ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 41574—2022

信息技术　安全技术
公有云中个人信息保护实践指南

Information technology—Security techniques—Code of practice for protection of personal information in public clouds

（ISO/IEC 27018:2019，Information technology—Security techniques—Code of practice for protection of personally identifiable information（PII）in public clouds acting as PII processors，MOD）

2022-07-11 发布　　2023-02-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅴ
引言 …… Ⅶ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　概述 …… 2
4.1　本文件的结构 …… 2
4.2　控制类别 …… 3
5　信息安全策略 …… 3
5.1　信息安全管理指导 …… 3
5.1.1　信息安全策略 …… 3
5.1.2　信息安全策略的评审 …… 4
6　信息安全组织 …… 4
6.1　内部组织 …… 4
6.1.1　信息安全的角色和责任 …… 4
6.1.2　职责分离 …… 4
6.1.3　与职能机构的联系 …… 4
6.1.4　与特定相关方的联系 …… 4
6.1.5　项目管理中的信息安全 …… 4
6.2　移动设备和远程工作 …… 4
7　人力资源安全 …… 4
7.1　任用前 …… 4
7.2　任用中 …… 5
7.2.1　管理责任 …… 5
7.2.2　信息安全意识、教育和培训 …… 5
7.2.3　违规处理过程 …… 5
7.3　任用的终止和变更 …… 5
8　资产管理 …… 5
9　访问控制 …… 5
9.1　访问控制的业务要求 …… 5
9.2　用户访问管理 …… 5
9.2.1　用户注册和注销 …… 6
9.2.2　用户访问供给 …… 6
9.2.3　特许访问权管理 …… 6
9.2.4　用户的秘密鉴别信息管理 …… 6
9.2.5　用户访问权的评审 …… 6

9.2.6 访问权的移除或调整 …… 6
9.3 用户责任 …… 6
9.3.1 秘密鉴别信息的使用 …… 6
9.4 系统和应用访问控制 …… 6
9.4.1 信息访问限制 …… 6
9.4.2 安全登录规程 …… 6
9.4.3 口令管理系统 …… 6
9.4.4 特权实用程序的使用 …… 7
9.4.5 程序源代码的访问控制 …… 7
10 密码 …… 7
10.1 密码控制 …… 7
10.1.1 密码控制的使用策略 …… 7
10.1.2 密钥管理 …… 7
11 物理和环境安全 …… 7
11.1 安全区域 …… 7
11.2 设备 …… 7
11.2.1 设备安置和保护 …… 7
11.2.2 支持性设施 …… 7
11.2.3 布缆安全 …… 7
11.2.4 设备维护 …… 8
11.2.5 资产的移动 …… 8
11.2.6 组织场所外的设备与资产安全 …… 8
11.2.7 设备的安全处置或再利用 …… 8
11.2.8 无人值守的用户设备 …… 8
11.2.9 清理桌面和屏幕策略 …… 8
12 运行安全 …… 8
12.1 运行规程和责任 …… 8
12.1.1 文件化的操作规程 …… 8
12.1.2 变更管理 …… 8
12.1.3 容量管理 …… 8
12.1.4 开发、测试和运行环境的分离 …… 8
12.2 恶意软件防范 …… 9
12.3 备份 …… 9
12.3.1 信息备份 …… 9
12.4 日志和监视 …… 9
12.4.1 事态日志 …… 9
12.4.2 日志信息的保护 …… 9
12.4.3 管理员和操作员日志 …… 10
12.4.4 时钟同步 …… 10
12.5 运行软件控制 …… 10
12.6 技术方面的脆弱性管理 …… 10
12.7 信息系统审计的考虑 …… 10

13 通信安全 …… 10
13.1 网络安全管理 …… 10
13.2 信息传输 …… 10
13.2.1 信息传输策略和规程 …… 10
13.2.2 信息传输协议 …… 10
13.2.3 电子消息发送 …… 10
13.2.4 保密或不披露协议 …… 10
14 系统获取、开发和维护 …… 11
15 供应商关系 …… 11
16 信息安全事件管理 …… 11
16.1 信息安全事件的管理和改进 …… 11
16.1.1 责任和规程 …… 11
16.1.2 报告信息安全事态 …… 11
16.1.3 报告信息安全弱点 …… 11
16.1.4 信息安全事态的评估和决策 …… 11
16.1.5 信息安全事件的响应 …… 11
16.1.6 从信息安全事件中学习 …… 11
16.1.7 证据的收集 …… 12
17 业务连续性管理的信息安全方面 …… 12
18 符合性 …… 12
18.1 符合法律和合同要求 …… 12
18.2 信息安全评审 …… 12
18.2.1 信息安全独立评审 …… 12
18.2.2 符合安全策略和标准 …… 12
18.2.3 技术符合性评审 …… 12
附录 A（资料性） 本文件与 ISO/IEC 27018:2019 结构编号对照情况 …… 13
附录 B（规范性） 公有云个人信息处理者保护个人信息的扩展控制措施集 …… 15
附录 C（资料性） 云服务提供者、云服务客户和云服务用户的关系 …… 21
参考文献 …… 22

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件修改采用ISO/IEC 27018:2019《信息技术　安全技术　个人可识别信息(PII)处理者在公有云中保护PII的实践指南》。

本文件与ISO/IEC 27018:2019相比，在结构上有较多调整。两个文件之间的结构编号变化对照一览表见附录A。

本文件与ISO/IEC 27018:2019的技术差异及其原因如下：

——将术语“个人可识别信息(PII)”更改为“个人信息”，并更改了定义，与GB/T 35273—2020的术语和定义保持一致(见3.1，ISO/IEC 27018:2019的3.2)；

——将术语“PII控制者”更改为“个人信息控制者”，并更改了定义，与GB/T 35273—2020的术语和定义保持一致(见3.2，ISO/IEC 27018:2019的3.3)；

——将术语“PII主体”更改为“个人信息主体”，并更改了定义，与GB/T 35273—2020的术语和定义保持一致(见3.3，ISO/IEC 27018:2019的3.4)；

——将术语“PII处理者”更改为“个人信息处理者”，并更改了定义，与GB/T 35273—2020的术语和定义保持一致(见3.4，ISO/IEC 27018:2019的3.5)；

——将术语“PII处理”更改为“个人信息处理”，并更改了定义，与GB/T 35273—2020的术语和定义保持一致(见3.5，ISO/IEC 27018:2019的3.6)；

——将表题中的ISO/IEC 27002更改为GB/T 22081(见表1，ISO/IEC 27018:2019的表1)；

——增加处理者委托分包商处理个人信息的建议，与GB/T 35273—2020中9.1 c) 2)关于受委托者的要求保持一致(见5.1.1)；

——删除“公有云PII保护其他信息”中法律法规对处理者和控制者不同要求的表述，以符合我国标准化文件的起草规则(见ISO/IEC 27018:2019的5.1.1)；

——删除“公有云PII保护其他信息”中法律法规对处理者处罚的要求，以符合我国标准化文件的起草规则(见ISO/IEC 27018:2019的7.2.2)；

——增加采用密码技术解决机密性、完整性、真实性、不可否认性需求的要求(见10.1.1)；

——增加处理者转让个人信息的建议，与GB/T 35273—2020的相关条款保持一致(见B.2.3)；

——增加处理者向境外提供个人信息的建议，以适应我国的技术条件，便于本文件的应用(见B.4.1、B.7.14)；

——增加处理者委托代理商处理个人信息的建议，与GB/T 35273—2020中9.1 c) 2)关于受委托者的要求保持一致(见B.7.1)；

——增加数据恢复日志包含信息的建议(见B.7.3)；

——删除“公有云PII保护实现指南”中关于处理者告知义务的相关法律表述，以符合我国标准化文件的起草规则(见ISO/IEC 27018:2019的A.10.1)。

本文件做了下列编辑性改动：

——为与现有标准系列一致，将标准名称更改为《信息技术　安全技术　公有云中个人信息保护实践指南》；

——更改附录B中新增控制措施的分类原则，与我国的个人信息保护原则保持一致(见B.1，ISO/IEC 27018:2019的A.1)；

——增加对“脱链”的解释说明，以提高条款的易读性，便于本文件的应用（见 B.2.3 注 1）；
——增加对“消磁”的解释说明，以提高条款的易读性，便于本文件的应用（见 B.2.3 注 2）；
——增加附录 A（资料性）“本文件与 ISO/IEC 27018:2019 结构编号对照情况”；
——增加附录 C（资料性）“云服务提供者、云服务客户和云服务用户的关系”；
——删除 ISO/IEC 27018:2019 的 9.2.1 注；
——删除 ISO/IEC 27018:2019 的 10.1.1 注；
——删除 ISO/IEC 27018:2019 的 12.3.1 注 1 和注 2；
——删除 ISO/IEC 27018:2019 的 A.6.1 示例；
——删除 ISO/IEC 27018:2019 的 A.11.3 注的第 1 句；
——将本项控制措施和指南可归入的其他原则改为“公开透明”原则，与我国的个人信息保护原则保持一致（见 B.2.3 注 3，ISO/IEC 27018:2019 的 A.10.3 注）；
——更改“公有云 PII 保护实现指南”中涉及 PII 收集和使用所遵循原则的表述，与我国的个人信息保护原则保持一致（见 B.3.1，ISO/IEC 27018:2019 的 A.3.1）；
——更改“公有云 PII 保护实现指南”中的“PII 控制者”为“云服务客户”，以提高易读性，便于本文件的应用（见 B.8.1，ISO/IEC 27018:2019 的 A.2.1）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）归口。

本文件起草单位：山东省标准化研究院、杭州拓深科技有限公司、中国网络安全审查技术与认证中心、陕西省网络与信息安全测评中心、艺龙网信息技术（北京）有限公司、中电长城网际系统应用有限公司、北京钱袋宝支付技术有限公司、国家工业信息安全发展研究中心、腾讯云计算（北京）有限责任公司、陕西省信息化工程研究院、中电数据服务有限公司、上海市信息安全行业协会、上海安言信息技术有限公司、安徽省电子产品监督检验所、山东中测信息技术有限公司。

本文件主要起草人：王庆升、尤其、党斌、闵京华、兰安娜、柳彩云、王永霞、张勇、张博、周亚超、孙岩、张轩铭、靳倩、王利强、赵首花、王爱义、杨帆、石磊、黄磊、王理冬、赵倩倩、马卓元、贾梦妮、闫育芸、秦峰、杨向东、王法中、许立前、范正翔、于秀彦、刘勘伪、吴博。

引　言

0.1　背景和环境

近年，越来越多的云服务客户使用云服务提供者的服务，委托其进行个人信息处理。GB/T 35273—2020 中规定了对接受委托处理一方(GB/T 35273—2020 中 9.1 称为“受委托者”，本文件中的“处理者”即“受委托者”)的要求。本文件按照 GB/T 35273—2020 对处理者的要求，提供了一种在公有云中保护个人信息的通用合规框架，指导处理者开展公有云中个人信息处理操作。

公有云服务提供者通常需要依据与云服务客户签订的合同，并在双方均遵守个人信息保护法律法规相关要求的前提下开展服务。对于个人信息保护的这些要求，云服务提供者与云服务客户是依据法律法规和它们之间的合同来确定的。

当公有云服务提供者按照云服务客户的要求处理个人信息时，公有云服务提供者充当“个人信息处理者”的角色。与公有云个人信息处理者有合同关系的云服务客户是“个人信息控制者”。在云计算环境下，个人信息控制者掌握个人信息的控制权，其也具有处理和使用个人信息的权限。个人信息控制者与个人信息处理者均可处理个人信息，但个人信息处理者作为受委托的一方，只能执行个人信息控制者要求的个人信息处理操作和为实现个人信息控制者目标而进行的必要操作。同时，云服务客户也可授权一个或多个云服务用户使用其服务，但这些服务仅限于云服务客户与公有云个人信息处理者签订合同中约定的可用服务。

本文件旨在创建一组通用的控制类别和控制措施，与 GB/T 22081 中的信息安全控制目标和控制措施结合使用，由个人信息处理者来实现。本文件的目的如下：

——帮助公有云个人信息处理者履行相应义务，这些义务包括法律法规规定的直接义务及合同约定的其他义务；

——使公有云个人信息处理者在相关事务上保持透明，便于云服务客户选择管理良好的基于云的个人信息处理服务；

——协助云服务客户和公有云个人信息处理者签订合同协议；

——在单个云服务客户无法对托管在多方或虚拟化服务器(云)中的数据进行审计，或者此类审计可能增加现有物理和逻辑网络安全控制风险的情况下，为云服务客户行使审计权力和承担符合性责任提供一种机制。

本文件可为公有云服务提供者，特别是跨国运营的公有云服务提供者，提供一种通用的合规框架。

0.2　公有云计算服务的个人信息保护控制

在基于 GB/T 22080 实施云计算信息安全管理体系的过程中，公有云个人信息处理者可参考本文件选择个人信息保护控制措施。本文件也可作为公有云个人信息处理者实施通用的个人信息保护控制措施的指导文件。尤其是，本文件在 GB/T 22081 的基础上，考虑了个人信息处理者所面临的特定风险环境。

通常来说，组织实施 GB/T 22080 是为了保护自身的信息资产。然而，公有云个人信息处理者保护的个人信息，实际上是云服务客户的信息资产。因此，由公有云个人信息处理者实施 GB/T 22081 中的

控制措施是合理的，也是必要的。同时，为适应公有云计算环境中风险分散的特点，并符合云服务客户与公有云个人信息处理者之间的合同要求，本文件增强了 GB/T 22081 中的控制措施。本文件通过以下 2 种方式增强了 GB/T 22081：

——为 GB/T 22081 中的某些控制措施提供了适用于公有云个人信息保护的实现指南；

——附录 B 提供了一组新的控制措施和相关指南，以解决 GB/T 22081 中的控制措施集未能满足的公有云个人信息保护要求。

0.3 个人信息保护要求

组织确定其对个人信息的保护要求。这些要求有以下 3 个主要来源。

a) 法律、法规、监管和合同要求：一个来源是组织及其贸易伙伴、承包商和服务商满足的法律、法规、监管和合同要求或义务，以及社会文化责任和运营环境要求。需要注意的是，法律、法规和合同可能强制要求个人信息处理者选择特定的控制措施，也可能要求其制定具体的准则来实现这些控制措施。

b) 风险：另一个来源是，考虑组织整体业务战略和目标的基础上，组织对个人信息相关的评估风险。组织通过风险评估识别威胁、评估脆弱性和发生的可能性、估计潜在影响。GB/T 31722 提供了信息安全风险管理指南，包括风险评估、风险接受、风险沟通、风险监视和风险审查的建议。ISO/IEC 29134 提供了有关隐私影响评估的指南。

c) 组织政策：尽管组织政策涵盖了来自法律和社会文化的诸多义务，但组织仍可自愿选择超出 a)的要求。

0.4 云计算环境下控制措施的选择和实现

组织可能从本文件中选择控制措施（包括引用的 GB/T 22081 中的控制措施，以及面向具体应用创建的组合参考控制措施集）。若需要，组织还可能从其他控制措施集中选择控制措施，或者设计新的控制措施以满足特定要求。

控制措施的选择取决于组织的决策。这些决策是基于风险接受程度、风险处理方案，以及适用于组织与其有合同关系的客户、供应商的一般风险管理方法作出的。控制措施的选择还受国内外法律法规的约束。若未选择本文件中的控制措施，则需说明并记录未选择的理由。

此外，控制措施的选择和实现还取决于组织在整个云计算参考架构中的实际角色（见 GB/T 32399）。在云计算环境中，可能存在多个组织参与提供基础设施服务和应用服务的情况。在某些情况下，所选控制措施对于云计算参考架构中的特定服务类别来说可能是唯一的。而在其他情况下，实现安全控制措施可能共享角色。合同协议需要规定提供或使用云服务的所有组织承担的个人信息保护责任。这些组织包括公有云个人信息处理者及其分包商、云服务客户。

本文件中的控制措施可视为一种指导原则，适用于大多数组织。下文将给出这些控制措施的详细说明和实现指南。若公有云个人信息处理者在设计信息系统、服务和操作的过程中预先考虑了保护个人信息的要求，那么这些控制措施的实现将会更加简单。这是“隐私设计”（参见参考文献[9]）的一部分。

0.5 制定额外指南

本文件可看作开发个人信息保护指南的起点。对于保护个人信息而言，本文件中的控制措施和实现指南可能并非都是适用的，并且可能还需要本文件未包含的额外控制措施和实现指南。在开发包含

额外控制措施或指南的文件时，交叉引用本文件中的适用条款可有助于审计人员和业务合作伙伴进行合规性检查。

0.6 生命周期的考虑

个人信息有其固有的生命周期，即从创建和生成，经过存储、处理、使用、传输到最终销毁或消失。个人信息在生命周期中面临不同的风险，但在生命周期的各个阶段保护个人信息仍很重要。

个人信息保护需结合现有的和新的信息系统进行考虑，并进行全生命周期管理。

信息技术　安全技术
公有云中个人信息保护实践指南

1　范围

本文件给出了在公有云中实施个人信息保护的控制目标和控制措施，在 GB/T 22081 基础上给出了公有云个人信息保护指南。

本文件适用于作为个人信息处理者的所有类型和规模的组织，包括公有和私营公司、政府机构和非营利组织。

本文件也可能适用于作为个人信息控制者的组织。但是，个人信息控制者可能还受额外的个人信息保护法律法规和义务的约束，而这些法律法规和义务不适用于个人信息处理者。本文件不涵盖此类额外义务。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22081—2016　信息技术　安全技术　信息安全控制实践指南（ISO/IEC 27002:2013，IDT）

GB/T 29246　信息技术　安全技术　信息安全管理体系　概述和词汇（GB/T 29246—2017，ISO/IEC 27000:2016，IDT）

GB/T 32400　信息技术　云计算　概览与词汇（GB/T 32400—2015，ISO/IEC 17788:2014，IDT）

GB/T 35273—2020　信息安全技术　个人信息安全规范

3　术语和定义

GB/T 29246 和 GB/T 32400 界定的以及下列术语和定义适用于本文件。

3.1

个人信息　personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注 1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注 2：关于个人信息的判定方法和类型参见 GB/T 35273—2020 中附录 A。

注 3：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如，用户画像或特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，属于个人信息。

［来源：GB/T 35273—2020，3.1］。

3.2

个人信息控制者　personal information controller

有能力决定个人信息处理目的、方式等的组织或个人。

［来源：GB/T 35273—2020，3.4］。