

国际标准      **ISO/IEC 27018**

第二版  
**2019-01**

---

信息技术 安全技术 公有云中个人信息处理者保护个人信息的实践规范

查阅全文请联系北京海德国际认证有限公司  
联系电话：010-84905056，010-65817800  
邮箱地址：common@hicchina.com.cn

---

参考号  
ISO/IEC 27018:2019E  
O ISO/IEC 2019

前言	6
介绍	7
0.1 背景和语境	7
0.2 公有云计算服务的 PII 保护控制	8
0.3 PII 保护要求	8
0.4 在云计算环境中选择和实施控制	9
0.5 开发其他指南	9
0.6 生命周期注意事项	10
1 范围	11
2 引用标准	11
3 术语和定义	11
3.1 数据泄露 (data breach)	12
3.2 个人身份信息 PII (personally identifiable information PII)	12
3.3 PII 控制者 (PII controller)	12
3.4 PII 主体 (PII principal)	12
3.5 PII 处理者 (PII processor)	13
3.6 PII 的处理 (processing of PII)	13
3.7 公有云服务提供商 (public cloud service provider)	13
4 概述	13
4.1 本文件的结构	13
4.2 控制类别	14
5 信息安全策略	15
5.1 信息安全管理指导	15
5.1.1 信息安全策略	15
5.1.2 审查信息安全策略的评审	16
6 信息安全组织	16
6.1 内部组织	16
6.1.1 信息安全角色和职责	16
6.1.2 职责分离	16
6.1.3 与职能机构的联系	16
6.1.4 与特定相关方的联系	16
6.1.5 项目管理中的信息安全	16
6.2 移动设备和远程工作	17
7 人力资源安全	17
7.1 任用前	17
7.2 任用中	17
7.2.1 管理职责	17
7.2.2 信息安全意识、教育和培训	17
7.2.3 违纪处理过程	17
7.3 任用职责的终止或变更	18
8 资产管理	18

9 访问控制.....	18
9.1 访问控制的业务要求.....	18
9.2 用户访问管理.....	18
9.2.1 用户注册和注销.....	18
9.2.2 用户访问供给.....	18
9.2.3 特权访问权限管理.....	18
9.2.4 用户的秘密鉴别信息管理.....	19
9.2.5 用户访问权限的评审.....	19
9.2.6 访问权限的移出或调整.....	19
9.3 用户责任.....	19
9.3.1 秘密鉴别信息的使用.....	19
9.4 系统和应用访问控制.....	19
9.4.1 信息访问限制.....	19
9.4.2 安全的登录过程.....	19
9.4.3 口令管理系统.....	19
9.4.4 特权实用程序的使用.....	20
9.4.5 程序源代码的访问控制.....	20
10 密码.....	20
10.1 密码控制.....	20
10.1.1 密码控制的使用政策.....	20
10.1.2 密钥管理.....	20
11 物理和环境安全.....	20
11.1 安全区域.....	20
11.2 设备.....	20
11.2.1 设备安置和保护.....	20
11.2.2 支持行设施.....	21
11.2.3 布线安全.....	21
11.2.4 设备维护.....	21
11.2.5 资产的移动.....	21
11.2.6 组织场外设备和资产的安全.....	21
11.2.7 设备的安全处置或再利用.....	21
11.2.8 无人值守的用户设备.....	21
11.2.9 清空桌面和屏幕策略.....	21
12 运行安全.....	21
12.1 运行规程和责任.....	21
12.1.1 文件化的操作规程.....	21
12.1.2 变更管理.....	22
12.1.3 容量管理.....	22
12.1.4 开发，测试和运行环境分离.....	22
12.2 恶意软件防范.....	22
12.3 备份.....	22

12.3.1 信息备份 .....	22
12.4 日志和监视 .....	23
12.4.1 事态日志 .....	23
12.4.2 日志信息的保护 .....	23
12.4.3 管理员和操作员日志 .....	24
12.4.4 时钟同步 .....	24
12.5 运行系统的软件安装 .....	24
12.6 技术方面的脆弱性管理 .....	24
12.7 信息系统审计的考虑 .....	24
13 通讯安全 .....	24
13.1 网络安全管理 .....	24
13.2 信息传递 .....	24
13.2.1 信息传输策略和规程 .....	24
13.2.2 信息传输协议 .....	25
13.2.3 电子消息发送 .....	25
13.2.4 保密性或不泄露协议 .....	25
14 系统获取、开发和维护 .....	25
15 供应商关系 .....	25
16 信息安全事件管理 .....	25
16.1 信息安全事件的管理和改进 .....	25
16.1.1 责任和规程 .....	25
16.1.2 报告信息安全事态 .....	26
16.1.3 报告信息安全弱点 .....	26
16.1.4 信息安全事态的评估和决策 .....	26
16.1.5 信息安全事件的响应 .....	26
16.1.6 从信息安全事件中学习 .....	26
16.1.7 证据收集 .....	26
17 业务连续性管理的信息安全方面 .....	26
18 符合性 .....	26
18.1 符合法律和合同要求 .....	27
18.2 信息安全评审 .....	27
18.2.1 信息安全的独立评审 .....	27
18.2.2 符合安全策略和标准 .....	27
18.2.3 技术符合性评审 .....	27
附件 A .....	28
(规范性) .....	28
用于 PII 保护的公有云 PII 处理者扩展控制集 .....	28
A.1 总则 .....	28
A.2 同意和选择 .....	28
A.2.1 在 PII 主体的权利方面进行合作的义务 .....	28
A.3 目的合法性和规范 .....	28

A.3.1 公有云 PII 处理者的目的 .....	28
A.3.2 公有云 PII 处理者的商用 .....	29
A.4 收集限制.....	29
A.5 数据最小化 .....	29
A.5.1 安全擦除临时文件.....	29
A.6 使用，保留和披露限制.....	30
A.6.1 PII 披露通知 .....	30
A.6.2 PII 披露的记录 .....	30
A.7 准确性和质量 .....	30
A.8 公开，透明和通知 .....	30
A.8.1 分包 PII 处理的披露.....	30
A.9 个体参与和访问 .....	31
A.10 问责制.....	31
A.10.1 涉及 PII 的数据泄露的通知 .....	31
A.10.2 行政安全策略和指导方针的保留期 .....	32
A.10.3 PII 的的归还、转移和处置.....	32
A.11 信息安全.....	32
A.11.1 保密或不泄露协议 .....	32
A.11.2 创建硬拷贝材料的限制 .....	33
A.11.3 数据恢复的控制和记录.....	33
A.11.4 保护离开场所的存储介质上的数据 .....	33
A.11.5 未加密的便携式存储介质和设备的使用.....	33
A.11.6 通过公共数据传输网络传输的 PII 的加密.....	33
A.11.7 硬拷贝材料的安全处置.....	34
A.11.8 用户 ID 的唯一使用 .....	34
A.11.9 授权用户记录.....	34
A.11.10 用户 ID 管理.....	34
A.11.11 合同措施.....	34
A.11.12 分包 PII 处理 .....	35
A.11.13 用过的的数据存储空间的数据访问 .....	35
A.12 隐私合规性 .....	36
A.12.1 PII 的地理位置.....	36
A.12.2 PII 的预期目的地.....	36