国际标准

ISO/IEC 27018

第三版 2025-08

# 信息安全、网络安全与隐私保护——作为 PII 处理方的公共云中个人可识别信息（PII）保护指南

*信息安全、网络安全与隐私保护——隐私保护指南*
*在公共云信息技术中作为 PII 处理器运行的可识别个人身份信息（PII）*



参考编号
ISO/IEC 27018:2025（中文翻译版）© ISO/IEC 2025
ISO/IEC 2025

ISO/IEC 27018:2025（中文翻译版）©

## 版权所有文档



国际版权局
CP 401 • 布兰东内街 8 号
CH-1214 维尼耶，日内瓦
电话：+41 22 749 01 11
电子邮件：
copyright@iso.org 网站：
www.iso.org

在瑞士出版

# Contents （目录）

Page

# 前言

国际标准化组织（ISO）与国际电工委员会（IEC）共同构建了全球标准化的专业体系。作为 ISO 或 IEC 成员的各国机构，通过各自组织设立的技术委员会参与国际标准制定工作，这些委员会专门负责特定技术领域的标准化事务。ISO 与 IEC 技术委员会在共同关注的领域开展协作。此外，其他国际组织（包括政府机构和非政府组织）在与 ISO 及 IEC 保持联络后，也会参与相关标准化工作。

本文件编制所采用的程序及其后续维护方案详见 ISO/IEC 指令第 1 部分。需特别注意不同类型文件所需的差异化审批标准。本文件依据 ISO/IEC 指令第 2 部分的编辑规范起草（参见 www.iso.org/directives 或 www.iec.ch/members_experts/refdocs）。

ISO 与 IEC 特别指出，本文件的实施可能涉及(a)专利技术的应用。对于相关专利权利的有效性、证据支持度及适用性，ISO 与 IEC 均不持任何立场。截至本文件发布时，ISO 与 IEC 尚未收到实施本文件可能需要(a)专利技术的相关通知。但需提醒实施方注意，这些信息可能并非最新动态，建议通过 www.iso.org/patents 及 https://patents.iec.ch 提供的专利数据库获取最新资料。ISO 与 IEC 不对识别任何或全部此类专利权利承担法律责任。

本文件中使用的任何商品名称仅为方便用户而提供，不构成任何背书。

关于标准的自愿性说明、ISO 特定术语及与合格评定相关的表述含义，以及 ISO 对世界贸易组织（WTO）《技术性贸易壁垒（TBT）》原则的遵循情况，请参阅 www.iso.org/iso/foreword.html。有关 IEC 的信息，请参阅 www.iec.ch/understanding-standards。

本文件由 ISO/IEC 联合技术委员会 JTC 1 信息技术分委会 SC27 信息安全、网络安全与隐私保护分组委员会编制。

第三版废止并取代了技术性修订后的第二版（ISO/IEC 27018:2019）。

主要变化如下：

— 文本已按照 ISO/IEC 27002:2022 标准进行对齐；

— 已添加附录 B。

如对本文件有任何反馈意见或疑问，请联系用户所在国家的标准机构。完整标准机构名录可查阅 www.iso.org/members.html 及 www.iec.ch/national-committees。

# 引言

## 0.1 背景与背景信息

根据合同条款处理个人身份信息（PII）的云服务提供商，应当以符合相关法律法规要求的方式运营服务，确保双方共同满足 PII 保护规范。具体要求及其在云服务提供商与客户之间的责任划分，会因司法管辖区不同以及合同条款差异而有所区别。规范 PII 处理方式（包括收集、使用、传输及处置）的法律法规通常被称为数据保护法规，其中 PII 也常被称为个人数据或个人信息。由于各司法管辖区对 PII 处理者的义务要求存在差异，这给提供云计算服务的企业在跨国运营时带来了诸多挑战。

当公共云服务提供商根据云服务客户的指令处理 PII 时，其本质属于“ PII 处理方”。与公共云 PII 处理方存在合同关系的云服务客户，其身份范围涵盖自然人（即“ PII 主体”，在云端处理自身 PII）至组织机构（即“ PII 控制方”，处理涉及多个 PII 主体的 PII）。云服务客户可授权与其关联的一个或多个云服务用户使用根据合同向其开放的服务。云服务客户对数据处理及使用行为拥有自主权。若云服务客户同时担任 PII 控制方，则需遵守比公共云 PII 处理方更为严格的 PII 保护义务。维持 PII 控制方与 PII 处理方的区分，关键在于公共云 PII 处理方除需处理客户指定的 PII 外，不得设立其他数据处理目标，且其运营活动必须严格服务于实现客户既定目标。

注 1：当公共云 PII 处理器处理云服务客户账户数据时，可作为 PII 控制器使用。本文件不涵盖此类活动。 注 1：当公共云 PII 处理器处理云服务客户账户数据时，可作为 PII 控制器使用。本文件不涵盖此类活动。

本文件旨在与 ISO/IEC27002 中的信息安全目标及控制措施结合使用，以建立一套通用的安全类别与控制措施，供作为 PII 处理方的公共云计算服务提供商实施。本文件具有以下目标：

—使公共云 PII 处理器在相关事务中保持透明化运作，从而让云服务客户能够选择治理完善的基于云的 PII 处理服务；

—协助云服务客户及公共云 PII 处理方签订合同协议；

— 为云服务客户提供审计与合规权责行使机制：当客户数据托管于多方虚拟化服务器（云）环境时，若采用传统审计方式存在技术可行性不足，且可能加剧现有物理与逻辑网络安全防护措施的风险，则需建立该机制。

注 2 公共云服务提供商在担任 PII 处理方时，应遵守相关义务。 注 2 公共云服务提供商在担任 PII 处理方时，应遵守相关义务。

本文件旨在为公共云服务提供商（特别是跨国市场运营者）提供统一的合规框架，从而提供有效支持。

## 0.2 公共云计算服务的 PII 防护控制措施

本文件旨在为组织机构提供参考依据，用于在实施基于 ISO/IEC 27001 标准的云计算信息安全管理体系过程中选择 PII 防护控制措施，或作为公共云 PII 处理机构实施通用 PII 防护控制措施的指导文件。特别需要说明的是，本文件以 ISO/IEC 27002 标准为基础，同时充分考虑了公共云计算服务提供商作为 PII 处理机构时可能面临的特定风险环境，这些风险环境源于相关 PII 防护要求。
在公共云服务提供商作为 PII 处理方的 PII 保护要求框架下，企业需对其客户委托的信息资产实施保护。公共云 PII 处理方采用 ISO/IEC 27002 标准控制措施，既符合该保护需求，又具有必要性。本文

件通过以下两种方式扩展 ISO/IEC 27002 标准控制措施：一是针对风险分布特性进行调整；二是考虑云服务客户与公共云 PII 处理方之间存在的合同关系。具体而言，本文件通过以下方式对 ISO/IEC 27002 标准进行扩展：

—适用于公共云 PII 保护的实施指南，涵盖部分现行 ISO/IEC 27002 控制措施

—附录 A 中包含的附加控制措施及相关指南，旨在满足现有 ISO/IEC 27002 控制措施未涵盖的公共云 PII 保护要求，其组织结构遵循 ISO/IEC 29100 的隐私原则。

本文件中的大部分控制措施和指南同样适用于 PII 控制器。然而，在多数情况下， PII 控制器还需履行本文未明确规定的额外义务。

### 0.3 PII 保护要求

组织必须明确其对 PII 保护的需求。需求主要来源于以下三个方面。

a) 法律与合同要求：其一来源是组织机构、贸易伙伴、承包商及服务提供商所须遵守的法律与合同要求，以及涉及其社会文化背景和运营环境的相关责任。需注意的是， PII 处理方制定的法律法规及合同承诺可能强制要求采用特定控制措施，并规定实施这些控制措施的具体标准。此类要求在不同司法管辖区可能存在差异。 a) 法律与合同要求：其一来源是组织机构、贸易伙伴、承包商及服务提供商所须遵守的法律与合同要求，以及涉及其社会文化背景和运营环境的相关责任。需注意的是， PII 处理方制定的法律法规及合同承诺可能强制要求采用特定控制措施，并规定实施这些控制措施的具体标准。此类要求在不同司法管辖区可能存在差异。

b)风险评估：另一来源是通过评估与 PII 相关的组织风险，同时结合组织的整体业务战略与目标。通过风险评估，可识别风险、评估其后果与发生概率，并对风险进行量化分析。ISO/IEC 27005 标准提供了信息安全风险管理指南，涵盖风险评估、风险接受、风险沟通、风险监控及风险评审等建议。ISO/IEC 29134 标准则制定了隐私影响评估指南。 b)风险评估：另一来源是通过评估与 PII 相关的组织风险，同时结合组织的整体业务战略与目标。通过风险评估，可识别风险、评估其后果与发生概率，并对风险进行量化分析。ISO/IEC 27005 标准提供了信息安全风险管理指南，涵盖风险评估、风险接受、风险沟通、风险监控及风险评审等建议。ISO/IEC 29134 标准则制定了隐私影响评估指南。

c) 企业政策：尽管企业政策涵盖的诸多内容源自法律及社会文化要求，但组织亦可自主选择突破基于 a)项要求所确立的标准。 c) 企业政策：尽管企业政策涵盖的诸多内容源自法律及社会文化要求，但组织亦可自主选择突破基于 a)项要求所确立的标准。

### 0.4 云计算环境中的控制措施选择与实施

可从本文件中选取控制措施（该文件通过引用方式整合了 ISO/IEC 27002 标准中的控制措施，为相关行业或应用场景构建了统一的参考控制集）。必要时，亦可从其他控制集选取措施，或根据具体需求设计新控制措施。

注 A：公共云 PII 处理器提供的 PII 处理服务可视为云计算的应用实例，而非独立行业领域。尽管如此，本文档仍采用“公共云服务提供商专属”这一术语，因其为 ISO/IEC JTC 1/SC27 制定的其他信息安全管理体系标准中惯用表述。 注 A：公共云 PII 处理器提供的 PII 处理服务可视为云计算的应用实例，而非独立行业领域。

尽管如此，本文档仍采用“公共云服务提供商专属”这一术语，因其为 ISO/IEC JTC 1/SC27 制定的其他信息安全管理体系标准中惯用表述。

控制措施的选择需依据组织决策制定，具体考量风险接受标准、风险处理方案以及组织整体风险管理策略，并通过合同协议与客户及供应商达成一致。同时须符合相关国家及国际法规要求。若组织或公有云服务商未采用本文件规定的控制措施，应提供充分论证依据。

此外，控制措施的选择与实施需根据公共云服务商在整个云计算参考架构中的实际角色来确定（参见 ISO/IEC 22123-3 标准）。在云计算环境中，可能有多个不同组织参与基础设施与应用服务的提供。在某些情况下，所选控制措施可能仅适用于特定服务类别。

云计算参考架构。在其他情况下，安全控制措施的实施可能涉及共享职责。合同协议应明确规定所有参与提供或使用云服务的组织的 PII 保护责任，包括公共云 PII 服务提供商、其分包商及云服务客户。

本文件中的控制措施可视为指导原则，适用于大多数组织。本文档中详细阐述了这些原则并附有实施指南。若在公共云 PII 处理器的信息系统、服务及运营设计阶段就已考虑 PII 保护要求，则可简化实施过程。这种考量属于常被称为‘隐私即设计’（参见参考文献[64]和[65]）的核心理念要素。

### 0.5 制定额外指南

本文件可作为制定 PII 保护指南的起点。本实践准则中的控制措施与指导原则并非全部适用，且可能需要补充未收录的其他控制措施与指导原则。在制定包含新增指导原则或控制措施的文件时，若适用可添加与本文件条款的交叉引用，以便审计师及业务合作伙伴进行合规性核查。

### 0.6 生命周期考量因素

PII 具有自然生命周期，从创建与起源开始，经过存储、处理、使用和传输，直至最终销毁或废弃。PII 在生命周期中面临的风险可能各不相同，但各阶段对 PII 的保护仍至关重要。

在现有及新信息系统生命周期管理过程中，预计将考虑 PII 防护要求。

# 信息安全、网络安全与隐私保护——作为 PII 处理方的公共云中个人可识别信息（PII）保护指南

## 1 范围

本文件确立了通用控制目标、控制措施及实施指南，旨在根据 ISO/IEC29100 标准的隐私原则，为公共云计算环境中的个人身份信息（PII）保护措施提供实施依据。

具体而言，本文件基于 ISO/IEC 27002:2022 标准制定指南，同时考虑了公共云服务提供商在信息安全风险环境中可能适用的 PII 保护监管要求。

本文件适用于各类规模的组织机构，包括上市公司、私营企业、政府机构及非营利组织，这些机构通过云计算技术以 PII 处理方身份，根据合同向其他组织提供信息处理服务。

本文件中的指南同样适用于担任 PII 控制者的组织机构。

## 2 规范性引用文件

本文档中引用的下列文件，其部分内容或全部内容均构成本文件的要求。对于标注日期的引用文件，仅引用的版本具有法律效力；对于未标注日期的引用文件，则以所引用文件的最新版本（包括任何修订内容）为准。

*ISO/IEC 27000，信息技术——安全技术——信息安全管理系统——概述与术语*

*ISO/IEC 27002:2022《信息安全、网络安全与隐私保护——信息安全控制措施》*

*ISO/IEC 22123-1 信息技术——云计算 第 1 部分：术语*

## 3 术语与定义

就本文件而言，适用 ISO/IEC 22123-1、ISO/IEC 27000、ISO/IEC 27002 中给出的术语及定义，以及以下内容。

ISO 与 IEC 维护术语数据库，用于标准化工作，具体地址如下：

- ISO 在线浏览平台：网址为 https://www.iso.org/obp

— IEC Electropedia：访问地址 https://www.electropedia.org/

**3.1**
**数据泄露**
导致传输、存储或以其他方式处理的受保护数据发生意外或非法破坏、丢失、篡改、未经授权披露或访问的安全漏洞
[来源：ISO/IEC 27040:2024,3.5.2]

**3.2**
**个人身份信息 PII**
信息满足以下任一条件：a) 可用于建立该信息与相关信息所涉及自然人之间的关联；或 b) 已经或能够直接或间接与某自然人相关联

条目注释 1：定义中的“自然人”指 PII 主体（3.4）。判断 PII 主体是否可识别时，需综合考虑数据持有方（隐私利益相关方）或其他任何主体为建立 PII 集合与自然人之间的关联关系而合理采用的所有手段。

条目注释 2：本定义旨在界定本文档中使用的术语 PII 。公共云 PII 处理器（3.5）通常无法明确判断其所处理的信息是否属于任何特定类别，除非云服务客户对此进行明确说明。

[来源：ISO/IEC 29100:2024,3.7，修订版——新增条目注释 2。]

**3.3**
**PII 控制器**
隐私利益相关方（或隐私利益相关方群体），其确定处理个人可识别信息（PII）（3.2）的目的和方式，但不包括将数据用于个人目的的自然人
条目注释 1： PII 控制器有时会指示其他设备[例如 PII 处理器（3.5）]代其处理 PII，但处理责任仍由 PII 控制器承担。

[来源：ISO/IEC 29100:2024,3.8]

**3.4**
**PII 本金**
与个人可识别信息（PII）（3.2）相关的自然人
条目注释 1：根据司法管辖区及特定 PII 保护与隐私法规，可使用“数据主体”这一同义词替代“ PII 主体”术语。

[来源：ISO/IEC 29100:2024,3.9，修订版——新增条目注释 1。]

**3.5**
**PII 处理机**
代表 PII 控制者并根据其指示处理个人可识别信息（PII）（3.2）的隐私利益相关方（3.3）

[来源：ISO/IEC 29100:2024,3.10]

**3.6**
PII 处理对个人身份信息（PII）执行的操作或操作集（3.2）
条目注释 1： PII 处理操作示例包括但不限于：收集、存储、修改、检索、查阅、披露、匿名化、假名化、传播或以其他方式提供、删除或销毁 PII 。

[来源：ISO/IEC 29100:2024 标准第 3.21 节（修订版）——新增‘ PII 处理’作为首选术语。]

**3.7**
**公共云服务提供商**
根据公有云模型提供云服务的厂商

## 4 概述

### 4.1 本文件结构

本文件采用 ISO/IEC 27002:2022 标准中描述控制措施的结构框架。在此方面，沿用了本文件早期版本（ISO/IEC 27018:2019）所采用的策略，即通过参照 ISO/IEC 27002:2013 标准中的控制措施进行重复阐述。

附录 B 提供了本文件与前一版本（ISO/IEC 27018:2019）中两种控制布局的对比分析。

具体而言，本文件在对照 ISO/IEC 27002:2022 标准中的控制措施时采用了以下规则：对于控制布局中各要素（详见 4.2 章节）完全相同的控制措施，仅需引用 ISO/IEC 27002:2022 中的对应条款。针对需要在公共云 PII 防护领域补充指导及相关信息的控制措施，分别在“公共云 PII 防护实施指南”和“公共云 PII 防护其他信息”章节提供补充说明。此类指导文件亦统称为“公共云服务提供商专项实施指南”。此外，适用于云计算服务提供商 PII 防护的附加控制措施及相关实施指南详见附录 A。需要特别说明的是，本文件中的条款编号与 ISO/IEC 27002:2022 标准中的对应条款编号保持完全一致。

表 1 中的对照组按四个主题进行分类，其对应关系如下：与第 5 至 8 条款所列对照组相对应。

—主题“提供公共云服务提供商专用实施指南”对应控制项“公共云 PII 保护实施指南”；

—主题“提供公共云服务提供商特定实施指南及其他信息”对应控制项“公共云 PII 保护实施指南及其他公共云 PII 保护相关信息”；

—主题“未提供额外的公共云服务提供商特定实施指南或其他 informationisprovided“correspondstothecontrol”nospecificGuidanceorotherinformationforPublic 云 PII 保护措施”；

—主题“公共云服务提供商专用实施指南，附附录 A 中控制措施的交叉引用”对应控制措施“公共云 PII 保护实施指南及附录 A 中 控制措施的交叉引用”。

**表 1 — ISO/IEC 27002:2022 标准中针对公共云服务提供商实施控制措施的专项指南及其他信息定位**

| ISO/IEC 27002:2022 控制标识符 | ISO/IEC 27002:2022 控制名称 | 主题 |
|---|---|---|
| **第 5 条 – 组织控制措施** | | |
| 5.1 | 信息安全政策 | 本文提供了针对公共云服务提供商的实施指南及其他相关信息。 |
| 5.2 | 信息安全职责与权限 | 本文提供了针对公共云服务提供商的实施指南。 |
| 5.3 | 职责分离 | 无额外公共云服务<br>提供了针对特定供应商的实施指南或其他相关信息。 |
| 5.4 | 管理职责 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.5 | 与主管部门接触 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.6 | 与特殊利益集团接触 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.7 a | 威胁情报 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.8 | 项目管理中的信息安全问题 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.9 | 信息及其他相关资产清单 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.10 | 信息及其他关联资产的可接受使用 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.11 | 资产返还 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.12 | 信息分类 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.13 | 信息标签 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |

ISO/IEC 27002:2022 标准中引入的控制措施。

该控制措施可作为《公共云 PII 保护实施指南》适用。

该控制措施适用于《公共云 PII 保护实施指南》及面向公共云 PII 的其他相关信息。

该控制措施的适用性表述为“未针对公共云 PII 保护提供具体指导或其他信息”。

该控制措施适用于《公共云 PII 保护实施指南》及其中对照的控制措施。

*表1（续）*

| ISO/IEC 27002:2022 控制标识符 | ISO/IEC 27002:2022 控制名称 | 主题 |
|---|---|---|
| 5.14 | 信息传递 | 提供了针对公共云服务提供商的实施指南。b |
| 5.15 | 访问控制 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.16 | 身份管理 | 提供了针对公共云服务提供商的实施指南。b |
| 5.17 | 认证信息 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.18 | 访问权限 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.19 | 供应商关系中的信息安全问题 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.20 | 在供应商协议中解决信息安全问题 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.21 | 信息通信技术供应链中的信息安全管理 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.22 | 供应商服务的监控、评审与变更管理 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.23 a | 云服务使用中的信息安全 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.24 | 信息安全事件管理计划的制定与准备 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.25 | 信息安全事件评估与决策 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.26 | 对信息安全事件的响应 | 提供了针对公共云服务提供商的具体实施指南，并附有对附件 A 中控制措施的交叉引用。 |
| 5.27 | 从信息安全事件中吸取教训 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.28 | 证据收集 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |

ISO/IEC 27002:2022 标准中引入的控制措施。

该控制措施可作为《公共云 PII 保护实施指南》适用。

该控制措施适用于《公共云 PII 保护实施指南》及面向公共云 PII 的其他相关信息。

该控制措施的适用性表述为“未针对公共云 PII 保护提供具体指导或其他信息”。

该控制措施适用于《公共云 PII 保护实施指南》及其中对照的控制措施。

*表 1（续）*

| ISO/IEC 27002:2022 控制标识符 | ISO/IEC 27002:2022 控制名称 | 主题 |
|---|---|---|
| 5.29 | 中断期间的信息安全 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.30 a | 企业持续经营的 ICT 准备情况 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.31 | 法律、法规、监管及合同要求 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.32 | 知识产权 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.33 | 记录保护 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.34 | PII 隐私与保护 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.35 | 信息安全的独立审查 | 提供了针对公共云服务提供商的实施指南。b |
| 5.36 | 遵守信息安全相关的政策、规则及标准 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 5.37 | 有文件记录的操作规程 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| **第 6 条 – 人员控制** | | |
| 6.1 | 放映 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 6.2 | 雇佣条款与条件 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 6.3 | 信息安全意识、教育和培训 | 本文提供了针对公共云服务提供商的实施指南及其他相关信息。 |
| 6.4 | 纪律程序 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 6.5 | 终止或变更雇佣关系后的责任 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |

ISO/IEC 27002:2022 标准中引入的控制措施。

该控制措施可作为《公共云 PII 保护实施指南》适用。

该控制措施适用于《公共云 PII 保护实施指南》及面向公共云 PII 的其他相关信息。

该控制措施的适用性表述为“未针对公共云 PII 保护提供具体指导或其他信息”。

该控制措施适用于《公共云 PII 保护实施指南》及其中对照照的控制措施。

*表 1（续）*

| ISO/IEC 27002:2022 控制标识符 | ISO/IEC 27002:2022 控制名称 | 主题 |
|---|---|---|
| 6.6 | 保密协议或非披露协议 | 提供了针对公共云服务提供商的具体实施指南，并附有对附件 A 中控制措施的交叉引用。 |
| 6.7 | 远程工作 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 6.8 | 信息安全事件报告 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| **第 7 条 – 物理控制措施** | | |
| 7.1 | 物理安全边界 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 7.2 | 物理入口 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 7.3 | 确保办公室、房间和设施的安全 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 7.4 a | 物理安全监控 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 7.5 | 防范物理和环境威胁 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 7.6 | 在安全区域工作 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 7.7 | 清理桌面和屏幕 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 7.8 | 设备选址与防护 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 7.9 | 场外资产安全 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 7.10 | 存储介质 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 7.11 | 辅助公用工程 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |

ISO/IEC 27002:2022 标准中引入的控制措施。

该控制措施可作为《公共云 PII 保护实施指南》适用。

该控制措施适用于《公共云 PII 保护实施指南》及面向公共云 PII 的其他相关信息。

该控制措施的适用性表述为“未针对公共云 PII 保护提供具体指导或其他信息”。

该控制措施适用于《公共云 PII 保护实施指南》及其中对照照的控制措施。

*表 1（续）*

| ISO/IEC 27002:2022 控制标识符 | ISO/IEC 27002:2022 控制名称 | 主题 |
|---|---|---|
| 7.12 | 布线安全 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 7.13 | 设备维护 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 7.14 | 设备的安全处置或重复使用 | 提供了针对公共云服务提供商的具体实施指南，并附有对附件 A 中控制措施的交叉引用。 |
| **第 8 条 – 技术控制措施** | | |
| 8.1 | 用户终端设备 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.2 | 特权访问权限 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.3 | 信息访问限制 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.4 | 源代码访问权限 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.5 | 安全认证 | 提供了针对公共云服务提供商的实施指南。b |
| 8.6 | 容量管理 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.7 | 恶意软件防护 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.8 | 技术漏洞管理 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.9 a | 配置管理 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.10 a | 信息删除 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.11 a | 数据掩蔽 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |

ISO/IEC 27002:2022 标准中引入的控制措施。

该控制措施可作为《公共云 PII 保护实施指南》适用。

该控制措施适用于《公共云 PII 保护实施指南》及面向公共云 PII 的其他相关信息。

该控制措施的适用性表述为“未针对公共云 PII 保护提供具体指导或其他信息”。

该控制措施适用于《公共云 PII 保护实施指南》及其中对照照的控制措施。

*表 1（续）*

| ISO/IEC 27002:2022 控制标识符 | ISO/IEC 27002:2022 控制名称 | 主题 |
|---|---|---|
| 8.12 a | 数据泄露预防 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.13 | 信息备份 | 提供了针对公共云服务提供商的实施指南。b |
| 8.14 | 信息处理设施冗余 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.15 | 记录 | 提供了针对公共云服务提供商的具体实施指南，并附有对附件 A 中控制措施的交叉引用。 |
| 8.16 a | 监测活动 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.17 | 时钟同步 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.18 | 特权实用程序的使用 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.19 | 操作系统上软件的安装 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.20 | 网络安全 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.21 | 网络服务安全性 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.22 | 网络隔离 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.23 a | Web 过滤 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.24 | 密码学的应用 | 提供了针对公共云服务提供商的实施指南。b |
| 8.25 | 安全开发生命周期 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.26 | 应用安全要求 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |

ISO/IEC 27002:2022 标准中引入的控制措施。

该控制措施可作为《公共云 PII 保护实施指南》适用。

该控制措施适用于《公共云 PII 保护实施指南》及面向公共云 PII 的其他相关信息。

该控制措施的适用性表述为“未针对公共云 PII 保护提供具体指导或其他信息”。

该控制措施适用于《公共云 PII 保护实施指南》及其中对照照的控制措施。

*表 1（续）*

| ISO/IEC 27002:2022 控制标识符 | ISO/IEC 27002:2022 控制名称 | 主题 |
|---|---|---|
| 8.27 | 安全系统架构与工程原理 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.28 a | 安全编码 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.29 | 开发与验收阶段的安全测试 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.30 | 外包开发 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.31 | 开发环境、测试环境与生产环境的分离 | 提供了针对公共云服务提供商的实施指南。b |
| 8.32 | 变更管理 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.33 | 试验信息 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |
| 8.34 | 审计测试期间信息系统保护 | 无额外公共云服务<br>未提供特定供应商的实施指南或其他相关信息。d |

ISO/IEC 27002:2022 标准中引入的控制措施。

该控制措施可作为《公共云 PII 保护实施指南》适用。

该控制措施适用于《公共云 PII 保护实施指南》及面向公共云 PII 的其他相关信息。

该控制措施的适用性表述为“未针对公共云 PII 保护提供具体指导或其他信息”。

该控制措施适用于《公共云 PII 保护实施指南》及其中对照照的控制措施。

## 4.2 控制布局

根据 ISO/IEC 27002:2022 标准，所有控制措施均按照上表 1 中列出的 4 个主题进行分类。每项控制措施包含以下要素：

a) 控制项名称：控制项的简称；

b) 属性表：该表格显示给定控件中各属性的数值；

c) 对照组：对照组的定义；

d) 目的：为何需实施该控制措施；

e) 指导原则：控制措施的实施方式；

f) 其他信息：解释性文字或对其他相关文件的引用。

子标题用于某些控制措施的指导文本中，以提高可读性，特别是在指导内容冗长且涉及多个主题时。此类标题并非所有指导文本中均需使用。

g) 公共云 PII 保护指南
该文件提供了更详尽的信息以支持控制措施的实施并达成控制目标。需注意，该指南并非适用于所有情况，亦不具有绝对充分性，因此无法满足组织特定的控制要求。故可采用替代性或补充性控制措施，或其他形式的风险处理方式（如规避、转移或接受风险）。

h) 公共云 PII 保护的其他信息

这提供了需进一步考量的补充信息，例如法律考量因素及其他标准的引用依据。

# 5 组织控制措施

## 5.1 信息安全政策

ISO/IEC 27002:2022 标准第 5.1 节中的指导原则适用。此外，以下针对公共云服务提供商的专项指导及相关信息亦适用。

a) 公共云 PII 防护实施指南

合同协议应明确公共云 PII 服务提供商、其分包商与云服务客户之间的责任划分，需根据所涉云服务类型进行考量[例如云计算参考架构中的基础设施即服务（IaaS）、平台即服务（PaaS）或软件即服务（SaaS）类别]。举例而言，应用层控制权的分配可能因公共云 PII 服务提供商提供的服务类型而异——若为 SaaS 服务，则与提供 PaaS 或 IaaS 服务的情况存在差异，后者允许云服务客户在其基础上构建或部署自有应用程序。

b) 公共云 PII 保护的其他信息

在某些司法管辖区，公共云 PII 处理器直接适用 PII 保护法规；而在其他地区， PII 保护法规仅适用于 PII 控制者。

云服务客户与公共云 PII 处理方之间的合同必须包含确保公共云 PII 处理方支持并管理合同合规性的机制。该合同可要求通过客户认可的独立合规审计，例如通过实施本文件及 ISO/IEC27002 标准中的相关控制措施。

## 5.2 信息安全职责与权限

ISO/IEC 27002:2022 标准第 5.2 节中的指导原则适用。此外，以下针对公共云服务提供商的专项指导原则亦适用。

a) 公共云 PII 防护实施指南

公共云 PII 处理系统应配备 PII 专家，为云服务客户提供 PII 信息妥善处理的指导建议。

### 5.3 职责分离

ISO/IEC 27002:2022 标准第 5.3 节中的指导原则适用。

### 5.4 管理职责

ISO/IEC 27002:2022 标准第 5.4 节中的指导原则适用。

### 5.5 与主管部门的联系

适用 ISO/IEC 27002:2022 标准第 5.5 节中的指导原则。

### 5.6 与特殊利益集团的接触

ISO/IEC 27002:2022 标准第 5.6 节中的指导原则适用。

### 5.7 威胁情报

注：ISO/IEC 27002:2022 中引入的新控制措施。 注：ISO/IEC 27002:2022 中引入的新控制措施。

ISO/IEC 27002:2022 标准第 5.7 节中的指导原则适用。

### 5.8 项目管理中的信息安全

适用 ISO/IEC 27002:2022 标准第 5.8 节中的指导原则。

### 5.9 信息库存及其他关联资产

ISO/IEC 27002:2022 标准第 5.9 节中的指导原则适用。

### 5.10 信息及相关资产的可接受使用方式

适用 ISO/IEC 27002:2022 标准第 5.10 条中的指导原则。

### 5.11 资产返还

ISO/IEC 27002:2022 标准第 5.11 节中的指导原则适用。

### 5.12 信息分类

适用 ISO/IEC 27002:2022 标准第 5.12 条中的指导原则。

### 5.13 信息标签

适用 ISO/IEC 27002:2022 标准第 5.13 条中的指导原则。

### 5.14 信息传递

ISO/IEC 27002:2022 标准第 5.14 条中的指导原则适用。此外，以下针对公共云服务提供商的专项指导原则亦适用。

a) 公共云 PII 防护实施指南

在使用物理介质进行信息传输时，系统应建立机制来记录包含 PII 的进出物理介质信息，包括介质类型、授权发送方/接收方、日期时间及介质数量。云服务客户应酌情实施相关措施，公共云 PII 服务商需具备技术支持能力，通过加密等附加防护手段降低未经授权访问在传输过程中（即到达目标目的地前）发生的可能性。在此类场景下，双方均可自主采取相应防护措施。

### 5.15 访问控制

适用 ISO/IEC 27002:2022 标准第 5.15 条中的指导原则。

### 5.16 身份管理

ISO/IEC 27002:2022 标准第 5.16 节中的指导原则适用。此外，以下针对公共云服务提供商的专项指导及相关信息亦适用。

a) 公共云 PII 防护实施指南

在云计算参考架构的服务类别框架下，云服务客户可负责其管辖范围内云服务用户的部分或全部访问管理。在适用情况下，公共云 PII 处理方应支持云服务客户对其管辖范围内的云服务用户访问权限进行管理。

用户注册与注销流程应针对用户访问控制遭破坏的情况进行设计，例如密码或其他注册数据（如因意外泄露所致）遭到篡改或泄露的情形。

注：各司法管辖区可对未使用认证凭证的检查频率制定具体要求。运营于这些司法管辖区的组织有责任确保其符合相关要求。 注：各司法管辖区可对未使用认证凭证的检查频率制定具体要求。运营于这些司法管辖区的组织有责任确保其符合相关要求。

### 5.17 认证信息

适用 ISO/IEC 27002:2022 标准第 5.17 条中的指导原则。

### 5.18 访问权限

适用 ISO/IEC 27002:2022 标准第 5.18 条中的指导原则。

### 5.19 供应商关系中的信息安全

适用 ISO/IEC 27002:2022 标准第 5.19 条中的指导原则。

### 5.20 供应商协议中的信息安全条款

适用 ISO/IEC 27002:2022 标准第 5.20 条中的指导原则。

### 5.21 信息通信技术供应链中的信息安全管理

ISO/IEC 27002:2022 标准第 5.21 条中的指导原则适用。

### 5.22 供应商服务的监控、评审与变更管理

适用 ISO/IEC 27002:2022 标准第 5.22 条中的指导原则。

### 5.23 云服务使用中的信息安全

注：ISO/IEC 27002:2022 中引入的新控制措施。 注：ISO/IEC 27002:2022 中引入的新控制措施。

适用 ISO/IEC 27002:2022 标准第 5.23 条中的指导原则。

### 5.24 信息安全事件管理规划与准备

ISO/IEC 27002:2022 标准第 5.24 条中的指导原则适用。

### 5.25 信息安全事件评估与决策

适用 ISO/IEC 27002:2022 标准第 5.25 条中的指导原则。

### 5.26 信息安全事件响应

适用 ISO/IEC 27002:2022 标准第 5.26 条中的指导原则。

a) 公共云 PII 防护实施指南

信息安全事件应触发公共云 PII 处理方的审查，作为其信息安全事件管理流程的一部分，以确定是否发生了涉及 PII 的数据泄露事件（参见 A.10.1）。

并非所有信息安全事件都必然需要触发此类审查。信息安全事件可能并未导致实际或显著概率的未授权访问 PII，或未导致对存储 PII 的公共云 PII 处理器设备或设施的未授权访问，且可能包括但不限于向防火墙或边缘服务器发送 ping 请求及其他诊断探测。

### 5.27 从信息安全事件中汲取经验教训

适用 ISO/IEC 27002:2022 标准第 5.27 条中的指导原则。

### 5.28 证据收集

适用 ISO/IEC 27002:2022 标准第 5.28 条中的指导原则。

### 5.29 系统中断期间的信息安全

适用 ISO/IEC 27002:2022 标准第 5.29 条中的指导原则。

### 5.30 企业持续运营所需的 ICT 基础设施准备情况

注：ISO/IEC 27002:2022 中引入的新控制措施。

适用 ISO/IEC 27002:2022 标准第 5.30 条中的指导原则。

### 5.31 法律、法规、规章及合同要求

ISO/IEC 27002:2022 标准第 5.31 条中的指导原则适用。

### 5.32 知识产权

适用 ISO/IEC 27002:2022 标准第 5.32 条中的指导原则。

### 5.33 记录保护

适用 ISO/IEC 27002:2022 标准第 5.33 条中的指导原则。

### 5.34 隐私与 PII 保护

ISO/IEC 27002:2022 标准第 5.34 条中的指导原则适用。

### 5.35 信息安全的独立审查机制

ISO/IEC 27002:2022 标准第 5.35 条中的指导原则适用。此外，以下针对公共云服务提供商的专项指导原则亦适用。

a) 公共云 PII 防护实施指南

若对个别云服务客户进行审计不切实际或可能增加安全风险，公共云 PII 处理方应在合同签订前及整个合同期内，向潜在云服务客户提供独立证据，证明其已实施信息安全措施。

根据公共云 PII 服务提供商的政策和程序进行运营。若能提供充分透明度，公共云 PII 服务提供商选定的相关独立审计通常可作为满足云服务客户审查 PII 服务提供商处理操作需求的有效方式。

### 5.36 信息安全政策、法规及标准的合规性

ISO/IEC 27002:2022 标准第 5.36 条中的指导原则适用。

### 5.37 有文件记录的操作规程

ISO/IEC 27002:2022 标准第 5.37 条中的指导原则适用。

## 6 人控制

### 6.1 筛选

ISO/IEC 27002:2022 标准第 6.1 节中的指导原则适用。

### 6.2 雇佣条款与条件

ISO/IEC 27002:2022 标准第 6.2 节中的指导原则适用。

### 6.3 信息安全意识、教育与培训

ISO/IEC 27002:2022 标准第 6.3 节中的指导原则适用。此外，以下针对公共云服务提供商的专项指导及相关信息亦适用。

a) 公共云 PII 防护实施指南

应制定相应措施，使相关人员充分认识到违反隐私或安全规则及程序（特别是涉及 PII 处理的相关规定）可能对公共云 PII 处理者（如业务损失、品牌受损或声誉损害）、员工（如纪律处分）及 PII 主体（如人身伤害、财产损失及精神损害）造成的潜在后果。

b) 公共云 PII 保护的其他信息 b) 公共云 PII 保护的其他信息

在某些司法管辖区，公共云 PII 处理者可能面临法律制裁，包括直接由当地 PII 保护机构处以巨额罚款。

### 6.4 纪律处分程序

ISO/IEC 27002:2022 标准第 6.4 节中的指导原则适用。

### 6.5 劳动合同终止或变更后的责任

适用 ISO/IEC 27002:2022 标准第 6.5 条中的指导原则。

### 6.6 保密协议或非披露协议

注：与保密协议或非披露协议相关的其他控制措施及指导原则可参见 A.10.1 章节。

ISO/IEC 27002:2022 标准第 6.6 节中的指导原则适用。

### 6.7 远程办公

ISO/IEC 27002:2022 标准第 6.7 节中的指导原则适用。

### 6.8 信息安全事件报告

适用 ISO/IEC 27002:2022 标准第 6.8 条中的指导原则。

## 7　7 体格控制措施

### 7.1 物理安全边界

ISO/IEC 27002:2022 标准第 7.1 节中的指导原则适用。

### 7.2 物理进入

ISO/IEC 27002:2022 标准第 7.2 节中的指导原则适用。

### 7.3 办公室、房间及设施的安保措施

ISO/IEC 27002:2022 标准第 7.3 节中的指导原则适用。

### 7.4 物理安全监控

注：ISO/IEC 27002:2022 中引入的新控制措施。

ISO/IEC 27002:2022 标准第 7.4 节中的指导原则适用。

### 7.5 防止物理和环境威胁

适用 ISO/IEC 27002:2022 标准第 7.5 章中的指导原则。

### 7.6 在安全区域工作

适用 ISO/IEC 27002:2022 标准第 7.6 节中的指导原则。

### 7.7 桌面和屏幕保持整洁

ISO/IEC 27002:2022 标准第 7.7 节中的指导原则适用。

### 7.8 设备选址与保护

适用 ISO/IEC 27002:2022 标准第 7.8 条中的指导原则。

### 7.9 市场外资产担保

ISO/IEC 27002:2022 标准第 7.9 条中的指导原则适用。

### 7.10 存储介质

适用 ISO/IEC 27002:2022 标准第 7.10 条中的指导原则。

### 7.11 辅助设施

ISO/IEC 27002:2022 标准第 7.11 节中的指导原则适用。

### 7.12 电缆布线安全

适用 ISO/IEC 27002:2022 标准第 7.12 条中的指导原则。

### 7.13 设备维护

适用 ISO/IEC 27002:2022 标准第 7.13 条中的指导原则。

### 7.14 设备的安全处置或再利用

适用 ISO/IEC 27002:2022 标准第 7.14 条中的指导原则。以下针对公共云服务提供商的专项指导原则亦适用。

a) 公共云 PII 防护实施指南

为确保安全处置或重复使用，对于可能含有 PII 的存储介质设备，应采取与实际存在 PII 时相同的处理措施。

注：关于设备安全处置或重复使用的其他控制措施与指导原则可参见 A.11.7 章节。

## 8　8 技术控制措施

### 8.1 用户终端设备

ISO/IEC 27002:2022 标准第 8.1 节中的指导原则适用。

### 8.2 特殊访问权限

ISO/IEC 27002:2022 标准第 8.2 节中的指导原则适用。

### 8.3 信息访问限制

ISO/IEC 27002:2022 标准第 8.3 节中的指导原则适用。

### 8.4 源代码访问权限

ISO/IEC 27002:2022 标准第 8.4 节中的指导原则适用。

### 8.5 安全认证

ISO/IEC 27002:2022 标准第 8.5 条中的指导原则适用。以下针对公共云服务提供商的专项指导原则亦适用。

a) 公共云 PII 防护实施指南

在需要时，公共云 PII 处理方应为云服务客户所申请的、由其控制的云服务用户账户提供安全登录流程。

### 8.6 容量管理

ISO/IEC 27002:2022 标准第 8.6 节中的指导原则适用。

### 8.7 防恶意软件保护

ISO/IEC 27002:2022 标准第 8.7 节中的指导原则适用。

### 8.8 技术漏洞管理

ISO/IEC 27002:2022 标准第 8.8 节中的指导原则适用。

### 8.9 配置管理

注：ISO/IEC 27002:2022 中引入的新控制措施。

ISO/IEC 27002:2022 标准第 8.9 节中的指导原则适用。

### 8.10 信息删除

注：ISO/IEC 27002:2022 中引入的新控制措施。

ISO/IEC 27002:2022 标准第 8.10 节中的指导原则适用。

### 8.11 数据掩蔽

注：ISO/IEC 27002:2022 中引入的新控制措施。

ISO/IEC 27002:2022 标准第 8.11 节中的指导原则适用。

### 8.12 数据泄露预防

注：ISO/IEC 27002:2022 中引入的新控制措施。

ISO/IEC 27002:2022 标准第 8.12 节中的指导原则适用。

### 8.13 信息备份

ISO/IEC 27002:2022 标准第 8.13 条中的指导原则适用。以下针对公共云服务提供商的专项指导原则亦适用。

a) 公共云 PII 防护实施指南

基于云计算模型的信息处理系统引入了额外或替代性异地备份机制，旨在防范数据丢失风险、保障

数据处理业务连续性，并在突发事件后具备数据恢复能力。为满足备份或恢复需求（或两者兼具），应在物理位置、逻辑位置或两者兼备的不同区域（包括系统内部存储空间）创建或维护数据副本。

在这方面， PII 特定责任可由云服务客户承担。若公共云 PII 服务提供商明确向云服务客户提供备份与恢复服务，则该提供商应向客户说明其云服务在数据备份与恢复方面的功能能力。

应制定相应程序，以确保在破坏性事件发生后，在特定且有文件记录的期限内恢复数据处理操作。

备份与恢复程序应按照规定的、有文件记录的频率进行审查。

注：部分司法管辖区可对备份与恢复程序的审查频率施加特定要求。在这些司法管辖区运营的组织有责任确保其符合相关要求。

使用分包商存储正在处理的数据的复制或备份副本，适用本文件中针对分包 PII 处理的控制措施 A.8.1 和 A.11.12。若涉及物理介质传输，则本文件中控制措施 5.14 和 A.11.5 亦适用。

公共云 PII 处理器应制定相关政策，明确信息备份要求及针对备份信息中所含 PII 的删除要求（如合同条款等附加要求）。

### 8.14 信息处理设施的冗余性

ISO/IEC 27002:2022 标准第 8.14 节中的指导原则适用。

### 8.15 记录

ISO/IEC 27002:2022 标准第 8.15 条中的指导原则适用。以下针对公共云服务提供商的专项指导原则亦适用。

a) 公共云 PII 防护实施指南
应建立流程，按照规定的、有文件记录的周期性对事件日志进行审查，以识别异常情况并提出补救措施。

在可行情况下，事件日志应记录事件是否导致 PII 发生变更（如新增、修改或删除）以及变更者信息。当多个服务提供商参与提供云计算参考架构中不同服务类别的服务时，实施本指南时可能涉及不同或共享的角色分工。

公共云 PII 处理器应制定标准，明确日志信息是否、何时以及如何向云服务客户开放或供其使用。这些操作流程需向云服务客户公开。

若云服务客户被授权访问由公共云 PII 处理器控制的日志记录，公共云 PII 处理器应确保该客户仅能访问与其自身活动相关的日志记录，且不得访问任何涉及其他云服务客户活动的日志记录。

为安全监控和运行诊断等目的记录的日志信息可能包含 PII 。应采取访问控制等措施，确保日志信息仅用于其预定用途。

应建立一套程序（优选自动化程序），以确保记录信息在规定且有文档记录的期限内被删除。

### 8.16 监测活动

注：ISO/IEC 27002:2022 中引入的新控制措施。

ISO/IEC 27002:2022 标准第 8.16 条中的指导原则适用。

### 8.17 时钟同步

ISO/IEC 27002:2022 标准第 8.17 条中的指导原则适用。

### 8.18 特权实用程序的使用

适用 ISO/IEC 27002:2022 标准第 8.18 条中的指导原则。

### 8.19 操作系统上的软件安装

ISO/IEC 27002:2022 标准第 8.19 条中的指导原则适用。

### 8.20 网络安全

适用 ISO/IEC 27002:2022 标准第 8.20 条中的指导原则。

### 8.21 网络服务的安全性

ISO/IEC 27002:2022 标准第 8.21 节中的指导原则适用。

### 8.22 网络隔离

适用 ISO/IEC 27002:2022 标准第 8.22 条中的指导原则。

### 8.23 网络过滤

注：ISO/IEC 27002:2022 中引入的新控制措施。

适用 ISO/IEC 27002:2022 标准第 8.23 条中的指导原则。

### 8.24 加密技术的应用

ISO/IEC 27002:2022 标准第 8.24 条中的指导原则适用。以下针对公共云服务提供商的专项指导原则亦适用。

a) 公共云 PII 防护实施指南

公共云 PII 处理器还应向云服务客户提供其提供的各项功能信息，这些功能可协助云服务客户实施和管理自身的加密保护措施及流程，例如：采用多种密钥管理方法、使用金库存储密钥或机密数据、部署密钥管理系统（KMS）、依托硬件安全模块（HSM）的服务、实施云 HSM 等。

注：在某些司法管辖区，可能需要采用加密技术来保护特定类型的 PII，例如涉及 PII 主体的健康数据、居民登记号码、护照号码及驾驶执照号码。

### 8.25 安全的开发生命周期

ISO/IEC 27002:2022 标准第 8.25 条中的指导原则适用。

### 8.26 应用程序安全要求

适用 ISO/IEC 27002:2022 标准第 8.26 条中的指导原则。

### 8.27 安全系统架构与工程原理

适用 ISO/IEC 27002:2022 标准第 8.27 条中的指导原则。

### 8.28 安全编码

注：ISO/IEC 27002:2022 中引入的新控制措施。

适用 ISO/IEC 27002:2022 标准第 8.28 条中的指导原则。

### 8.29 开发与验收阶段的安全测试

适用 ISO/IEC 27002:2022 标准第 8.29 条中的指导原则。

### 8.30 外包开发

适用 ISO/IEC 27002:2022 标准第 8.30 条中的指导原则。

### 8.31 开发环境、测试环境与生产环境的隔离

ISO/IEC 27002:2022 标准第 8.31 条中的指导原则适用。以下针对公共云服务提供商的专项指导原则亦适用。

a) 公共云 PII 防护实施指南
若无法避免使用 PII 进行检测，则应开展风险评估。需采取技术和组织措施以最大限度降低已识别风险。

### 8.32 变更管理

ISO/IEC 27002:2022 标准第 8.32 条中的指导原则适用。

### 8.33 测试信息

适用 ISO/IEC 27002:2022 标准第 8.33 条中的指导原则。

### 8.34 审计测试期间的信息系统保护

ISO/IEC 27002:2022 标准第 8.34 条中的指导原则适用。

# 附录 A
# (参考性)

# 面向 PII 保护的公共云 PII 处理器扩展控制集

## A.1 概述

本附录规定了新的控制措施及相关实施指南，这些措施与 ISO/IEC27002 标准中的控制措施和指南（参见第 5 至 8 条）相结合，构成一套扩展控制措施，以满足作为 PII 处理方的公共云服务提供商所适用的 PII 保护要求。

这些附加控制措施根据 ISO/IEC 29100 标准的 11 项隐私原则进行分类。在多数情况下，这些控制措施可归属于多项隐私原则之列。此类情形下，其分类依据以最相关的原则为准。

## A.2 同意与选择

### A.2.1 关于 PII 方权利的合作义务

a) 控制

公共云 PII 处理方应通过提供相关工具，使云服务客户能够履行其义务，从而保障 PII 主体对其相关 PII 的访问、更正及删除权利的行使。

b) 公有云 PII 防护实施指南

PII 控制者在此方面的义务可通过法律、法规或合同予以规定。这些义务可能涉及云服务客户使用公共云 PII 处理方服务进行实施的情形，例如及时修正或删除 PII 。

若 PII 控制者依赖公共云 PII 处理程序获取信息或技术手段以便利 PII 主体权利的行使，则相关信息或技术手段应在合同中予以明确。

## A.3 目的的合法性与具体说明

### A.3.1 公共云 PII 处理器的用途

a) 控制

根据合同需处理的 PII ，不得脱离云服务客户的指示进行任何独立用途的处理。

b) 公有云 PII 防护实施指南

公共云 PII 服务提供商与云服务客户之间的合同中可包含相关说明，例如服务需达成的目标及时间框

架。

为实现云服务客户的业务目标，公共云 PII 处理器在遵循客户总体指导方针的前提下，可基于技术考量自主确定 PII 处理方案，无需客户明确指示。例如，为高效利用网络或处理资源，可能需要进行特定资源分配。

处理资源的分配需依据 PII 主体的特定特征。当公共云 PII 处理方在确定处理方法时涉及 PII 的收集与使用时，应遵循 ISO/IEC 29100 标准中规定的相关隐私原则及‘隐私设计原则’（参见参考文献[64]和[65]）。

公共云 PII 处理方应及时向云服务客户提供所有相关信息，以确保其符合目的规范与限制原则，并保证公共云 PII 处理方及其分包商不会为超出云服务客户指令范围的其他用途处理 PII 。

### A.3.2 公共云 PII 处理器的商业应用

a) 控制

根据合同处理的 PII 未经明确同意，不得由公共云 PII 处理方用于营销和广告目的。此类同意不得作为接收服务的条件。

注：该控制措施是对 A.3.1 章节中更广泛控制措施的补充，并不替代或以其他方式取代其效力。

## A.4 收集限制

本隐私原则未涉及其他相关控制措施。

## A.5 数据最小化

### A.5.1 临时文件的安全删除

a) 控制

临时文件和文档应在规定且有记录的期限内予以删除或销毁。

b) 公有云 PII 防护实施指南

关于 PII 删除的操作指南详见 A.10.3 章节。

信息系统在运行过程中可能会生成临时文件。这类文件具有系统或应用程序的专属性，通常包含文件系统回滚日志、数据库更新相关临时文件以及其他应用软件运行时产生的临时文件。当对应的信息处理任务完成后，这些临时文件通常无需保留，应当及时删除——除非特殊情况需要保留。这些文件的保留时长并非固定不变，但系统应通过“垃圾回收”机制自动识别相关文件，并计算其自上次使用以来的持续时间。

PII 处理信息系统应实施定期检查，对超过指定保存期限的未使用临时文件进行删除。

## A.6 使用、保留及披露限制

### A.6.1 PII 披露通知

a) 控制

根据规定，公共云 PII 处理方与云服务客户之间的合同要求，公共云 PII 处理方必须按照既定流程向云服务客户发出通知。

合同约定的时间段内，执法机构提出任何具有法律约束力的 PII 披露请求，除非此类披露另有禁止规定。

b) 公有云 PII 防护实施指南

公共云 PII 处理方应提供合同保障，承诺其将：

— 拒绝任何不具备法律约束力的 PII 披露请求；

在进行任何 PII 披露前，若法律允许，应咨询相应的云服务客户；以及

—接受经相应云服务客户授权的、合同约定的 PII 披露请求。

示例：一种可能的披露禁令可为刑法中的禁止条款，旨在保护执法调查的机密性。

### A.6.2 PII 披露记录

a) 控制 a) 控制

向第三方披露 PII 时应做好记录，包括披露内容、披露 PII 、披露原因、披露对象及披露时间。

b) 公有云 PII 防护实施指南

PII 可在正常运营过程中予以披露，此类披露内容应予以记录。若涉及第三方披露（如合法调查或外部审计所引发的披露），亦需同步记录。相关记录应包含披露来源、披露原因及授权来源。

## A.7 准确性与质量

本隐私原则未涉及其他相关控制措施。

## A.8 开放性、透明度与信息披露

### A.8.1 分包 PII 处理过程的披露

a) 控制

若公共云 PII 处理方计划通过分包商处理 PII ， 应提前向相关云服务客户披露该情况。

b) 公有云 PII 防护实施指南

关于使用分包商处理 PII 的规定，应在公共云 PII 服务提供商与云服务客户之间的合同中明确透明。合同应明确规定，分包商的委派必须基于云服务客户在服务初期通常可给予的同意。公共云 PII 服务提供商应及时向云服务客户通报相关变更意向，以便云服务客户能够对变更提出异议或终止合同。

披露的信息应涵盖分包合同的使用情况及相关分包商名称，但不得包含任何业务细节。披露信息还应包括分包商可处理数据的国家（参见 A.12.1 条款），以及分包商必须履行或超越公共云 PII 处理方义务的具体方式（参见 A.11.12 条款）。

若公开分包商信息可能导致安全风险增加，则应在保密协议框架下披露，或根据云服务客户的要求进行披露。同时需向云服务客户明确说明相关信息的公开性。

## A.9 个人参与与访问权限

本隐私原则未涉及其他相关控制措施。

## A.10 责任制

### A.10.1 涉及 PII 的数据泄露事件通知

a) 控制

公共云 PII 处理方若发现任何未经授权访问 PII 、处理设备或设施的行为，导致 PII 丢失、泄露或篡改，应立即通知相关云服务客户。

b) 公有云 PII 防护实施指南

涉及 PII 数据泄露事件的通报条款应作为公共云 PII 服务商与云服务客户合同的组成部分。合同需明确服务商如何提供必要信息，以协助客户履行向主管部门报告的义务。该通报义务不适用于由云服务客户或 PII 主体自身导致的数据泄露事件，也不涵盖其负责的系统组件内部发生的数据泄露。合同还应规定涉及 PII 数据泄露事件的通报时限上限。

若发生涉及 PII 的数据泄露事件，应留存记录，内容包括：事件描述、发生时间范围、事件后果、举报人姓名、事件上报对象、事件处理步骤（含负责人及恢复数据信息），以及事件导致 PII 丢失、泄露或篡改的事实。

若发生涉及 PII 的数据泄露事件，记录中应包含已知数据泄露内容的描述。若已发出通知，记录应详细说明为通知云服务客户、监管机构或两者所采取的具体措施。

在某些司法管辖区，相关法律法规可能要求公共云 PII 处理方直接向相关监管机构（如 PII 保护机构）通报涉及 PII 的数据泄露事件。

注：可能存在其他需报告但未涵盖在此处的违规行为，例如未经同意或未获授权的收集行为、未经授权的用途等。

### A.10.2 行政安全政策与指南的保留期限

a) 控制

已更新的安全政策及操作规程现有副本，应按规定的文件化周期予以保留，直至替换完成。

b) 公有云 PII 防护实施指南

可能需要审查现行及历史政策与程序，例如在客户纠纷解决或 PII 保护机构调查的情况下。若无具体合同要求或其他适用规定，则建议至少保留五年期限。

### A.10.3 PII 退货、转移及处置

a) 控制
公共云 PII 处理器应针对这些活动制定相关政策，并向云服务客户提供该政策。

b) 公有云 PII 防护实施指南

在某个时间点， PII 需要以某种方式被处理。处理方式可能包括：将 PII 返还给云服务客户、转移至其他公共云 PII 处理方或 PII 控制方（例如因合并而转移）、安全删除或销毁、匿名化处理或归档保存。

公共云 PII 处理方应提供必要信息，使云服务客户能够确保合同项下 PII（由公共云 PII 处理方及其分包商）在存储位置被彻底清除（包括用于备份和业务连续性目的），且清除操作需在数据不再满足云服务客户特定需求时立即执行。合同中应明确规定数据处置机制（解绑、覆盖、消磁、销毁或其他形式的清除）的性质及适用商业标准。

公共云 PII 处理器应制定并实施关于 PII 处置的政策，并向云服务客户提供该政策。

该政策应涵盖合同终止后 PII 销毁前的保留期限，以保护云服务客户避免因合同意外失效导致 PII 丢失。

注：本控制与指导原则亦适用于“使用、保留及披露限制”原则中的保留要素（参见 A.6）。

## A.11 信息安全

### A.11.1 保密协议或非披露协议

a) 控制

受公共云 PII 处理器控制且可访问 PII 的个人，应承担保密义务。

b) 公有云 PII 防护实施指南

公共云 PII 处理方与其员工及代理之间签订的保密协议（无论何种形式）应确保员工及代理不得为独立于云服务客户指示之外的目的披露 PII（参见 A.3.1）。保密协议的义务应在相关合同终止后继续有效。

### A.11.2 禁止制作纸质材料

a) 控制

应限制制作展示 PII 的纸质材料。

b) 公有云 PII 防护实施指南

纸质材料包括通过印刷工艺制成的材料。

### A.11.3 数据恢复过程中的控制与日志记录

a) 控制

应建立数据恢复操作流程及记录日志。

b) 公有云 PII 防护实施指南

数据恢复工作日志应包含以下内容：责任人、恢复数据的描述以及手动恢复的数据。

### A.11.4 保护离开场所的存储介质上的数据

a) 控制

媒体离开组织场所时 PII 应遵循授权程序，且仅限授权人员访问（例如通过加密相关数据）。

### A.11.5 未加密便携式存储介质及设备的使用

a) 控制

除不可避免的情况外，不得使用不支持加密的便携式物理介质及便携式设备，且此类便携式介质与设备的使用情况均应予以记录。

### A.11.6 公共数据传输网络中传输 PII 的加密

a) 控制

通过公共数据传输网络传输的 PII 应在传输前进行加密处理。

b) 公有云 PII 防护实施指南

在某些情况下（例如电子邮件交换过程中），公共数据传输网络系统的固有特性可能要求暴露部分报文头或流量数据，以确保有效传输。

当多个服务提供商参与云计算参考架构中不同服务类别的服务提供时，在实施本指南过程中可能承担多样化或共享的角色。

### A.11.7 硬拷贝材料的安全处置

a) 控制

对于纸质材料的销毁，应采用交叉切割、粉碎、焚烧、制浆等安全处置方式。

### A.11.8 用户 ID 的唯一性使用

a) 控制

若多个用户可访问存储的 PII，则应为每位用户分配独立的用户 ID，用于身份识别、身份验证及权限授权。

### A.11.9 用户 ID 管理

a) 控制

停用或过期的用户 ID 不得授予其他个人。

b) 公有云 PII 防护实施指南

在整体云计算参考架构框架下，云服务客户可对其管辖范围内的云服务用户承担部分或全部用户 ID 管理职责。

### A.11.10 授权用户的记录

a) 控制

应维护一份最新记录，记录已授权访问该信息系统用户的用户信息或用户档案。

b) 公有云 PII 防护实施指南

所有经公共云 PII 处理器授权访问的用户均需维护用户档案。用户档案包含该用户的相关数据集合，包括用户 ID，这些数据是实施技术控制措施以实现对信息系统授权访问所必需的。

### A.11.11 合同措施

a) 控制

云服务客户与公共云 PII 处理方签订的合同应明确规定最低技术及组织保障措施，以确保合同约定的安全安排得以落实，且数据处理不得脱离控制方指令而进行任何用途。此类保障措施不得由公共云 PII 处理方单方面缩减。

b) 公有云 PII 防护实施指南

与公共云 PII 处理者相关的信息安全与 PII 保护义务可直接依据适用法律产生。若无此规定，则相关 PII 保护义务应由合同予以涵盖。

本文件中的控制措施与 ISO/IEC 27002 标准中的控制措施共同构成参考目录，旨在协助信息处理合同中关于 PII 的条款制定。公共云 PII 服务提供商应在签订合同前，向潜在云服务客户说明为保护 PII 所实施的信息安全与隐私控制措施。

公共云 PII 服务提供商在签订合同时应明确其服务范围。但最终由云服务客户负责确保公共云 PII 服务提供商采取的措施符合其义务要求。

### A.11.12 分包的 PII 处理

a) 控制

公共云 PII 处理方与处理 PII 的分包商之间签订的合同，应明确规定满足公共云 PII 处理方信息安全与 PII 保护义务要求的最低技术及组织措施。此类措施不得由分包商单方面缩减。

b) 公有云 PII 防护实施指南

使用分包商存储备份副本的行为受本控制措施约束（参见 A.8.1 节）。

### A.11.13 获取已使用数据存储空间的相关数据

a) 控制

公共云 PII 处理器应确保，每当向云服务客户分配数据存储空间时，该存储空间中先前存储的所有数据对该云服务客户不可见。

b) 公有云 PII 防护实施指南

当云服务用户删除信息系统中存储的数据时，性能问题可能导致数据的明确清除无法实现。这会引发其他用户可能读取数据的风险。应通过特定技术措施来规避此类风险。

在实施该控制措施时，尚无适用于所有场景的特定指导方案。但举例而言，若云服务用户试图读取未被其自身数据覆盖的存储空间，部分云基础设施、平台或应用程序将返回零值或 nonce 值。

## A.12 隐私合规性

### A.12.1 PII 地理位置

a) 控制

公共云 PII 处理器应明确并记录可能存储 PII 的国家。

b) 公有云 PII 防护实施指南

应向云服务客户提供可能存储 PII 的国家身份信息，其中需包含因使用外包 PII 处理而产生的国家信息。若涉及国际数据传输的具体合同协议（如标准合同条款、具有约束力的企业规则或跨境隐私规则），还应明确标注相关协议内容及其适用国家或情形。公共云 PII 处理方应及时向云服务客户通报此类变更计划，以便客户能够对变更提出异议或终止合同。

### A.12.2 PII 的预期目的地

a) 控制

通过数据传输网络进行的 PII 应受到适当控制措施的约束，以确保数据能够到达预期目的地。

# 附录 B（参考性）

## 本文件与第一版 ISO/IEC 27018:2019 之间的对应关系

本附录旨在为当前使用本文件（ISO/IEC 27018:2019）且希望过渡至该版本的组织提供与第一版的向后兼容性。

表 B.1 列出了第 5 至 8 条款中规定的控制措施与 ISO/IEC 27018:2019 标准中对应控制措施的对应关系。

**表 B.1 — 本文件中对照组与 ISO/IEC 27018:2019 中对照组的对应关系**

| ISO/IEC 27018:2025 控制标识符 | ISO/IEC 27018:2019 控制检验人 | 控制名 |
|---|---|---|
| 5.1 | 05.1.1, 05.1.2 | 信息安全政策 |
| 5.2 | 06.1.1 | 信息安全职责与权限 |
| 5.3 | 06.1.2 | 职责分离 |
| 5.4 | 07.2.1 | 管理职责 |
| 5.5 | 06.1.3 | 与主管部门接触 |
| 5.6 | 06.1.4 | 与特殊利益集团接触 |
| 5.7 | 新的 | 威胁情报 |
| 5.8 | 06.1.5, 14.1.1 | 项目管理中的信息安全问题 |
| 5.9 | 08.1.1, 08.1.2 | 信息及其他相关资产清单 |
| 5.10 | 08.1.3, 08.2.3 | 信息及其他关联资产的可接受使用 |
| 5.11 | 08.1.4 | 资产返还 |
| 5.12 | 08.2.1 | 信息分类 |
| 5.13 | 08.2.2 | 信息标签 |
| 5.14 | 13.2.1, 13.2.2, 13.2.3 | 信息传递 |
| 5.15 | 09.1.1, 09.1.2 | 访问控制 |
| 5.16 | 09.2.1 | 身份管理 |
| 5.17 | 09.2.4, 09.3.1, 09.4.3 | 认证信息 |
| 5.18 | 09.2.2, 09.2.5, 09.2.6 | 访问权限 |
| 5.19 | 15.1.1 | 供应商关系中的信息安全问题 |
| 5.20 | 15.1.2 | 在供应商协议中解决信息安全问题 |
| 5.21 | 15.1.3 | 信息通信技术供应链中的信息安全管理 |
| 5.22 | 15.2.1, 15.2.2 | 供应商服务的监控、评审与变更管理 |
| 5.23 | 新的 | 云服务使用中的信息安全 |
| 5.24 | 16.1.1 | 信息安全事件管理规划与准备 |
| 5.25 | 16.1.4 | 信息安全事件评估与决策 |
| 5.26 | 16.1.5 | 对信息安全事件的响应 |

*表 B.1（续）*

| ISO/IEC 27018:2025 控制标识符 | ISO/IEC 27018:2019 控制检验人 | 控制名 |
|---|---|---|
| 5.27 | 16.1.6 | 从信息安全事件中吸取教训 |
| 5.28 | 16.1.7 | 证据收集 |
| 5.29 | 17.1.1, 17.1.2, 17.1.3 | 中断期间的信息安全 |
| 5.30 | 新的 | 企业持续经营的 ICT 准备情况 |
| 5.31 | 18.1.1, 18.1.5 | 法律、法规、监管及合同要求 |
| 5.32 | 18.1.2 | 知识产权 |
| 5.33 | 18.1.3 | 记录保护 |
| 5.34 | 18.1.4 | PII 隐私与保护 |
| 5.35 | 18.2.1 | 信息安全的独立审查 |
| 5.36 | 18.2.2, 18.2.3 | 遵守信息安全相关的政策、规则及标准 |
| 5.37 | 12.1.1 | 有文件记录的操作规程 |
| 6.1 | 07.1.1 | 放映 |
| 6.2 | 07.1.2 | 雇佣条款与条件 |
| 6.3 | 07.2.2 | 信息安全意识、教育和培训 |
| 6.4 | 07.2.3 | 纪律程序 |
| 6.5 | 07.3.1 | 终止或变更雇佣关系后的责任 |
| 6.6 | 13.2.4 | 保密协议或非披露协议 |
| 6.7 | 06.2.2 | 远程工作 |
| 6.8 | 16.1.2, 16.1.3 | 信息安全事件报告 |
| 7.1 | 11.1.1 | 物理安全边界 |
| 7.2 | 11.1.2, 11.1.6 | 物理入口 |
| 7.3 | 11.1.3 | 确保办公室、房间和设施的安全 |
| 7.4 | 新的 | 物理安全监控 |
| 7.5 | 11.1.4 | 防范物理和环境威胁 |
| 7.6 | 11.1.5 | 在安全区域工作 |
| 7.7 | 11.2.9 | 清理桌面和屏幕 |
| 7.8 | 11.2.1 | 设备选址与防护 |
| 7.9 | 11.2.6 | 场外资产安全 |

| | | |
|---|---|---|
| 7.10 | 08.3.1, 08.3.2, 08.3.3, 11.2.5 | 存储介质 |
| 7.11 | 11.2.2 | 辅助公用工程 |
| 7.12 | 11.2.3 | 布线安全 |
| 7.13 | 11.2.4 | 设备维护 |
| 7.14 | 11.2.7 | 设备的安全处置或重复使用 |
| 8.1 | 06.2.1, 11.2.8 | 用户终端设备 |
| 8.2 | 09.2.3 | 特权访问权限 |
| 8.3 | 09.4.1 | 信息访问限制 |
| 8.4 | 09.4.5 | 源代码访问权限 |
| 8.5 | 09.4.2 | 安全认证 |
| 8.6 | 12.1.3 | 容量管理 |
| 8.7 | 12.2.1 | 恶意软件防护 |
| 8.8 | 12.6.1, 18.2.3 | 技术漏洞管理 |



***表 B.1（续）***

| **ISO/IEC 27018:2025 控制标识符** | **ISO/IEC 27018:2019 控制 检验人** | **控制名** |
|---|---|---|
| 8.9 | 新的 | 配置管理 |
| 8.10 | 新的 | 信息删除 |

| | | |
|---|---|---|
| 8.11 | 新的 | 数据掩蔽 |
| 8.12 | 新的 | 数据泄露预防 |
| 8.13 | 12.3.1 | 信息备份 |
| 8.14 | 17.2.1 | 信息处理设施冗余 |
| 8.15 | 12.4.1, 12.4.2, 12.4.3 | 记录 |
| 8.16 | 新的 | 监测活动 |
| 8.17 | 12.4.4 | 时钟同步 |
| 8.18 | 09.4.4 | 特权实用程序的使用 |
| 8.19 | 12.5.1, 12.6.2 | 操作系统上软件的安装 |
| 8.20 | 13.1.1 | 网络安全 |
| 8.21 | 13.1.2 | 网络服务安全性 |
| 8.22 | 13.1.3 | 网络隔离 |
| 8.23 | 新的 | Web 过滤 |
| 8.24 | 10.1.1, 10.1.2 | 密码学的应用 |
| 8.25 | 14.2.1 | 安全开发生命周期 |
| 8.26 | 14.1.2, 14.1.3 | 应用安全要求 |
| 8.27 | 14.2.5 | 安全系统架构与工程原理 |
| 8.28 | 新的 | 安全编码 |
| 8.29 | 14.2.8, 14.2.9 | 开发与验收阶段的安全测试 |
| 8.30 | 14.2.7 | 外包开发 |
| 8.31 | 12.1.4, 14.2.6 | 开发环境、测试环境与生产环境的分离 |
| 8.32 | 12.1.2, 14.2.2, 14.2.3, 14.2.4 | 变更管理 |
| 8.33 | 14.3.1 | 试验信息 |
| 8.34 | 12.7.1 | 审计测试期间信息系统保护 |

# 参考文献


[1] ISO 9000，质量管理体系——基础与术语

[2] ISO 55001，资产管理——资产管理体系——要求

[3] ISO/IEC 11770（全部部分），信息安全——密钥管理

[4] ISO/IEC 15408（全部部分），信息安全、网络安全与隐私保护——信息技术安全评估标准

[5] ISO 15489（全部部分），信息与文件——记录管理

[6] ISO/IEC 22123-1 信息技术——云计算——第 1 部分：术语

[7] ISO/IEC 22123-2 信息技术——云计算——第 2 部分：概念

[8] ISO/IEC 22123-3 信息技术——云计算——第 3 部分：参考架构

[9] ISO/IEC 19086（全部部分），云计算——服务级别协议（SLA）框架

[10] ISO/IEC 19770（全部部分），信息技术——IT 资产管理

[11] ISO/IEC 19941《信息技术——云计算——互操作性与可移植性》

[12] ISO/IEC 20889《隐私增强型数据去标识化术语及技术分类》

[13] ISO 21500：项目、计划与组合管理——背景与概念

[14] ISO 21502，项目、计划与组合管理——项目管理指南

[15] ISO 22301，安全与韧性——业务连续性管理系统——要求

[16] ISO 22313《安全与韧性——业务连续性管理系统——ISO 22301 应用指南》

[17] ISO/TS 22317，安全与韧性——业务连续性管理系统——业务影响分析指南

[18] ISO 22396，安全与韧性——社区韧性——组织间信息交换指南

[19] ISO/IEC/TS 23167，《信息技术——云计算——通用技术与方法》

[20] ISO/IEC 23751《信息技术——云计算与分布式平台——数据共享协议（DSA）框架》

[21] ISO/IEC 24760（全部部分），《信息技术安全与隐私——身份管理框架》

[22] ISO/IEC 27001:2022《信息安全、网络安全与隐私保护——信息安全管理体系要求》

[23] ISO/IEC 27002:2013《信息技术——安全技术——信息安全控制实践规范》1)

[24] ISO/IEC 27005《信息安全、网络安全与隐私保护——信息安全风险管理指南》

[25] ISO/IEC 27007《信息安全、网络安全与隐私保护——信息安全管理体系审核指南》

1) 已被 ISO/IEC 27002:2022 标准取消并取代。

[26] ISO/IEC/TS 27008《信息技术——安全技术——信息安全控制评估指南》

[27] ISO/IEC 27011《信息安全、网络安全与隐私保护——基于 ISO/IEC 27002 标准的电信组织信息安全控制措施》

[28] ISO/IEC/TR 27016，《信息技术——安全技术——信息安全管理体系——组织经济学》

[29] ISO/IEC 27017《信息技术——安全技术——基于 ISO/IEC 27002 的云服务信息安全控制实践规范》

[30]ISO/IEC27018《信息技术——安全技术——作为 PII 处理者的公共云中个人身份信息（PII）保护实践规范》

[31] ISO/IEC 27019《信息安全、网络安全与隐私保护——能源公用事业行业信息安全控制措施》

[32] ISO/IEC 27031《网络安全——信息与通信技术对业务连续性的准备状态》

[33] ISO/IEC 27033（全部部分）——信息技术——网络安全

[34] ISO/IEC 27034（全部部分），信息技术——应用安全

[35] ISO/IEC 27035-1 信息技术——信息安全事件管理 第 1 部分：原则与流程

[36] ISO/IEC 27035-2 信息技术——信息安全事件管理 第 2 部分：事件响应计划与准备指南

[37] ISO/IEC 27036（全部部分），网络安全——供应商关系

[38] ISO/IEC 27037《信息技术——安全技术——数字证据识别、收集、获取与保存指南》

[39] ISO/IEC 27040《信息技术——安全技术——存储安全》

[40] ISO/IEC 27050（全部部分），信息技术——电子取证

[41] ISO/IEC/TS 27110，《信息技术、网络安全与隐私保护——网络安全框架开发指南》

[42] ISO/IEC 27701，《安全技术——隐私信息管理对 ISO/IEC 27001 和 ISO/IEC 27002 的扩展——要求与指南》

[43] ISO 27799《健康信息学——基于 ISO/IEC 27002 标准的医疗健康领域信息安全管理体系》

[44] ISO/IEC 29100，信息技术——安全技术——隐私框架

[45] ISO/IEC 29115，《信息技术——安全技术——实体认证保证框架》

[46] ISO/IEC 29134，《信息技术——安全技术——隐私影响评估指南》

[47] ISO/IEC 29146，《信息技术——安全技术——访问管理框架》

[48] ISO/IEC 29147，《信息技术——安全技术——漏洞披露》

[49] ISO 30000《船舶与海洋技术——船舶回收管理系统——安全与环境友好型船舶回收设施管理系统的规范》

[50] ISO/IEC 30111，《信息技术——安全技术——漏洞处理流程》

[51] ISO 31000:2018 风险管理——指南

[52] IEC 31010《风险管理——风险评估技术》

[53] ISO/IEC 22123（全部部分），信息技术——云计算

[54] ISO/IEC 27555《信息安全、网络安全与隐私保护——个人身份信息删除指南》

[55]信息安全论坛（ISF）。《信息安全良好实践标准 2020》。可访问 https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for -information-security/

[56] ITIL 基金会，《 ITIL 4 版》， AXELOS ，2019 年 2 月，ISBN：9780113316076

[57] 美国国家标准与技术研究院（NIST），SP 800-37《信息系统与组织的风险管理框架：基于系统生命周期的安全与隐私保护方法》，第 2 版。2018 年 12 月[引用日期：2023-08-09]。可获取于 https://doi.org/10.6028/NIST.SP.800-37r2

[58] 开放网络应用安全项目（OWASP）。OWASP 十大风险榜单——2021 年十大最关键网络应用安全风险，2021 年[引用日期：2023-08-09]。获取地址：https://owasp.org/Top10/

[59]开放网络应用安全项目（OWASP）。《OWASP 开发者指南》，[在线] [访问日期：2023-08-09]。可获取于 https://owasp.org/www-project-developer-guide/

[60]开放网络应用安全项目（OWASP）。OWASP 十大 API 安全风险——2023 年版，[在线] [访问日期：2023-08-09]。可获取于 https://owasp.org/API-Security/editions/2023/en/0x11-t10/

[61]美国国家标准与技术研究院（NIST）National Institute SP800-63B《数字身份指南：认证与生命周期管理》。2020 年 2 月发布[引用日期：2023-08-09]。获取地址：https://doi.org/10.6028/NIST.SP.800-63b

[62] oasis，结构化威胁信息表达。可获取于 https://www.oasis-open.org/standards #stix2.0

[63] oasis，可信指标信息自动化交换平台。访问地址：https://www.oasis-open.org/standards#taxii2.0

[64] ISO 31700-1:2023 消费者保护---消费品和服务中的隐私设计原则 第 1 部分：高层次要求

[65] ISO/TR 31700-2:2023 消费者保护---消费品和服务中的隐私设计原则 第 2 部分：使用场景