证信息	11
5.18 访问权限	11
5.19 供应商关系中的信息安全	11
5.20 供应商协议中的信息安全条款	11
5.21 ICT 供应链中的信息安全管理	11
5.22 供应商服务的监控、审查和变更管理	11
5.23 云服务使用的信息安全	11
5.24 信息安全事件管理的规划和准备	11
5.25 信息安全事件的评估和决策	11
5.26 信息安全事件的响应	11
5.27 从信息安全事件中学习	11
5.28 证据收集	11
5.29 中断期间的信息安全	11
5.30 业务连续性的 ICT 准备度	12
5.31 法律、法规、监管及合同要求	12
5.32 知识产权	12
5.33 记录保护	12
5.34 隐私和个人可识别信息保护	12
5.35 信息安全的独立审查	12
5.36 信息安全政策、规则和标准的合规性	12
5.37 成文的操作程序	12
6 人员控制措施	12
6.1 背景审查	12
6.2 雇佣条款和条件	12
6.3 信息安全意识、教育和培训	12
6.4 纪律处分程序	13
6.5 雇佣终止或变更后的职责	13
6.6 保密或不披露协议	13
6.7 远程工作	13
6.8 信息安全事件报告	13
7 物理控制措施	13

7.1 物理安全边界	13
7.2 物理入口控制	13
7.3 办公场所、房间和设施的安全防护	13
7.4 物理安全监控	13
7.5 物理和环境威胁防护	13
7.6 安全区域内工作	13
7.7 桌面清理和屏幕清理	13
7.8 设备选址和防护	13
7.9 场外资产安全	14
7.10 存储介质	14
7.11 辅助设施	14
7.12 布线安全	14
7.13 设备维护	14
7.14 设备的安全处置或再利用	14
8 技术控制措施	14
8.1 用户终端设备	14
8.2 特权访问权限	14
8.3 信息访问限制	14
8.4 源代码访问	14
8.5 安全认证	14
8.6 容量管理	14
8.7 恶意软件防护	14
8.8 技术漏洞管理	15
8.9 配置管理	15
8.10 信息删除	15
8.11 数据脱敏	15
8.12 数据泄露防护	15
8.13 信息备份	15
8.14 信息处理设施的冗余	15
8.15 日志记录	15
8.16 监控活动	16
8.17 时钟同步	16

8.18 特权实用程序的使用	16
8.19 运行系统上的软件安装	16
8.20 网络安全	16
8.21 网络服务安全	16
8.22 网络隔离	16
8.23 网页过滤	16
8.24 加密技术的使用	16
8.25 安全开发生命周期	17
8.26 应用程序安全要求	17
8.27 安全系统架构和工程原则	17
8.28 安全编码	17
8.29 开发和验收阶段的安全测试	17
8.30 外包开发	17
8.31 开发、测试和生产环境的分离	17
8.32 变更管理	17
8.33 测试信息	17
8.34 审核测试期间的信息系统保护	17
附录 A 公有云个人可识别信息处理者的个人可识别信息保护扩展控制措施集	18
A.1 总则	18
A.2 同意与选择	18
A.2.1 配合个人可识别信息主体行使权利的义务	18
A.3 目的合法性与明确性	18
A.3.1 公有云个人可识别信息处理者的处理目的	18
A.3.2 公有云个人可识别信息处理者的商业使用	18
A.4 收集限制	19
A.5 数据最小化	19
A.5.1 临时文件的安全删除	19
A.6 使用、保留和披露限制	19
A.6.1 个人可识别信息披露通知	19
A.6.2 个人可识别信息披露记录	19
A.7 准确性和质量	19
A.8 公开性、透明度和通知	19

A.8.1 分包个人可识别信息处理的披露	19
A.9 个人参与和访问	20
A.10 问责制	20
A.10.1 涉及个人可识别信息 (PII) 的数据泄露通知	20
A.10.2 行政安全政策和指南的保留期限	21
A.10.3 个人可识别信息的返还、传输和处置	21
A.11 信息安全	21
A.11.1 保密或不披露协议	21
A.11.2 硬拷贝材料生成限制	21
A.11.3 数据恢复的控制和日志记录	22
A.11.4 离开场所的存储介质上的数据保护	22
A.11.5 未加密便携式存储介质和设备的使用	22
A.11.6 公共数据传输网络上传输的个人可识别信息加密	22
A.11.7 硬拷贝材料的安全处置	22
A.11.8 用户标识符 (ID) 的唯一使用	22
A.11.9 用户 ID 管理	22
A.11.10 授权用户记录	23
A.11.11 合同措施	23
A.11.12 分包的个人可识别信息处理	23
A.11.13 已使用数据存储空间上的数据访问控制	23
A.12 隐私合规	24
A.12.1 个人可识别信息的地理位置	24
A.12.2 个人可识别信息的目标传输地	24
附录 B 本文件与第一版 ISO/IEC 27018:2019 的对应关系	25
参考文献	29