国际标准

# ISO/IEC 29151

第一版
2017-08

# 信息技术-安全技术-个人身份信息保护业务守则

*信息技术--安全技术--人员信息保护规范*

参考编号ISO/IEC
29151:2017(E)

**受版权保护的文件**



国际标准化组织版权局
Ch.de Blandonnet 8-CP 401
CH-1214 Vernier,Geneva,
Switzerland电话：+412274901
11+41227490111
传真：+41227490947
copyright@iso.org
www.iso.org

# 目录

# 前言

国际标准化组织(ISO) 和国际电工委员会(IEC) 构成了世界标准化的专门体系。作为国际标准化组织或国际电工委员会成员的国家机构通过各自组织设立的技术委员会参与国际标准的制定，这些技术委员会负责特定领域的技术活动。国际标准化组织和国际电工委员会的技术委员会在共同感兴趣的领域开展合作。其他国际组织、政府组织和非政府组织也与国际标准化组织和国际电工委员会联络，参与制定工作。在信息技术领域，国际标准化组织和国际电工委员会成立了一个联合技术委员会，即ISO/IEC JTC1。

ISO/IEC 指令》第1部分介绍了制定本文件的程序和进一步维护本文件的程序。需要特别注意的是，不同类型的文件需要不同的审批标准。本文件根据《ISO/IEC 指令》第2部分的编辑规则起草(见 www.iso.org/directives)。

请注意，本文件的某些内容可能涉及专利权。国际标准化组织和国际电工委员会不负责确定任何或所有此类专利权。在本文件编写过程中发现的任何专利权的详细信息，将在导言和/或国际标准化组织收到的专利声明清单中列出(见www.iso.org/patents)。

本文件中使用的任何商品名称都是为方便用户而提供的信息，并不构成认可。

欲了解标准的自愿性质、与合格评定有关的ISO 专用术语和表述的含义，以及ISO 在技术性贸易壁垒 (TBT)中遵守世界贸易组织 (WTO) 原则的情况，请访问以下 URL: www.iso.org/iso/foreword.html。

负责本文件的委员会是ISO/IEC JTC1,信息技术，SC27,IT 安全技术，与ITU-T 协作。相同的文本作为ITU-T 建议X.1058 发布。

## 导言

处理个人身份信息(PII) 的机构越来越多，这些机构处理的PII 数量也越来越大。与此同时，社会对保护PII 和个人相关数据安全的期望也在不断提高。 一些国家正在加强其法律，以应对日益增多的引人注目的数据泄露事件 。

随 着PII 外泄事件的增加，收集或处理PII 的组织越来越需要关于如何保护PII 的指导，以降低发生隐私外泄的风险，并减少外泄事件对组织和相关个人的影响。本规范提供了此类指导。

本规范为PII 控制者提供了广泛的信息安全和PII 保护控制措施方面的指导，这些控制措施通常应用于处理PI 保护问题的许多不同组织中。这里列出的ISO/EC 标准系列的其他部分，为保护PII 的整个过程的其他方面提供了指导或要求：

-ISO/IEC 27001规定了信息安全管理流程和相关要求，可作为保护PII 的基础。

-ISO/IEC 27002为组织信息安全标准和信息安全管理实践提供了指导，包括控制措施的选择、实施和管理，同时考虑到组织的信息安全风险环境。

-ISO/IEC 27009规定了在任何特定部门(领域、应用领域或市场部门)使用ISO/EC 27001的要求。它解释了如何在ISO/EC27001 的要求之外增加其他要求，如何细化ISO/EC27001 的任何要求，以及如何在 ISO/IEC27001 附 件A 之外增加控制或控制集。

-ISO/IEC 27018为作为PII 处理者的组织在提供云服务处理功能时提供指导。

-ISO/EC29134 提供了识别、分析和评估隐私风险的指南，而ISO/IEC 27001和 ISO/IEC 27005则提供了识别、分析和评估安全风险的方法。

应根据风险分析结果确定的风险选择控制措施，以制定全面、 一致的控制制度。控制措施应适应特定的PII 处理环境。

本规范包括两个部分：1)由第1至18条组成的主体；2)规范性附件。这种结构反映了开发ISO/IEC 27002行业扩展的常规做法。

本规范主体结构(包括条款标题)反映了ISO/EC 27002的主体结构。引言和第1至4条介绍了本规范的使用背景。第5至18条的标题反映了ISO/IEC27002 的标题，反映了本规范以ISO/IEC 27002的指导为基础，增加了专门用于保护PII 的新控制措施。在PII 控制器方面，ISO/EC 27002中的许多控制措施无需赘述。不过，在某些情况下，需要额外的实施指导，这将在ISO/IEC27002 的相应标题(和条款编号)下给出。

该规范性附件包含一套扩展的PII 保护特定控制措施，对ISO/EC 27002中给出的控制措施进行了补充。这些新 的PII 保护控制措施及其相关指导分为12个类别，与ISO/IEC 29100中的隐私政策和11项隐私原则相对应：

- 同意和选择；
  目的、合法性和规格；
- 收集限制；
- 数据最小化；
- 使用、保留和披露限制；
- 准确性和质量；
- 公开、透明和通知；
- 个人参与和获取；
- 问责制；
- 信息安全；以及
- 隐私合规。

图1描述了本规范与ISO/IEC 标准系列之间的关系。

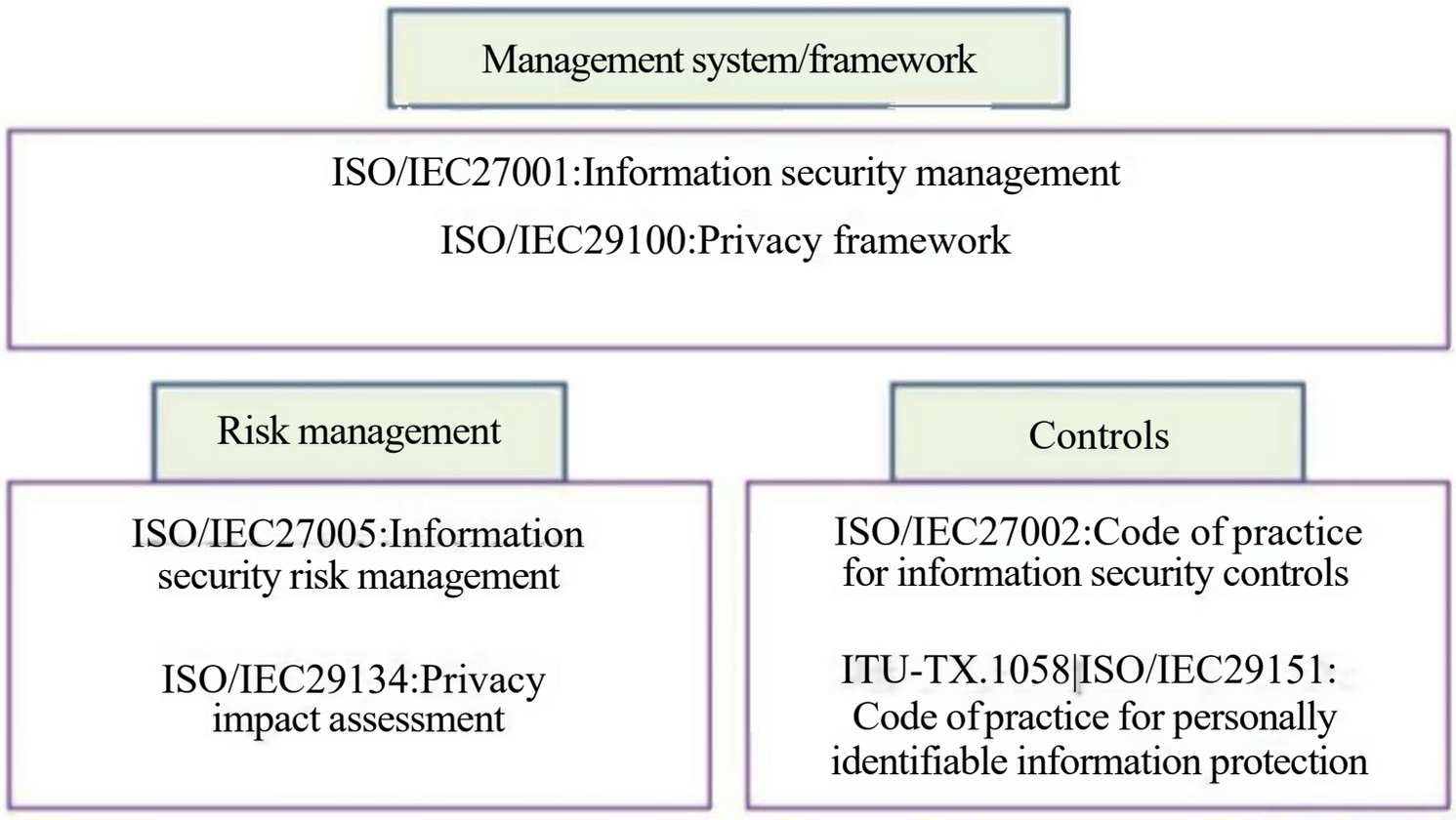


**图1-本规范与ISO/IEC标准系列的关系**

本规范包括基于 ISO/EC　27002的指导原则，并根据需要对其进行调整，以满足处理PII 时产生的隐私保护要求：

a)　在不同的处理领域，如

公共云服务、

- 社交网络应用、
- 家庭中与互联网连接的设备、

搜索、分析、

将PII用于广告和类似目的、

大数据分析计划、

- 就业处理、
- 销售和服务方面的业务管理(企业资源规划、客户关系管理)；

b)　在不同的地点，例如

- 在提供给个人的个人处理平台上(如智能卡、智能手机及其应用程序、智能电表、可穿戴设备)、
- 数据传输和收集网络内(例如，通过网络处理在操作中创建的移动电话位置数据，在某些司法管辖区可能被视为PII)、

在组织自身的处理基础设施内、

在第三方处理平台上；

c)　对于收集特性，例如

-一次性数据收集(如注册服务时)、

-持续的数据收集(例如，通过个人身上或体内的传感器频繁监测健康参数、使用非接触式支付卡进行支付的多重数据收集、智能电表数据收集系统等)。

注-正在进行的数据收集可能包含或产生行为、位置和其他类型的PII。在这种情况下，需要考虑使用PII 保护控制措施，在征得同意的基础上对访问和收集进行管理，并允许PII委托人对此类访问和收集进行适当控制。

**国际标准ITU-T 建议书**

# 信息技术-安全技术-个人身份信息保护业务守则

## 1 范围

本国际标准建议书确定了控制目标、控制措施和实施控制措施的指导原则，以满足与个人身份信息(PI) 保 护相关的风险和影响评估所确定的要求。

本建议书|国际标准特别规定了以ISO/EC 27002为基础的指导原则，同时考虑了在组织的信息安全风险环境中可能适用的PII 处理要求。

本建议书|国际标准适用于作为PII 控制者(如ISO/EC 29100所定义)的所有类型和规模的组织，包括处理PII的公共和私营公司、政府实体和非营利组织。

## 2 规范性参考资料

下列建议书和国际标准中的条款，通过在本文中引用，构成本建议书和国际标准的条款。在出版时，所标明的版本有效。所有建议书和标准均可修订，鼓励根据本建议书|国际标准达成协议的各方调查是否有可能采用下列建议书和标准的最新版本。国际电工委员会(IEC) 和国际标准化组织(ISO) 的成员都有目前有效的国际标准登记册。国际电信联盟(ITU) 电信标准化局保存一份当前有效的ITU-T 建议书清单。

- *ISO/IEC27002:2013, 信息技术--安全技术--信息安全控制操作规范。*
- *ISO/IEC 29100:2011,信息技术--安全技术--隐私框架。*

## 3 定义和缩写

### 3.1 定义

在本建议书|国际标准中，适用ISO/IEC 27000:2016、ISO/IEC29100和下列文件中的术语和定义。

*ISO在线浏览平台、IEC Electropedia和ITU术语和定义是标准化工作中使用的术语数据库。*

**3.1.1 首席隐私官(CPO):** 负责保护组织内个人身份信息(PII) 的高级管理人员。

**3.1.2 去身份识别过程:** 使用去标识化技术消除一组标识数据与数据主体之间的关联的过程。

### 3.2 简称

本规范使用以下缩写。

BCR具有约束力的 公司
规则 CCTVC 闭路电视CPOC
首席 隐私官PBDP隐私
设计
PDA 个人数字助理
PET 隐私增强技术

隐私影响评估
PIIP个人身份信息RFID 无线　　射频识
别USB 通 用　　串行总线

# 4　概述

## 4.1　保护PII的目标

本规范提供了一套保护PII的控制措施。保护PII 的目的是使组织能够制定一套控制措施，作为其整体PII 保护计划的一部分。根据ISO/IEC29100 中描述的隐私原则，这些控制措施可用于维护和改进隐私相关法律法规的合规性、管理隐私风险以及满足PII 委托人、监管机构或客户的期望。

## 4.2　要求保护PII

组织应确定其PII 保护要求。ISO/EC 29100中的隐私原则适用于确定要求。PII 保护要求有三个主要来源：

- 与保护PII 相关的法律、法规、监管和合同要求，例如，包括组织、其贸易伙伴、承包商和服务提供商必须遵守的PII 要求；
- 通过风险评估，在考虑到组织的整体业务战略和目标的情况下，评估组织和PII 委托人所面临的风险(即安全风险和隐私风险)；

  企业政策：企业也可以自愿选择超越先前要求中的标准。

各组织还应考虑为支持其运营而制定的处理PII 的原则(即ISO/IEC 29100中定义的隐私原则)、目标和业务要求。

应根据风险评估结果选择PII 保护控制措施(包括安全控制措施)。隐私影响评估(PIA) 的结果，如ISO/IEC 29134中规定的结果，将有助于指导和确定适当的处理措施和优先事项，以管理PII 保护风险和实施为防范这些风险而选定的控制措施。

PIA 规范(如ISO/IEC 29134中的规范)可提供PIA 指导，包括有关风险评估、风险处理计划、风险接受和风险审查的建议。

## 4.3　控制装置

隐私风险评估可帮助各组织确定因非法处理而导致隐私泄露的具体风险，或在设想的操作中涉及的PI 委托人的权利受到侵犯的具体风险。各组织应确定并实施控制措施，以处理风险影响过程中确定的风险。然后，应将控制措施和处理方法记录在案，最好是分别记录在单独的风险登记册中。某些类型的PII 处理可能需要特定的控制措施，只有在对设想的操作进行仔细分析后才会发现有此必要。

## 4.4　选择控制

可从本规范(其中包括ISO/IEC 27002中的参考控制，形成一个综合参考控制集)中选择控制。如有需要，也可从其他控制集中选择控制，或根据具体需要设计新的控制。

控制措施的选择取决于组织根据风险处理方案的标准和一般风险管理方法做出的决定，适用于组织，并通过合同协议适用于其客户和供应商，还应遵守所有适用的国家和国际法律法规。

控制措施的选择和实施还取决于组织在提供基础设施或服务中的角色。许多不同的组织都可能参与提供基础设施或服务。在某些情况下，选定的控制措施可能是某个特定组织独有的。在其他情况下，则可能需要共同承担实施控制的角色。合同协议应明确规定参与提供或使用服务的所有组织的PII 保护责任。

本规范中的控制措施可供处理PII 的机构参考，并适用于作为PII 控制者的所有机构。作为PII 处理者的机构应按照PII 控制者的指示行事。PII 控制者应确保其PII 处理者能够根据 PII处理的目的，执行PII 处理协议中包含的所有必要控制措施。使用云服务作为PII 处理程序的PII 控制者可以查看ISO/IEC 27018,以确定需要实施的相关控制措施。

本规范中的控制措施在第5至18条中有更详细的解释，并附有实施指南。如果在设计组织的信息系统、服务和操作时已经考虑到保护PII 的要求，那么实施起来就会更加简单。这种考虑是隐私设计(PBD) 概念的一个要素。有关选择控制措施和其他风险处理方案的更多信息，请参阅ISO/EC 29134。其他相关参考文献列于参考书目中。

## 4.5 制定针对具体组织的指导方针

本《规范》可视为制定针对具体组织的指导原则的起点。并非本规范中的所有控制和指导都适用于所有组织。此外，可能还需要本规范未包含的其他控制措施和指南。在制定包含附加指南或控制措施的文件时，在适用的情况下，最好包含与本规范中条款的交叉引用，以方便审计人员和业务合作伙伴进行合规性检查。

## 4.6 生命周期

PII 有一个自然的生命周期，从创建或起源、收集、存储、使用和转让到最终处置(如安全销毁)。在其生命周期中，PII 的价值和风险可能会有所不同，但在其生命周期的各个阶段和各种情况下，对PII 的保护在某种程度上仍然非常重要。

信息系统也有生命周期，在生命周期内，信息系统要经过构思、规定、设计、开发、测试、实施、使用、维护以及最终退役和处置。在上述每个阶段都应考虑到PII 的保护问题。新系统的开发和现有系统的变更为各组织提供了更新和改进安全控制措施以及PII 保护控制措施的机会，同时要考虑到实际事件以及当前和预计的信息安全和隐私风险。

## 4.7 本规范的结构

本规范的其余部分包括两个主要规范部分。

本规范的第一部分由第5至18条组成，包含ISO/IEC 27002中描述的某些相关现有控制的附加实施指导和其他信息。这一部分的格式使用了ISO/IEC27002 中相关条款的标题和编号，以便与该国际标准相互参照。

第二部分包含附件A 中规定的PI 保护的特定控制集。该控制集采用与ISO/IEC 27002相同的格式，规定了控制目标(方框内的文字),随后是一个或多个可应用的控制措施。控制说明的结构如下：

### 控制

本标题下的文字定义了实现控制目标的具体控制说明。

### 个人信息保护实施指南

本标题下的文字提供了更详细的信息，以支持控制的实施和控制目标的实现。本《规范》提供的指导可能并不完全适合或足以应对所有情况，也可能无法满足组织的具体控制要求。因此，替代或附加控制措施或其他形式的风险处理(避免或转移风险)可能是合适的。

### 保护PII的其他信息

本标题下的文字提供了可能需要考虑的进一步信息，如法律考虑因素和对其他标准的参考。

# 5 信息安全政策

## 5.1 信息安全的管理方向

### 5.1.1 导 言

ISO/IEC 27002:2013第5.1节规定的目标适用。

### 5.1.2 信息安全政策

ISO/IEC27002 中规定的控制5.1.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

信息安全政策应包括保护PII 的安全措施的适当说明。ISO/EC27002:2013 第18.1.4节提供了有关保护PII 的详细信息。

在设计、实施和审查信息安全政策时，组织应考虑ISO/IEC 29100中描述的隐私保护要求。

各组织应将与安全无关的PII 保护要素作为单独的隐私政策加以规定。参见条款A.2 中的指导。

### 5.1.3 审查信息安全政策

ISO/IEC27002 中规定的控制5.1.2和相关实施指南适用。

# 6 信息组织安全

## 6.1 内 部 组 织

### 6.1.1 导 言

ISO/IEC27002 中6.1规定的目标适用。

### 6.1.2 信息安全角色和责任

ISO/IEC27002 中规定的控制6.1.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

需要明确界定保护PII 的角色和责任，妥善记录并适当传达。具体来说

a) 应在组织内明确指定一名高级人员[有时称为首席隐私官(CPO)]，负 责PII 的保护；

b) 应指定一名或多名身份明确的个人(即PII 保护职能部门)负责与组织内的信息安全职能部门进行协调；以及

c) 所有参与处理PII 的人员(包括用户和辅助人员)的工作规范中都应包含适当的PII 保护要求。

已设立的PII 保护职能部门应与处理PII的其他职能部门、信息安全职能部门和法律职能部门密切合作，前者负责执行安全要求，其中包括PII保护法规定的安全要求，后者负责协助解释法律、法规和合同条款，并处理数据泄露事件。

组织应研究是否需要并酌情设立一个跨职能理事会或委员会，由处理PII 的职能部门的高级成员组成。保护个人信息安全是一项跨学科的职能，这样的小组可以帮助积极主动地发现改进的机会，确定新的风险和需要进行个人信息安全影响评估的领域，规划预防措施、检测和应对任何违规行为的措施等。建议此类小组定期召开会议，并由a) 项中确定的负责保护PII 的人员担任主席。

PII控制者应要求其PII 处理者指定一个联络点，负责处理与根据PII 处理合同处理PII 有关的问题。

负责PII 保护职能的个人应向CPO 报告，以确保他们有足够的权力履行职责。

### 6.1.3 职责分离

ISO/IEC27002 中规定的控制6.1.2和相关实施指南适用。以下补充指南也同样适用。

**个人信息保护实施指南**

保护个人信息安全的职责和责任范围应独立于信息安全的职责和责任范围。虽然认识到信息安全对保护个人信息安全的重要性，但信息安全和个人信息安全保护的职责和责任范围必须尽可能相互独立。如果有必要或有帮助，为了保护个人隐私，应促进信息安全负责人和个人隐私保护负责人之间的协调与合作。

在分配PII 处理的访问权限时，各组织应采用职责分离原则，特别是任何被确定为高风险的处理。

访问正在处理的PII 和访问与处理过程有关的日志文件应是不同的职责。

为回应PII 委托人的请求而获取与收集PII 有关的信息的权限应与获取PII 的所有其他形式的权限分开。访问权限应仅限于那些职责包括回应PII 委托人请求的人员。

### 6.1.4 与当局联系

ISO/IEC27002 中规定的控制6.1.3和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

在适用的情况下，组织应制定程序，明确规定何时以及由谁联系当局(包括数据保护当局),例如，报告隐私泄露或报告处理细节。

### 6.1.5 与特殊兴趣小组联系

ISO/IEC27002 中规定的控制6.1.4和相关实施指南及其他信息适用。

### 6.1.6 项目管理中的信息安全

ISO/IEC27002 中规定的控制6.1.5和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

任何新项目的启动都应至少进行一次阈值分析，以确定是否需要进行项目影响评估。请注意，项目一词涵盖组织实施或修改新的或现有技术、产品、服务、计划、信息系统、流程或项目的所有事件。

ISO/IEC29134 中规定的PIA 可提供进一步指导。

## 6.2 移动设备和远程办公

### 6.2.1 导言

ISO/IEC27002:2013 第6.2节规定的目标适用。

### 6.2.2 移动设备政策

ISO/IEC 27002中规定的控制6.2.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

组织应严格限制从便携式和移动设备(如笔记本电脑、移动电话、通用串行总线(USB) 设备和个人数字助理(PDA)) 访 问PII, 根据风险评估结果，这些设备通常可能比非便携式设备(如组织设施中的台式电脑)面临更高的风险。

组织应严格限制远程访问PII, 在远程访问不可避免的情况下，应确保远程访问的通信经过加密、信息验证和完整性保护。

### 6.2.3 远程办公

ISO/IEC27002 中规定的控制6.2.2和相关实施指南及其他信息适用。

# 7 人力资源安全

## 7.1 就 业 前

### 7.1.1 导言

ISO/IEC27002:2013 第7.1节规定的目标适用。

### 7.1.2 筛 选

ISO/IEC27002 中规定的控制7.1.1和相关实施指南及其他信息适用。

### 7.1.3 就业条款和条件

ISO/IEC27002 中规定的控制7.1.2和相关实施指南及其他信息适用。

## 7.2 就业期间

### 7.2.1 导 言

ISO/IEC27002:2013 第7.2节规定的目标适用。

### 7.2.2 管理职责

ISO/IEC27002 中规定的控制7.2.1和相关实施指南及其他信息适用。

### 7.2.3 信息安全意识、教育和培训

ISO/IEC27002 中规定的控制7.2.2和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

应采取措施，让相关工作人员了解违反隐私或安全规则和程序，特别是违反处理PII 的规则和程序可能给PII 控制者、工作人员和PII 委托人带来的后果(如法律后果、业务损失、品牌或声誉受损)。

与信息安全意识、教育和培训一样，组织也应提供有关保护和处理PII 的适当培训、教育和意识。

### 7.2.4 纪律程序

ISO/IEC27002 中规定的控制7.2.3和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

组织应制定正式的纪律政策。应向受影响的个人明确传达这一涉及隐私泄露的政策。组织应在所有侵犯隐私的情况下执行这一政策。

## 7.3 终止和变更

### 7.3.1 导言

ISO/IEC27002:2013 第7.3节规定的目标适用。

### 7.3.2 就业责任的终止或变更

ISO/IEC27002 中规定的控制7.3.1和相关实施指南及其他信息适用。

# 8 资产管理

## 8.1 资产的责任

### 8.1.1 导言

ISO/IEC27002:2013中8.1规定的目标适用。

### 8.1.2 资产清单

ISO/IEC27002 中规定的控制8.1.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

各组织应按照ISO/IEC29134 的规定，利用PIA 报告(如有)中提供的信息，建立、维护和更新资产清单。这应包括PII 资产和处理PII的所有系统。

在编制和维护清单时，各组织应从有关处理PII 的信息系统的PIA 中提取以下信息要素。以下清单仅作为示例，最终实施的清单可能会有增减：

a) 每个已确定系统的名称和缩写；

b) 这些系统处理的PII 类型；

c) 对所有类型的PII 进行分类(见8.2.2),既包括单个信息要素，也包括这些信息系统中的组合信息要素；

d) 任何PII 外泄事件对PII 委托人和组织的潜在影响程度；

e) 收 集PII的目的；

f) 是否将PII 处理外包给PII 处理商；

g) 是否将PII 传递给其他PII 控制者，如果是，传递给谁(或哪一组接收者)；

h)PII 的保留期限；

i) 收集或处理PII 的地理区域；以及

j) 是否涉及跨境数据传输。

各组织应定期向负责保护PII 的人员提供PII 清单的更新信息，以支持为所有新的或更新的处理PII的信息系统建立适当的安全控制。

### 8.1.3 资产所有权

ISO/IEC27002 中规定的控制8.1.2和相关实施指南及其他信息适用。

### 8.1.4 可接受的资产使用

ISO/IEC27002中规定的控制8.1.3和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

组织应保护支持PII的资产，防止未经授权的访问、未经授权的修改、未经授权的移除、丢失或毁坏，或错误和非法处理等。

### 8.1.5 资产返还

ISO/IEC27002中规定的控制8.1.4和相关实施指南及其他信息适用。

## 8.2 信 息 分 类

### 8.2.1 导言

ISO/IEC27002:2013 第8.2节规定的目标适用。

### 8.2.2 信息分类

ISO/IEC27002 中规定的控制8.2.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

组织应使用现有的分类类别(在ISO/IEC 27002中称为信息组)或新创建的分类类别，对包含PII 的所有信息进行分类。新的分类类别应包括但不限于敏感和非敏感PII等一般类别。分类方案还可包括更具体的类别，如个人健康信息(PHI)、个人财务信息(PFD。如果组织创建了新的分类类别，那么也应定义这些类别的保护级别。实际使用的类别还应取决于相关数据保护立法和法规中规定的要求、其他法律(如合同)义务、信息的性质和敏感性，以及发生泄密事件时可能产生的危害风险。

有些PII 在某个国家可能被归类为非敏感信息，但在其他国家可能被视为敏感信息，这取决于适用的数据保护法律。

当与一个或多个附加属性相关联时，PII 元素的分类可能需要重新评估和修改。应制定适当的准则和程序。

### 8.2.3 信息标签

ISO/IEC27002 中规定的控制8.2.2和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

如果组织没有将PII 划分到某个分类类别，则应确保受其控制的人员了解PII 的定义以及如何识别信息是否属于PII。

### 8.2.4 资产处理

ISO/IEC 27002中规定的控制8.2.3和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

如果组织允许受其控制的人员可以省略与PII 有关的分类类别的信息标签，则组织应让受其控制的人员将所有包含PII 的信息作为指定分类类别的信息处理。

## 8.3 媒 体 处 理

### 8.3.1 导言

ISO/IEC27002:2013第8.3节规定的目标适用。

### 8.3.2 可移动媒体的管理

ISO/IEC 27002中规定的控制8.3.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

某些司法管辖区可能要求对包含PII 的可移动媒体进行加密。无论法律是否要求，都建议进行加密，以降低PII外泄的风险。

如果数据保密性或完整性是重要的考虑因素，则应使用加密技术来保护可移动媒体上的PII。应进行风险评估，以确定所需的保护级别，这反过来将有助于确定所用加密算法的必要类型、强度和质量。

10.1中提供了有关使用加密控制的其他指导。

### 8.3.3 介质的处置

ISO/IEC27002 中规定的控制8.3.2和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

安全处置含有PII 的介质的程序应与信息的敏感性以及不当处理信息所造成的影响程度相称。某些司法管辖区可能会对用于处置含有PII 或特定类型PII （如健康数据、财务数据）的介质的程序规定标准。

### 8.3.4 物理介质传输

ISO/IEC27002 中规定的控制8.3.3和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

只要使用物理介质进行信息传输，就应采取措施记录含有PII 的物理介质的进出情况，包括物理介质的类型、任何识别码(如序列号或库存标签号)、授权的发送方/接收方、日期和时间、物理介质的数量及其所含PII 的类型，并检测物理介质的丢失情况。还应记录转移的目的和范围、负责授权的人员以及转移的法律/合同依据。还应考虑明确提及数据最小化原则。

## 9 访问控制

### 9.1 访问控制的业务要求

#### 9.1.1 导 言

ISO/IEC27002:2013 中9.1规定的目标适用。

#### 9.1.2 访问控制政策

ISO/IEC27002 中规定的控制9.1.1和相关实施指南及其他信息适用。

#### 9.1.3 访问网络和网络服务

ISO/IEC27002 中规定的控制9.1.2和相关实施指南及其他信息适用。

### 9.2 用户访问管理

#### 9.2.1 导言

ISO/IEC27002:2013 中9.2规定的目标适用。

#### 9.2.2 用户注册和注销

ISO/IEC27002 中规定的控制9.2.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

用户注册和注销注册以及用户生命周期管理程序应提供措施，以应对用户访问控制受损的情况，如密码或其他用户注册数据损坏或受损(如无意中泄露)。

#### 9.2.3 用户访问配置

ISO/IEC27002 中规定的控制9.2.2和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

各组织应根据ISO/IEC29100 中描述的数据最小化原则，为用户提供适当的访问处理PII 的信息系统的权利。

各组织应根据ISO/IEC 29100中描述的数据最小化原则，限制对处理PII 的信息系统的访问权限，只允许最少数量的个人访问，以实现处理PII 的特定目的。

对于特定的PII 和 PII 处理(如健康数据)，各组织应采用强大的身份验证方法。

### 9.2.4 特权访问权限管理

ISO/IEC27002 中规定的控制9.2.3和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

大规模处理PII（如批量查询、批量修改、批量导出、批量删除）会增加大规模泄密的风险。组织在为此类特权操作分配访问权限时应特别小心。为防止PII 被滥用，应严格限制为PII 处理（特别是高风险PI 处理）分配特权访问权限。分配这些权限的方式还应有助于降低两人或多人串通的风险。此类权限的授予和使用情况应记录在相关日志文件中。所有访问批准都应规定期限。组织应定期审查所有此类批准，并酌情延长、撤销或终止批准 。

### 9.2.5 管理用户的秘密认证信息

ISO/IEC27002 中规定的控制9.2.4和相关实施指南及其他信息适用。

### 9.2.6 审查用户访问权限

ISO/IEC27002 中规定的控制9.2.5和相关实施指南及其他信息适用。

### 9.2.7 取消或调整使用权

ISO/IEC27002 中规定的控制9.2.6和相关实施指南及其他信息适用。

## 9.3 用 户 责 任

### 9.3.1 导言

ISO/IEC27002:2013 中9.3规定的目标适用。

### 9.3.2 使用秘密认证信息

ISO/IEC27002 中规定的控制9.3.1和相关实施指南及其他信息适用。

## 9.4 系统和应用程序访问控制

### 9.4.1 导言

ISO/IEC27002:2013 中9.4规定的目标适用。

### 9.4.2 信息访问限制

ISO/IEC27002 中规定的控制9.4.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

在允许操作员和管理员等个人使用能够从包含PII 的数据库中自动大量检索PII 的查询语言之前，组织应审查在处理PII 时使用此类语言的必要性。

在使用查询语言符合保护要求的情况下，各组织应提供技术措施，将此类语言的使用限制在实现指定目的所需的最低限度。

例如，这可能意味着访问限制将查询语言的使用局限于记录中预先定义的几个敏感字段。

如果个人需要进入其通常无权进入的区域（如业务区域），则应实施强有力的审批机制。各组织应保存所有此类审批的记录。

### 9.4.3 安全登录程序

ISO/IEC27002 中规定的控制9.4.2和相关实施指南及其他信息适用。以下补充指南也同样适用。

个人信息保护实施指南

如果PII 委托人可以向PII 控制者申请账户，PII 控制者应根据风险分析结果，为这些账户提供安全登录程序。

### 9.4.4 密码管理系统

ISO/IEC27002 中规定的控制9.4.3和相关实施指南及其他信息适用。

### 9.4.5 使用特权实用程序

ISO/IEC27002 中规定的控制9.4.4和相关实施指南及其他信息适用。

### 9.4.6 程序源代码的访问控制

ISO/IEC27002 中规定的控制9.4.5和相关实施指南及其他信息适用。

## 10 加密技术

### 10.1 加 密 控 制

#### 10.1.1 导 言

ISO/IEC27002:2013 中10.1规定的目标适用。

#### 10.1.2 使用加密控制的政策

ISO/IEC27002 中规定的控制10.1.1和相关实施指南及其他信息适用。

#### 10.1.3 关键管理

ISO/IEC27002 中规定的控制10.1.2和相关实施指南及其他信息适用。

## 11 物理和环境安全

### 11.1 安全区域

#### 11.1.1 导 言

ISO/IEC27002:2013 中11.1规定的目标适用。

#### 11.1.2 实体安全边界

ISO/IEC 27002中规定的控制11.1.1和相关实施指南及其他信息适用。

#### 11.1.3 物理入口控制

ISO/IEC27002 中规定的控制11.1.2和相关实施指南及其他信息适用。

#### 11.1.4 确保办公室、房间和设施的安全

ISO/IEC27002 中规定的控制11.1.3和相关实施指南及其他信息适用。

#### 11.1.5 防范外部和环境威胁

ISO/IEC27002 中规定的控制11.1.4和相关实施指南及其他信息适用。

#### 11.1.6 在安全区域工作

ISO/IEC27002 中规定的控制11.1.5和相关实施指南及其他信息适用。

#### 11.1.7 运送和装卸区

ISO/IEC27002 中规定的控制11.1.6和相关实施指南及其他信息适用。

## 11.2 设 备

### 11.2.1 导 言

ISO/IEC 27002:2013第11.2节规定的目标适用。

### 11.2.2 设备选址和保护

ISO/IEC27002 中规定的控制11.2.1和相关实施指南及其他信息适用。

### 11.2.3 辅助公用设施

ISO/IEC27002 中规定的控制11.2.2和相关实施指南及其他信息适用。

### 11.2.4 布线安全

ISO/IEC27002 中规定的控制11.2.3和相关实施指南及其他信息适用。

### 11.2.5 设备维护

ISO/IEC27002 中规定的控制11.2.4和相关实施指南及其他信息适用。

### 11.2.6 拆除资产

ISO/IEC27002 中规定的控制11.2.5和相关实施指南及其他信息适用。

### 11.2.7 楼外设备和资产的安全

ISO/IEC27002 中规定的控制11.2.6和相关实施指南及其他信息适用。

### 11.2.8 设备的安全处置或再利用

ISO/IEC27002 中规定的控制11.2.7和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

为了安全处置或重新使用，应物理销毁含有可能含有PII 的存储介质的设备，或按照明确规定并记录在案的程序，使用经批准的技术销毁、删除或覆盖PII, 使 原 始PII无法恢复，而不是简单地使用标准的删除或格式化功能。对于含有可能包含加密PII 的存储介质的设备，有控制地销毁解密密钥或密钥持有人(如智能卡)可能就足够了 。

### 11.2.9 无人值守的用户设备

ISO/IEC27002 中规定的控制11.2.8和相关实施指南及其他信息适用。

### 11.2.10 清晰桌面和清晰屏幕政策

ISO/IEC 27002中规定的控制11.2.9和相关实施指南及其他信息适用。

# 12 业务安全

## 12.1 运行程序和责任

### 12.1.1 导 言

ISO/IEC27002:2013 中12.1规定的目标适用。

### 12.1.2 记录在案的操作程序

控制项12.1.1和相关实施指南以及ISO/IEC27002 中规定的其他信息均适用。

### 12.1.3 变革管理

控制项12.1.2和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

### 12.1.4 能力管理

控制项12.1.3和相关实施指南以及ISO/IEC 27002中规定的其他信息适用。

### 12.1.5 开发、测试和运行环境分离

ISO/IEC 27002中规定的控制项12.1.4和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

开发、测试和运行环境应在逻辑上分开，并尽可能在物理上分开。应实施适当的访问控制，确保只有经过适当授权的人员才能访问。如果测试或开发网络或设备需要访问运行网络，则应实施严格的访问控制。

无论使用环境如何，组织都应评估使用含有PII 的可移动媒体和具有无线功能的设备的风险。

在法律不允许或PII 委托人明确同意的情况下，未经事先匿名处理，不得将PII 用于开发和测试目的。

## 12.2 防止恶意软件

### 12.2.1 导 言

ISO/IEC27002:2013 第12.2节规定的目标适用。

### 12.2.2 控制恶意软件

控制项12.2.1和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

## 12.3 备份

### 12.3.1 导 言

ISO/IEC27002:2013 第12.3节规定的目标适用。

### 12.3.2 信息备份

ISO/IEC 27002中规定的控制项12.3.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

处 理PII 的信息系统应引入额外或替代机制，如异地备份，以防止PII 丢失，确保PII 处理操作的连续性，并在绝对必要的情况下，提供在中断事件后恢复PII 处理操作的能力。

注意：备份和恢复操作之间会间隔一段时间。在访问备份中存储的PII以进行恢复时，这些PII 可能不再是最新的。任何基于过期PII的操作都可能导致错误的结果，并带来隐私风险。

## 12.4 日志和监测

### 12.4.1 导 言

ISO/IEC27002:2013 第12.4节规定的目标适用。

### 12.4.2 事件记录

ISO/IEC 27002中规定的控制项12.4.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

在可能的情况下，事件日志应记录访问了哪些PII、对 PII 做了哪些操作(如读取、打印、添加、修改、删除)、何时以及由谁访问，特别是对于某些类型的PII （如健康数据)。如果有多个服务提供商参与提供某项服务，在执行本指南时可能会有不同或共同的角色。

应制定一个流程，按规定的、有记录的周期审查事件日志，以确定异常情况并提出补救措施。

PII 控制者应就日志信息是否、何时以及如何提供给管理员或管理员是否可将日志信息用于安全监控和运行诊断等目的制定相关程序。

### 12.4.3 保护日志信息

ISO/IEC 27002中规定的控制项12.4.2和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

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(见9.2.3)等措施，确保记录的信息仅用于预期目的。应采取措施确保日志文件的完整性。

### 12.4.4 管理员和操作员日志

ISO/IEC 27002中规定的控制项12.4.3和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

各组织应监控对PII 的特权访问(如系统管理员和操作员)以及这些个人随后的任何处理。这种监控应成为对处理PII 的信息系统进行全面监控的一部分。

各组织应界定它们认为的异常活动，并应实施自动程序，向组织内的相关人员报告此类活动。

### 12.4.5 时钟同步

控制项12.4.4和相关实施指南以及ISO/IEC 27002中规定的其他信息适用。

## 12.5 控制运行软件

### 12.5.1 导言

ISO/IEC27002:2013 第12.5节规定的目标适用。

### 12.5.2 在运行系统上安装软件

控制项12.5.1和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

## 12.6 技术漏洞管理

### 12.6.1 导言

ISO/IEC27002:2013 第12.6节规定的目标适用。

### 12.6.2 技术漏洞管理

控制项12.6.1和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

### 12.6.3 软件安装限制

控制项12.6.2和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

## 12.7 信息系统审计

### 12.7.1 导 言

ISO/IEC27002:2013第12.7节规定的目标适用。

### 12.7.2 信息系统审计控制

控制项12.7.1和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

# 13 通信安全

## 13.1 网络安全管理

### 13.1.1 导 言

ISO/IEC27002:2013 中13.1规定的目标适用。

### 13.1.2 网络控制

ISO/IEC27002 中规定的控制项13.1.1和相关实施指南及其他信息适用。

### 13.1.3 网络服务的安全性

ISO/IEC27002 中规定的控制项13.1.2和相关实施指南及其他信息适用。

### 13.1.4 网络中的隔离

ISO/IEC27002 中规定的控制项13.1.3和相关实施指南及其他信息适用。

## 13.2 信息转移

### 13.2.1 导 言

ISO/IEC27002:2013 第13.2节规定的目标适用。

### 13.2.2 信息传递政策和程序

ISO/EC 27002中规定的控制项13.2.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

应采取适当措施，降低信息传输过程中PII 泄露的风险。一般来说，这可以通过加密来解决，其他初步措施可包括去标识化、屏蔽或混淆。

### 13.2.3 信息转让协议

ISO/IEC27002 中规定的控制项13.2.2和相关实施指南及其他信息适用。

### 13.2.4 电子信息

ISO/IEC27002 中规定的控制项13.2.3和相关实施指南及其他信息适用。

### 13.2.5 保密或非披露协议

ISO/IEC 27002中规定的控制项13.2.4和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

各组织应明确规定外部处理PII 的条件。这些条件应成为适当协议(如合同、保密或保密协议)的一部分。

# 14 系统购置、开发和维护

## 14.1 信息系统的安全要求

### 14.1.1 导 言

ISO/IEC 27002:2013第14.1节规定的目标适用。

### 14.1.2 信息安全要求分析和说明

ISO/IEC27002 中规定的控制14.1.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

在开发处理PII 的信息系统或对其进行重大修改时，应进行PIA。关于进行PIA 的指导可参见ISO/IEC29134。PIA的结果应用于确定控制措施，以处理PIA 过程中发现的风险。

### 14.1.3 确保公共网络应用服务的安全

ISO/IEC27002 中规定的控制14.1.2和相关实施指南及其他信息适用。

### 14.1.4 保护应用服务交易

ISO/IEC 27002中规定的控制14.1.3和相关实施指南及其他信息适用。

## 14.2 开发和支持过程中的安全性

### 14.2.1 导 言

ISO/IEC27002:2013 第14.2节规定的目标适用。

### 14.2.2 安全发展政策

ISO/IEC27002 中规定的控制14.2.1和相关实施指南及其他信息适用。

### 14.2.3 系统变更控制程序

ISO/IEC27002 中规定的控制14.2.2和相关实施指南及其他信息适用。

### 14.2.4 操作平台变更后对应用程序进行技术审查

ISO/IEC27002 中规定的控制14.2.3和相关实施指南及其他信息适用。

### 14.2.5 对软件包更改的限制

ISO/IEC27002 中规定的控制项14.2.4和相关实施指南及其他信息适用。

### 14.2.6 安全系统工程原则

ISO/IEC27002 中规定的控制项14.2.5和相关实施指南及其他信息适用。

### 14.2.7 安全的开发环境

ISO/IEC27002 中规定的控制项14.2.6和相关实施指南及其他信息适用。

### 14.2.8 外包开发

ISO/IEC27002 中规定的控制项14.2.7和相关实施指南及其他信息适用。

### 14.2.9 系统安全测试

ISO/IEC27002 中规定的控制项14.2.8和相关实施指南及其他信息适用。

### 14.2.10 系统验收测试

ISO/EC 27002中规定的控制项14.2.9和相关实施指南及其他信息适用。以下补充指南也同样适用。



系统验收测试还应包括对隐私保护要求的测试。

## 14.3 测试数据

### 14.3.1 导言

ISO/IEC27002:2013 第14.3节规定的目标适用。

### 14.3.2 保护测试数据

ISO/IEC 27002中规定的控制项14.3.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

包含PII 的运行数据通常不应被用于开发和测试。在这些环境中使用真实的PII 会增加信息泄露的风险。相反，组织应使用合成数据，或采取措施"隐藏"(如屏蔽、混淆、去标识化)使用中的任何真实PII。

# 15 供应商关系

## 15.1 供应商关系中的信息安全

### 15.1.1 导 言

ISO/IEC27002:2013 第15.1节规定的目标适用。

### 15.1.2 供应商关系信息安全政策

ISO/IEC 27002中规定的控制项15.1.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

如果组织需要使用PII 处理程序的服务，则应根据经验、可信度及其满足适用法律、法规或合同或其他法律协议中规定的PII 保护要求的能力对PII 处理程序进行评估。

作为PII 控制者的组织应与作为PII 处理者的任何供应商签订书面合同。合同应明确规定PII 控制者与PII 处理者之间的作用和责任，并应包含与PII 保护有关的适当条款，以便让PII 处理者对所执行的处理工作负责。

PII控制者合同至少应规定

关于合同处理的规模、性质和目的的适当声明；

- 支持个人信息处理者的职责，让个人信息管理委托人能够访问和审查其个人信息管理，并处理个人信息管理委托人提出的任何投诉(见第A.10 条 ）；
- 为满足法律或监管要求而采取的其他组织措施；
- 授权PII 控制者对PII 处理者的场所进行审计；
- 在出现数据泄露、未经授权的处理或其他违反合同条款和条件的情况时的报告义务，包括确定双方的联系点；
- PII 控制器向PII 处理器发出指令的方法；
- 合同终止时适用的措施，特别是在安全删除PII 或归还PII 和物理介质方面。

PII 控制人应确保其PII 处理人员在未经PII 控制人事先批准的情况下，不得再将处理工作分包出去(即使用次级处理人员)。 PII 控制者应遵守这方面的所有相关法律和法规。

PII 控制者应确保其PII 处理者不会出于合同或其他法律协议规定以外的目的处理PII。

PII 控制者应确保其PI 处理人员按照PII 控制者的政策或其他指示(如具体的机构要求)安全地处置PII。

### 15.1.3 解决供应商协议中的安全问题

控制项15.1.2和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

### 15.1.4 信息和通信技术供应链

控制项15.1.3和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

## 15.2 供应商服务交付管理

### 15.2.1 导 言

ISO/IEC 27002:2013第15.2节规定的目标适用。

### 15.2.2 监测和审查供应商服务

控制项15.2.1和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

### 15.2.3 管理供应商服务的变更

控制项15.2.2和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

# 16 信息安全事件管理

## 16.1 信息安全事件的管理和改进

### 16.1.1 导 言

ISO/IEC27002:2013 第16.1节规定的目标适用。

### 16.1.2 责任和程序

ISO/IEC 27002中规定的控制项16.1.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

各组织应有能力(并准备好)对隐私事件做出有组织、有效的反应。因此，各组织应制定并实施隐私事件应对计划。

组织隐私事件响应计划应包括

a) 隐私事件的定义和隐私事件响应的范围；
b) 建立一个跨职能的隐私事件应对小组，负责制定、实施、测试、执行和审查隐私事件应对计划（该计划应由组织内的高级管理层批准)；
c) 明确界定隐私事件应对小组所有成员的角色、责任和权限；
d) 明确在发生跨境事件时与外部组织(国家和国际)合作的法律依据的程序；
e) 制定程序，确保所有受内部隐私政策约束的个人(如员工、承包商)根据组织的事件管理指示，及时向信息安全官员和PII 保护负责人(有时称为CPO) 报告任何隐私事件；
f) 事件影响评估(任务)，以确定对受影响的个人(如尴尬、不便或不公平)或组织造成的任何潜在或实际伤害的性质和程度；
g) 确定需要采取哪些措施来减轻上述危害并降低其再次发生的可能性；以及
h) 确定是否需要向受影响的个人和其他指定实体(如监管机构)发出通知的程序、发出通知的时间和通知的形式，以及在适当情况下发出通知的程序。

各组织可选择将隐私事件响应计划与安全事件响应计划整合，或将两者分开。作为信息安全事件管理流程的一部分，信息安全事件应触发PII 控制者进行审查，以确定是否发生了涉及PII 的数据泄露事件。

信息安全事件可能不会触发此类审查。信息安全事件可能包括但不限于对防火墙或边缘服务器的ping 和其他广播攻击、端口扫描、不成功的登录尝试、拒绝服务攻击和数据包嗅探。信息安全事件不一定会导致PII 或处理PII 的设备或设施可能或实际受损。

### 16.1.3　报告信息安全事件

ISO/IEC 27002中规定的控制项16.1.2和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

当PII 受到损害时，如果不立即采取措施，PII 委托人的权益就无法得到保护。

司法管辖区可能会对涉及PII 的安全事件(如未经授权的处理、违规)的报告或通知提出具体要求(如在法律或法规中)。当发生与PII 相关的安全事故时，应尽快将事故详情，包括组织建议的应对措施(其披露可能会受到某些限制)通知相关当局。这些机构可能包括数据保护机构、执法机构和受事件影响的个人。

如果发生了隐私泄露事件，各组织应向受影响的PII 委托人提供适当有效的补救措施，如更正或删除不正确的信息。

### 16.1.4　报告安全漏洞

ISO/IEC27002 中规定的控制项16.1.3和相关实施指南及其他信息适用。

### 16.1.5　评估信息安全事件并做出决定

ISO/IEC27002 中规定的控制项16.1.4和相关实施指南及其他信息适用。

### 16.1.6　应对信息安全事件

ISO/IEC27002 中规定的控制项16.1.5和相关实施指南及其他信息适用。

### 16.1.7　从信息安全事件中学习

ISO/IEC27002 中规定的控制项16.1.6和相关实施指南及其他信息适用。

### 16.1.8　收集证据

ISO/IEC27002 中规定的控制项16.1.7和相关实施指南及其他信息适用。

## 17　　业务连续性管理的信息安全方面

### 17.1　　信息安全的连续性

#### 17.1.1　导 言

ISO/IEC27002:2013 第17.1节规定的目标适用。

#### 17.1.2　规划信息安全的连续性

ISO/IEC27002 中规定的控制项17.1.1和相关实施指南及其他信息适用。

#### 17.1.3　落实信息安全的连续性

控制项17.1.2和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

#### 17.1.4　核实、审查和评估信息安全的连续性

ISO/IEC27002 中规定的控制项17.1.3和相关实施指南及其他信息适用。

### 17.2　　裁 员

#### 17.2.1　导言

ISO/IEC27002:2013 第17.2节规定的目标适用。

#### 17.2.2　信息处理设施的可用性

ISO/IEC27002 中规定的控制项17.2.1和相关实施指南及其他信息适用。

# 18 合规性

## 18.1 遵守法律和合同要求

### 18.1.1 导言

ISO/IEC27002:2013 第18.1节规定的目标适用。

### 18.1.2 确定适用的立法和合同要求

ISO/EC 27002中规定的控制项18.1.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

各组织应确定其应遵守的与PII 保护有关的法律法规。如果确定了这些法律法规，组织就应针对这些要求采取必要的措施。以下案例就是此类要求的例子。

a) 如果需要对某些类别的PII（如国家识别码、护照号码或信用卡号码）提供额外保护，则应使用加密等加密技术。应考虑所需加密算法的类型、强度和质量。只能从核准算法清单中选择加密算法。

   10.1.2中规定了与此要求相关的安全控制。

b) 司法管辖区可对包括PII 在内的信息规定最低数据备份频率，以及最低备份和恢复程序审查频率。

   12.3.2中规定了与此要求相关的安全控制。

各组织应制定PIA 并实施由此产生的隐私处理计划，以帮助确保与PII 处理相关的计划和服务符合隐私保护要求 。ISO/IEC 29134提供了进一步的指导。

各组织应制定审计计划，以帮助核实PII 处理过程是否符合相关的隐私保护要求。该计划应明确规定进行审计的频率 。

审计可由组织进行(如通过内部审计部门),也可由合格的独立第三方进行。

**保护PII的其他信息**

虽然在许多司法管辖区，PII 控制者对确保合规负有最终责任，但所有参与处理PII 的行为者都应采取积极主动的态度，确定法律或其他因素所产生的相关隐私保护要求。

PII控制者与PII 处理者之间的合同提供了确保PII 处理者支持和管理合规性的机制。合同应要求PII 处理程序接受独立审计的合规性，例如通过实施本规范、ISO/IEC27002 和 ISO/IEC27018 中的相关控制措施。

### 18.1.3 知识产权

控制项18.1.2和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

### 18.1.4 保护记录

控制项18.1.3和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

### 18.1.5 隐私和个人身份信息保护

控制项18.1.4和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

### 18.1.6 对加密控制的监管

控制项18.1.5和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

## 18.2 信息安全审查

### 18.2.1 导 言

ISO/IEC 27002:2013第18.2节规定的目标适用。

### 18.2.2 信息安全独立审查

ISO/IEC 27002中规定的控制项18.2.1和相关实施指南及其他信息适用。以下补充指南也同样适用。

**个人信息保护实施指南**

如果由单个相关方进行审计不切实际或可能增加安全风险，组织应在签订合同前向潜在相关方提供独立证据，证明信息安全是按照个人信息安全控制方的政策和程序实施和操作的。只要提供足够的透明度，PII 控制者选择的相关独立审计通常应是一种可接受的方法，以满足利益相关方审查PII 控制者处理操作的兴趣。

### 18.2.3 遵守安全政策和标准

控制项18.2.2和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

### 18.2.4 技术合规性审查

控制项18.2.3和相关实施指南以及ISO/IEC27002 中规定的其他信息适用。

# 附 件A

# 用于保护PII 的扩展控制集

(本附件是本建议书|国际标准的组成部分)。

## A.1 一般情况

本附件提供了新目标、新控制措施和新实施指南的定义，构成了一套扩展控制措施，以满足保护PII的具体要求。

本规范中的指导以ISO 29100:2011中提供的指导为基础，并假定ISO 29100:2011中的指导已得到实施。

第 A.2 条描述了保护PII 的一般政策，而随后的条款则反映了ISO/IEC 29100中描述的隐私原则。

## A.2 使用和保护PII的一般政策

目标：根据业务要求和相关法律法规，为PII保护提供管理指导和支持。

### 控制

参与处理PII 的组织应制定使用和保护PII 的政策。

### 个人信息保护实施指南

隐私政策应包括适当的声明(在单独的隐私政策中或作为现有政策的补充)，说明支持并承诺管理遵守适用的PII 保护立法、合同要求和其他内部政策。

隐私政策和安全政策虽然密切相关，但可能不涉及相同的主题。信息安全政策和隐私政策都应涉及信息的保密性、完整性和可用性，此外，隐私政策还应涉及同意和个人访问等主题。

ISO/IEC 29100为实施隐私框架提供了指导。PII 保护政策应

- 符合本组织的宗旨；
- 对组织收集和处理PII 的情况保持透明；
- 为制定保护PII 的目标提供框架；
- 确定在保护PII 问题上的决策规则；
- 定义隐私风险接受标准(另见ISO/IEC 29134的6.3.1)；
- 包括承诺满足适用的隐私保护要求；
- 包括承诺不断改进；
- 在组织内部传达；以及
- 酌情提供给有关各方。

## A.3 同意和选择

### A.3.1 同意书

目标：让PI 委托人通过行使有意义的、知情的和自由作出的同意，积极参与有关处理其PII的决策过程(法律法规另有规定的除外)。

### 控制

除 非PII 委托人不能自由拒绝同意，或适用法律明确允许在未经委托人同意的情况下处理PII, 否则各组织应为PII 委托人行使有意义的、知情的、明确的和自由给予的同意提供必要的手段。

**个人信息保护实施指南**

各组织应

a) 确定获得PII 委托人同意的实用方法，分析所选实用方法不再可行的情况，必要时确定替代解决方案，以确保在开始任何处理之前获得同意；

b) 在可行和适当的情况下，或在法律要求的情况下，为PII 委托人提供征得同意的途径，以确保在开始任何处理之前征得同意--处理包括收集、存储、更改、检索、咨询、披露、去标识化、匿名化、传播或以其他方式提供、删除或销毁PII;

c) 在法定代理人(如代表儿童或无法律行为能力者)表示同意的情况下，保存同意记录；

d) 必要时，告知PII 委托人向第三方转移PII 的所有情况，并提供适当的方式让PII 委托人同意这种转移；

e) 在可行和适当的情况下，或在法律要求的情况下，在对以前收集的个人信息进行任何新的使用或披露之前，征得个人信息当事人的同意，并确保在开始任何进一步处理之前征得同意；

f) 确保以知情、透明的方式获得有关处理目的的同意，并确保获得同意是出于特定目的；

g) 通过更新公告等方式提高认识和征得同意；

h) 为 PII 委托人提供修改其同意范围的机制--对同意的任何修改都应及时采取行动，并根据修改后的同意修改或停止处理；

i) 确保同意符合所有适用的法律要求，包括在适当情况下对敏感PII 的明确同意要求；

j) 在适当的情况下，允许默示同意，即PII 委托人已明确了解处理情况且未提出反对，因为这种行为可能表示同意；

k) 在执行所有处理操作之前，事先通知；以及

1) 必要时，确认PII 委托人或PII 委托人授权代理人的身份，提交处理同意书--为核实而要求提供的信息应保持在该目的所必需的最低限度，保留时间应仅限于该目的所必需的时间，不再需要时应安全处置。

**保护PII的其他信息**

在遵守适用法律的前提下，组织应通过选择同意或默示同意的方式获得同意。选择同意是首选方法，但并非总是可行。选择同意要求PII 委托人采取肯定行动，允许组织收集或使用PII。如果使用电子媒体收集同意，组织应确定是简单选择进入合适，还是需要双重选择进入。

有了退出机制，企业就可以假定PII 委托人已默示同意处理其PII，除 非PII 委托人采取肯定行动表示不同意。默示同意通常是根据个人的行为或不行为或其特定情况推断出来的。默示同意的例子：客户向在线零售商提供送货地址，零售商将该信息严格用于交付客户购买的商品。

各组织应提供切实可行的方法，以便在收集国家身份证号码(如社会保险号码、居民登记号码、护照号码)时 单独征得PII 委托人的同意。

例如，各组织可以提供PII 委托人的逐项选择，让他们选择是否希望以各种目的中的任何一种目的与他们联系。在这种情况下，组织要建立同意机制，确保组织的运作尽可能符合PII 委托人的选择。

根据适用的监管要求和实际情况，同意书可以是电子版或打印版。

如果PI 已转移到其他组织或从其他组织转移过来，各组织应建立更新记录的程序，以反映PII 委托人所做的内容更新和同意变更(如修改、撤销)，并确保将这些更新/变更传递给与之共享PII 的组织。只应向PII 委托人收集确保更新正确记录所需的最低信息量，并与其他组织共享。各组织应定期审查其流程，以确保没有不必要的PII 被处理。

### A.3.2 选择

目标：在适当和可行的情况下，向PII 委托人提供不允许处理其PII、拒绝或撤销同意或反对特定类型处理的选择，并向PII委托人解释同意或拒绝同意的影响。

**控制**

各组织应为PII 委托人提供清晰、醒目、易懂、方便和负担得起的机制，使其能够就其PII 的处理行使选择权，除非PII 委托人不能自由拒绝同意，或适用法律明确允许在未经PII 委托人同意的情况下处理PII。

**个人信息保护实施指南**

各组织应

a) 确保PII 委托人在处理其PII 之前可以行使选择权；

b) 如果PII 委托人拒绝提供与服务无关的PII，则不得拒绝为其提供服务。

c) 在相关法律法规有规定的情况下，确定将采取的切实可行的手段，使PII 委托人能够行使其反对处理其PII 的权利--应向PII 委托人提供多种行使这一权利的手段(如邮寄、电子邮件、电话)；

d) 在适用法律或组织政策规定的时限内确认反对声明；

e) 分析所选择的实用方法不再适用的情况，并在必要时确定备用解决方案，以便PII 委托人能够继续及时行使其反对权；

f) 确保PII 的分类、标记和存储方式有利于行使反对权，并确保PII 委托人能够及时、无偿地行使反对权；

g) 确认提交反对处理意见的PII 委托人或PII 委托人授权代理人的身份--为核实而要求提供的信息应保持在该目的所需的最低限度，保留时间应仅限于该目的所需的必要时间，并应在不再需要时安全处置；

h) 如果行使反对权需要法律依据，则应确保行使反对权的PII 委托人提供合理的反对理由--任何拒绝接受反对的行为都应详细说明PII 控制人认为这些理由不合法的原因；

i) 确保与之共享个人信息的所有组织都了解个人信息委托人提出的任何反对意见，并确保这些组织遵守任何有效的反对意见；以及

j) 在可能的情况下，让PII 委托人有能力反对PII 处理的某些方面，而不是必须接受或反对整个处理过程。

保护PII的其他信息

在许多情况下，根据适用法律的不同，在收集公开信息时提供选择机制可能没有必要或不可行。例如，在从公共记录或报纸上收集PII 委托人的姓名和地址时，就没有必要提供一种机制来让委托人作出选择。

## A.4 目的的合法性和规范性

### A.4.1 目的合法性

目的：确保处理PII 的目的符合适用法律，并以允许的法律依据为依据。

**控制**

各组织应采取适当措施，确保PII 处理符合适用法律，并以允许的法律依据为基础。

各组织应

a) 确定建议的处理是否可以基于同意以外的法律依据(如执法、公共安全、法律义务或PII 控制者的合法权益)进行;

b) 确定拟议的处理是否受法律依据(如执法、公共安全或法律义务)的制约，禁止PII 委托人就其PII 的处理行使选择权;

注--如果在国际范围内收集或处理PII, 那么在不同的适用法律框架下，同意的必要性和正确的处理方式可能会有所不同。

c) 确定允许处理个人隐私信息的法律依据(理由),无论是一般性的还是支持特定计划或信息系统的；以及

d) 纳入相关程序，确保信息处理符合所有适用的法规和主管当局对法规的解释。在确定处理目的的合法性时，应考虑处理的总体背景。这包括PII 控制者与PII 委托人之间基本关系的性质、科技发展以及社会和文化态度的变化。

各组织应制定程序，确保在处理PII 时不会违反或可能违反任何法律义务，包括法律规定、普通法或合同条款 。

如果组织设有职代会或工会，适用法律可能会要求在确定雇员的目的合法性时与这些机构进行协商。

计划官员应就任何计划或活动是否有权收集PII 的问题与负责保护PII 的个人(有时称为CPO) 或同等人员以及法律顾问进行协商。收集PII 的权限应记录在案。

### A.4.2 用途说明

目的：最迟在收集PII 时明确规定收集PII 的目的，并将随后的使用限制在实现最初目的的范围内。

**控制**

各组织应将收集PII 的目的和处理PII 的目的告知PII 委托人。此类沟通应在收集PII 之时或之前进行，并在处理 PII 用于任何事先未告知PII 委托人的目的之前进行。

**个人信息保护实施指南**

各组织应在收集信息或首次将信息用于新的目的之前，将目的告知PII 委托人，使用既清楚又适合具体情况的语言来说明目的，并充分解释处理敏感PII 的必要性。

通常，法律条文会明确授权收集和使用特定的PII。如果法律条文写得很宽泛，因此可以进行解释，那么组织应与CPO 和法律顾问协商，确保一般性授权与任何特定的PII 收集之间有明确的联系。

一旦确定了具体目的，就应在相关的隐私合规文件或组织用于收集PII 的表格中明确说明这些目的。此外，为避免未经授权收集或使用PII, 处 理PII 的人员应接受有关组织收集权限的培训。

各组织应

a) 确定仅对每个业务流程有用的PII;

b) 以逻辑方式分离对每个流程有用的PII;

c) 根据业务流程(包括薪资管理、休假申请管理和职业晋升)管理不同的访问权限，并为处理最敏感的PII 的系统建立专门的IT 环境；以及

d) 定期确认个人识别信息是否被有效分离，是否增加了接收者和相互联系。

## A.5 收集限制

| |
|---|
| 目的：将收集的PII 限制在适用法律的范围内，并严格限于特定目的所需的范围内。 |

### 控制

各组织应采取适当措施，将收集的PII 类型和数量限制在用于通知中所述目的的最低限度(见A.9.1)，并限制在适用法律和法规的范围内。

### 个人信息保护实施指南

各组织应

a) 将收集的PII 限制在为通知中所述目的(见A.9.1) 所确定的最低要素范围内，且PII 委托人已对此表示同意；

b) 不收集敏感的PII，除非收集敏感的PII 得到法律授权或征得同意；以及

c) 限制间接(如通过网络日志、系统日志)从PII 委托人处收集的信息量或关于PII 委托人的信息量。

各组织应明确处理PII的目的，确定实现该目的所需的PII，确定不需要收集的信息，并确认只收集必要的信息。

各组织在着手收集之前，应仔细考虑需要收集哪些PII 以实现特定目的。各组织不应不加区分地收集PII。

各组织应定期审查收集PI 的目的，确保其仍然有效。它们还应定期审查所收集的PII，以确保这些PII 仍是达到目的所必需的最低限度的信息。

组织不应收集敏感的PII，如国民身份证号码，除非收集此类信息已获得法律授权或明确同意。

### 保护PII的其他信息

某些司法管辖区可能会将某些类别的PII（如种族出身、政治观点或宗教或其他信仰、有关健康、性生活或刑事定罪的个人资料等)定义为敏感信息。这些司法管辖区可能会对收集这类PII 施加限制或规定条件，组织在决定收集哪些PII 时应考虑到这些限制和条件。

## A.6 数据最小化

| |
|---|
| 目的：将处理的PII 减少到PII 控制者所追求的合法利益所严格需要的程度，并将PII 的披露对象限制在最低数量的隐私利益相关者。 |

### 控制

各组织应采取适当措施，尽量减少所处理的PII 数量，以满足PII 控制者合法利益的严格需要(例如，某组织可能会设法增加或扩展其业务运营，从而合法地增加其处理和存储的PII 数量)。

### 个人信息保护实施指南

各组织应

a) 确保采用"有必要知道"的原则，即只允许个人在处理PII 的合法目的框架内，为执行公务而接触必要的PII;

b) 尽可能使用或提供不涉及识别PII 委托人身份的互动和交易作为默认选项；

c) 限制所收集的PII 的可链接性；

d) 对机构保留的PII 进行初步评估，并制定和遵循定期审查计划，以确保只收集通知中确定的PII, 而且这些PII 仍然是实现当前业务目的所必需的；

e) 将包含个人隐私信息的电子文件的传输限制在与工作有关的最低利益相关者范围内；

f) 根据上下文、PII 的存储形式(如数据库字段或文本摘录)和确定的风险，确定哪些PII 应匿名或去标识化；

g) 根据需要去标识化的数据形式(如数据库和文本记录)和确定的风险，去标识化需要去标识化的数据；

h) 在处理个人信息的目的已过期、没有法律要求保留个人信息或实际可行的情况下，删除和处置个人信息；以及

i) 考虑是否可以使用隐私增强技术(PET) 以及使用哪种技术。

支持特定组织业务流程所需的最小PII 要素集可能是该组织获准收集的PII 的子集。

收集的PII 应分为必填PII 和选填PII。各机构应只收集提供服务所需的强制性PII, 并在收集可选PII 时征得PII 委托人的适当同意。当PII 委托人拒绝提供可选PII 时，组织不应拒绝提供服务。

首席采购干事和法律顾问应要求计划官员说明拟议处理PII 的理由，以确保这是信息系统或活动实现法律授权目的所必需的最低限度。

注1--根据ISO/EC29100 的定义，匿名化是指对PII 进行不可逆转的更改，使PI 主体无法再被PII 控制者单独或与任何其他方合作直接或间接识别的过程。这一过程必然涉及(不可逆转的)信息丢失。在某些情况下，只需删除部分数据即可达到预期目的。

注2- 根据ISO/EC 29100中的隐私权原则，计划在今后的国际标准中对提高隐私权的数据去标识化技术进行说明，用于描述和设计去标识化措施。一般来说，为了断定去标识化过程符合法律规定，去标识化的方法包括删除或归纳属性，以及强有力的组织和技术措施。

注3-在为某一 目的处理PII 时，应尽量减少处理PI 的范围，以便只为预期目的服务，而不泄露有关当事人的过多信息，例如，如果需要交通相关调查的受访者的地理区域，可考虑只收集附近的地标而不是精确地址。

注4-在分析匿名数据时，当输出的数据集较小时，PII 委托人的身份往往会暴露。因此，好的做法是在记录数少于阀值数(如10条记录)时防止输出。需要根据数据分布模式仔细确定阈值。

各组织应酌情减少其PII 库存，从而降低隐私和安全风险。各机构应对其持有的PII 进行初步审查和后续审查，以在最大程度上确保此类数据堆栈的准确性、相关性、及时性和完整性。

还应指导各组织将其持有的PII 减少到适当实现记录在案的组织业务目的所需的最低限度。各组织应制定并公布对其数据堆栈进行定期审查的时间表，以补充初次审查。

通过定期评估，各组织可以降低风险，确保只收集通知中规定的数据，并确保所收集的数据仍然相关和必要。

## A.7 使用、保留和披露限制

### A.7.1 使用、保留和披露限制

目的：将PI 的使用和披露限制在特定、明确和合法的目的范围内，保留PII 的时间不得超过实现所述目的或遵守适用法律所必需的时间。

**控制**

各组织应采取适当措施，将PII 的处理限制在合法和预期目的范围内，并仅在实现所述目的或遵守适用法律所必需的时间内保留PII。

**个人信息保护实施指南**

各组织应

a) 将 PII 的使用、保留和披露(包括转让)限制在为实现特定、明确和合法目的所必需的范围内；以及

b) 对信息系统进行配置，以记录收集、创建或更新PII 的日期，以及根据经批准的记录保留时间表删除或存档PII 的日期。

**保护PII 的使用实施指南**

各组织应

a) 当所述目的已过期但适用法律要求保留时，锁定(即存档、保护和免于进一步处理)任何PII;

b) 使用适当的技术或方法确保安全删除或销毁PII（包括原件、副本和存档记录)；

c) 仅 将PI 用于收集前或收集时与PII 委托人商定或向其披露的目的，并在必要时，在为任何新目的进行处理之前征得其同意；

d) 限制外部人员访问组织系统和个人隐私信息，仅限于绝对必要且已获得正式授权的访问权限--如果访问权限确实是业务所必需的，则应遵循适当的审批程序；

e) 确认获准与组织系统连接的外部系统在获准连接前已实施适当的保障措施；

f) 定期审查第三方实施的保障措施，确保其继续满足组织的安全要求-如果审查发现保障措施不充分，则应切断第三方与组织的联系，直至第三方证明已恢复充分的保障措施；

g) 当通过远程接口访问个人信息安全时，实施适当的访问认证机制-需要记录访问个人信息安全的日志；以及

h) 发出通知，告知公众在安全监控过程中收集的PII 持有量的任何变化。

**关于保留个人信息的实施指南**

在某些情况下，保留PII 的法律要求可能会导致保留的PII 超出特定业务目的的需要。

各组织应

a) 仅在授权期限内保留PII, 以满足通知中确定的目的或法律和组织的要求，并在保留期满后立即删除PII;

b) 如果出于特定业务目的需要保留PII 的时间超过所需的时间，则采取去标识化等措施保护PII;

c) 确定有时间限制且与处理目的相适应的PII 保留期；

d) 确认信息系统能够检测到保存期限的到期；

e) 确保执行商定的保留期限，并根据保留期限处置PII;

f) 开发一种自动功能，在PII 保存期限到期时将其删除--应立即删除或在可行的情况下尽快删除；

g) 根据上下文、PII 的存储形式(包括数据库字段或文本摘录)和确定的风险，确定哪些信息应去掉标识；

h) 根据需要去标识化的数据形式(包括数据库和文本记录)和确定的风险，去标识化需要去标识化的数据；以及

i) 如果无法去除个人隐私数据的身份标识，则选择工具(包括部分删除、散列、密钥散列和索引)来保护个人隐私数据。

**关于披露个人信息以保护个人隐私的实施指南**

各组织应

a) 未 经PII 委托人事先知晓和同意，不得向外部各方披露PII, 除非相关法律允许披露-如果披露对象是有必要了解情况的内部各方(如员工)，则可能不需要PII 委托人知晓和同意；以及

b) 在传输PII 时提供强有力的保护机制，包括数据加密和完整性保护。

员工PII的处置(即安全删除或存档)应符合适用的法律法规，并符合组织处置政策，在适当情况下还应征得员工同意 。

### A.7.2 安全清除临时文件

| |
|---|
| 目的提供在特定期限内删除临时文件的技术措施。 |

**控制**

可能包含PII 的临时文件和文档应在规定的、有记录的期限内进行处置。

**个人信息保护实施指南**

信息系统在正常运行过程中可能会创建包含PII 的临时文件。此类文件与系统和应用程序有关，但可能包括具有回滚功能的文件系统，以及与数据库更新和其他应用软件操作有关的临时文件。在相关信息处理任务完成后，通常不再需要临时文件，但在某些情况下，临时文件可能不会被自动删除。这些文件的使用时间并不总是确定的，但"垃圾收集"程序应能识别相关的临时文件，并确定它们上次被使用的时间。

PII 处理信息系统应实施定期检查，确保删除超过规定年限的未使用临时文件。

### A.7.3 PII 披露通知

| |
|---|
| 目标：确保PII 处理者将任何具有法律约束力的PII 披露要求通知PII 控制者。 |

**控制**

PII控制者与PII 处理者之间的合同应要求PI 处理者按照合同中约定的任何程序和期限，将执法部门或其他机构提出的任何具有法律约束力的披露PII 的要求通知PII 控制者，除非法律禁止此类披露。

**个人信息保护实施指南**

各组织应采取措施(如合同义务)确保

a) 除非法律另行禁止，否则PII 处理者在接受任何具有法律约束力的 PII 披露请求之前，应咨询相关的PII 控制者；以及

b) 经相关PII 控制者授权，PII 处理者接受任何合同约定的PII 披露请求，除非法律另行禁止。

### A.7.4 记 录PII 的披露

| |
|---|
| 目标：确保记录向第三方披露PII 的情况。 |

**控制**

应记录向第三方披露PII 的情况，包括披露了哪些PII、向谁披露、何时披露以及披露的目的。

**个人信息保护实施指南**

在正常操作过程中可能会披露PII。这些披露都应记录在案。向第三方披露的任何其他信息，例如因合法调查或外部审计而披露的信息，也应记录在案。记录应包括披露信息的来源和披露授权的来源。

### A.7.5 分 包PII 处理的披露

目标：确保PII 处理者向PII 控制者披露分包商的任何使用情况。

#### 控制

PII 处理者使用分包商处理PII 时，应事先向PII 控制者披露。

#### 个人信息保护实施指南

PII 处理者与PII 控制者之间的合同中应明确规定使用分包商处理PII 的条款。合同应明确规定，只有在事先获得PII 控制者授权的情况下才能委托分包商。PII 处理者应及时向PII 控制者通报这方面的任何预期变动，以便PII 控制者能够反对这种变动或终止同意。

披露的信息应包括使用分包的事实和相关分包商的名称，但不包括任何具体业务细节。披露的信息还应包括分包商可能在哪些国家处理数据，以及分包商有义务履行或超越PII 处理商义务的方式。

如果公开披露分包商信息会增加安全风险，超出可接受的限度，则应根据保密协议或PII 控制人的要求进行披露。应让PII 控制员知道可以获得正在使用的分包商的信息。

## A.8 准确性和质量

目标：确保所处理的PII 准确、完整、及时、充分且与使用目的相关。

#### 控制

各组织应采取适当措施，确保直接或间接从PII 委托人处收集的PII 具有适当的质量。

#### 个人信息保护实施指南

实现数据质量意味着所处理的PII 准确、足够精确、完整、最新、充分且与使用目的相关。

各组织应

a) 建立有助于确保准确性和质量的PII 收集程序；

b) 收 集PII 的方式应确保在PII 离开权威来源后还能检测到任何修改；

c) 在收集或创建PII 时，尽最大可能确认PII 的准确性、相关性、及时性和完整性；

d) 在处理从PII 委托人以外的来源收集的PII 之前，确保其可靠性；

e) 在适当的情况下，在对PII 进行任何修改之前，通过适当的方式核实PII 委托人提出的修改要求的有效性和正确性；

f) 定期检查并在必要时纠正其程序或系统使用的任何不准确或过时的PII; 以 及

g） 发布指导方针，确保并最大限度地提高所传播信息的准确性、完整性、充分性和相关性。各组织应采取合理措施，确认PII 的准确性。例如，这些步骤可包括在收集地址或使用自动地址验证查询应用编程接口(API) 将地址输入信息系统时对其进行编辑和验证。

当PII 具有足够的敏感性时(例如，当它用于每年重新确认纳税人的收入以获得经常性福利时)，各组织应在信息系统中纳入相关机制，并制定相应的程序，规定信息更新的频率和方法。

为尽量减少数据不准确的可能性，应尽可能由PII 委托人直接将PII 输入信息系统，而无需由他人抄录数据。不过，如果需要转录

在不可避免的情况下，企业应考虑让PII 委托人验证转录的PII。这有助于在处理不准确的PII 造成任何后果之前纠正错误。

**保 护PII 的其他信息**

为保护数据质量而采取的措施类型可根据PII 的性质和背景、使用方式以及获取方式而定。为验证任何敏感PII 的准确性而采取的措施应比用于验证不太敏感的PII 的措施更加全面。对于从PII 委托人或PII 委托人授权代表以外的来源获得的PII，可能还需要采取其他步骤进行验证。

## A.9 公开、透明和通知

### A.9.1 隐私声明

目标：确保隐私声明包含适当程度的详细信息，以通俗易懂的语言撰写，并易于获取。

**控制**

各组织应采取适当措施，向PII 委托人提供有关PII 处理目的的适当通知。

**个人信息保护实施指南**

各组织应

a) 就以下方面向PII 校长发出有效通知：

1) 其影响隐私的活动，包括但不限于收集、使用、共享、保护和安全处置PII、

2) 收集PII 的权力、

3) PII 委托人在组织如何使用PII 方面的选择（如果有的话），以及行使或不行使这些选择的后果，以及

4) 反对处理的能力；

b) 提供符合业务需要的通知和同意机制；

c) 在变更前或变更后尽快修订通知，以反映影响PII的做法或政策的变更，或影响隐私的活动的变更；

d) 根 据PII 的性质、为提供通知而选择的实用方法以及PII 控制者和PII 委托人之间关系的性质，确保通知内容完整并适合目标受众；

e) 以清晰的方式提供信息，让不熟悉信息技术、互联网或法律术语的人也能理解；

f) 确保在收集PII 之前或之时发出通知；

g) 确保在未发出通知的情况下无法收集PII;

h) 在实际手段不再可行的情况下，确定替代解决方案；

i) 如有可能，提供证明已发出通知的方法；

j) 在以实物方式提供隐私通知的情况下，将此信息张贴在PII 委托人应该看到的标志上，或要求在通知或文件上签名或草签；以及

k) 制定政策，提供必要的标签和标志，让PII 负责人了解相关技术的使用情况[即闭路电视(CCTV)系 统 、WiFi 和无线射频识别(RFID)]。

在可能的情况下，通知应在收集点（如组织的网站或实体场所）的显著位置发布，无需PII 委托人特别要求。

### A.9.2 公开和透明

| |
|---|
| 目的：为PII 委托人提供关于PII 控制者处理PII 的政策、程序和做法的清晰易懂的信息。 |

**控制**

各组织应采取适当措施，向PII 委托人提供有关其处理PII 的政策、程序和做法的适当信息。

**个人信息保护实施指南**

各组织应

a) 向 PII 委托人提供关于PII 控制者处理PII 的政策、程序和做法的清晰易懂的信息；

b) 披 露PII 控制者向PII 委托人提供的选择和途径，以限制对其信息的处理，以及访问、更正和删除其信息。

此外，各组织还应说明

a) 机构收集的PII 及其目的；

b) 组织如何在内部使用PII;

c) 机构是否与外部实体共享PII、这些实体的类别以及共享的目的、

d)PII 委托人是否能够同意特定用途或共享PII,以及如何行使此类同意权；

e) PII 将保留多长时间；

f) 机构是否转售或转发数据供数据分析机构处理，以及适用于PII 风险的详细信息；

g)PII 委托人如何获取PII, 以便酌情对其进行修改或更正；

h) 关于如何保护PII 的适当信息；

i) 确 保PII 委托人能获取有关其隐私活动的信息，并能与其CPO 沟通；

j) 在收到请求时，提供与已经或可能已经导致请求人个人信息资料隐私泄露的隐私泄露事件相关的信息，以及请求人可以采取的任何相关行动，以降低泄露事件带来的额外风险。

各组织还应采用不同机制向公众通报其隐私保护措施，包括但不限于PIA 报告、隐私报告、公开网页、电子邮件发布、博客和定期出版物(如季度通讯)。各组织还应采用面向公众的电子邮件地址或电话线路，使公众能够提供反馈意见或直接向隐私办公室提出有关隐私惯例的问题。

## A.10 PII 校长参与和访问

### A.10.1 PII 校长访问

| |
|---|
| 目标：让PII 委托人能够访问和审查其PII, 并对其准确性和完整性提出质疑。 |

**控制**

各组织应采取适当措施，使PII 委托人能够查阅自己的PII, 并获得PII 的更正或删除。

**个人信息保护实施指南**

各组织应

a) 确定允许PII 委托人行使其访问权(在适用法律允许的情况下)的实际手段。个人应能及时行使这一权利，行使的方式应是PII 委托人可以理解和使用的，并与最初收集PII 时使用的方式(如普通邮件或电子邮件)类似;

b) 分析所选实用工具不再适用的情况，并在必要时确定备用解决方案;

c) 让 PII 委托人能够访问机构所持有的其PII，以评估其准确性并在必要时要求更正;

d) 应尽可能以与提出申请时相同的形式提供答复(例如，如果申请是通过普通邮件提出的，答复也应通过普通邮件提供);

e) 公布有关PII 委托人如何申请查阅其系统中保存的记录的规则和条例;

f) 允 许PII 委托人直接或间接质疑PII 的准确性和完整性，并根据具体情况酌情修改、更正或删除;

g) 制定程序，使PII 委托人能够以简单、快捷和高效的方式行使这些权利，而不致造成不当延误(例如，应根据适用的法律法规或组织政策的规定作出答复)或产生费用;

h) 建立一个程序，通知提交申请的PII 委托人其申请的状态和必要的处理过程(例如，通过邮寄邮件或电子邮件，说明已经收到申请，以及预计收到答复的日期)--就储存档案而言，如果PII 控制者通知提交申请的PII 委托人处理申请的时间范围，并提供了合理的答复时间，那么在答复日期方面可能会有一些余地;

i) 在法律允许的范围内，确保始终可以行使访问权;

j) 确保只有与信息相关的个人或该个人的授权代理人才能访问PII--这可能要求申请访问的个人以令人满意的方式进行身份识别和认证--适用法律或法规可能会对此类身份识别和认证要求做出规定;

k) 在需要对申请者进行身份识别和认证的情况下，除非法律法规另有规定，否则应确定适当的身份识别和认证形式--各组织应只要求提供确保正确识别所需的最低限度的信息--这些信息应妥善保管，并仅在必要时予以保留;

l) 确 保PII 只发送给相关的PII 委托人，并以安全的方式发送;

m) 确保能够提供PII 委托人可能要求的所有信息，同时仍然保护其他PII 委托人的PII;

n) 在某些司法管辖区的法律可能允许的情况下，在隐私通知中告知是否打算对访问收取任何费用;以及

o) 要求任何PII 处理者支持PII 控制者为PII 委托人行使访问、更正或删除其数据的权利提供便利。

访问权限使PII 委托人能够审查组织记录系统中保存的有关他们的PII。访问包括及时、简化和低成本地访问数据。允许访问记录的组织流程可能因资源、法律要求或其他因素而有所不同。

### A.10.2 补救和参与

目的：向PII 处理人和个人数据已披露给他们的第三方提供任何修改、更正或删除。

**控制**

除非相关法律或法规禁止，否则组织应采取适当措施，让PII 委托人能够更正、修改或删除组织保存的PII。组织还应建立一种机制，将任何更正、修改或删除通知PII 处理人，并尽可能通知已向其披露PII 的第三方。

**个人信息保护实施指南**

各组织应

a) 确保校长可以随时行使纠正权；

b) 分析所选实用工具不再适用的情况，并在必要时确定备用解决方案；

c) 在相关法律法规允许的范围内，确保PII 委托人能够行使其更正权；

d) 确保所要求更正的准确性；

e) 确保提交申请的PII 委托人得到确认；

f) 确保将所做的更正告知可能收到个人信息的第三方；以及

g) 只允许PII 委托人访问他们需要更正、修改和删除的PII。

### A.10.3 投诉管理

目标：建立有效的内部投诉处理和补救程序，供PII 负责人使用。

#### 控制

各组织应采取适当措施，有效处理PII 委托人提出的投诉。

#### 个人信息保护实施指南

各组织应实施投诉管理流程，并保留一个联络点，负责接收和回复PII 委托人对组织隐私惯例的投诉、疑虑或问题 。

各组织应提供以下投诉机制：PII 负责人可随时使用，包括成功投诉所需的所有信息(包括首席采购干事或其他被指定接受投诉的官员的联系信息)，并且易于使用。

组织投诉管理流程应包括跟踪机制，以确保及时审查和适当处理收到的所有投诉。投诉管理还应包括由投诉引发的纠正行动。

#### 保护PII的其他信息

PII 负责人的投诉、担忧和问题可以作为宝贵的外部意见来源，最终改进运营模式、技术使用、数据处理方法以及隐私和安全保障措施。

## A. 11 问责制

### A.11.1 管理

目标：建立有效的PII 处理管理机制。

#### 控制

各组织应采取适当措施，建立与PII 处理相关的有效管理。

#### 个人信息保护实施指南

各组织应

a) 指定专人负责制定、实施和维护全组织范围的治理和隐私计划，以确保遵守有关程序和信息系统处理个人信息学资料的所有适用法律和法规--可将指定人员指定为首席采购干事--作为另一种选择，可由董事会的一名专职成员承担责任，并由一名可能分包的专职工作人员提供支持；

b) 确保指定人员具备监督PII 处理工作所需的专业知识；

c) 确保指定人员参与所有与保护个人信息安全有关的问题，并能及时直接向高级管理层报告；

d) 为指定人员提供执行任务所需的人员、场所、设备和其他资源；

e) 提供一个监测隐私法律和政策变化的程序，以便对PII 保护计划产生影响；

f) 制定、传播和实施可操作的PII 保护政策和程序，对涉及PII 的计划、信息系统或技术的PII 保护和安全控制进行管理；

g) 定期更新PII 保护计划、政策和程序；以及

h) 定期监测机构在保护个人信息安全方面的表现--高级管理代表或董事会成员应负责管理，并了解量化指标、风险和违规情况等方面的信息--虽然这种审查可能是根据需要进行的，但也应定期进行，无需任何触发因素。

## A.11.2 隐私影响评估

目标：建立隐私影响评估程序，并在必要时进行隐私影响评估。

**控制**

如果一个组织正在处理PII，那么该组织就应该制定进行PIA 所需的程序。

**个人信息保护实施指南**

隐私风险评估通常由认真负责并充分对待PII 委托人的机构进行。在某些司法管辖区，为满足法律和监管要求，可能有必要进行PIA 。ISO/IEC 29134可用作PIA 的指南。

在进行隐私风险评估时，各组织应考虑资产、威胁、漏洞和保障措施(现有的和建议的)。各组织应记录

a) PIA 的结果，包括但不限于正在处理的PII;

b) 确定的隐私风险；以及

c) 建议的缓解措施。

## A.11.3 对承包商和个人信息处理者的隐私要求

目标：通过合同或强制内部政策等其他手段，确保第三方接收方提供至少同等水平的PII 保护。

**控制**

各组织应采取适当措施，确保承包商和PII 处理商已实施足够级别的PII 保护。

**个人信息保护实施指南**

各组织应

a) 在服务级别协议中记录PII 处理者必须满足的PII 保护要求；

b) 监督和审计承包商对这些要求的执行情况；

c) 确定承包商和PII 处理者的PII 保护角色和责任；

d) 通过合同确定提供服务的主体和时限，PII 处理者处理PII 的范围、方式和目的，以及所处理的PII类型；

e) 规定在服务完成、任何管理协议终止或应PII 控制者要求时，PII 处理者应归还或安全处置PII 的条件；

f) 包括一项保密条款，该条款对提供商及其任何可能接触到PII 的员工都具有约束力；

g) 确保服务提供商不会将PII 传递给第三方，即使是出于保存目的，除非合同中明确允许；

h) 明确服务提供商在发生任何影响PII 的数据泄露时通知PII 控制者的责任；

i) 在合同中规定，服务提供商应将服务的任何相关变更(如新增功能的实施)通知PII 控制者；以及

j) 酌情记录和传达所有与PII保护相关的政策、程序和做法。

各组织应就可能影响本控制措施实施的适用法律、指令、政策或规定咨询法律顾问、首席采购干事和合同官员。

注--同时执行15.1.2的补充实施指南。

### 保护PII的其他信息

承包商和PI 处理商可能包括但不限于服务局、信息提供商、信息处理商和其他提供信息系统开发、信息技术服务和其他外包应用程序的组织。

## A.11.4 隐 私监控和审计

| |
|---|
| 目标：监测和审计PII 保护控制措施和内部PII 保护政策的有效性。 |

### 控制

各组织应采取适当措施，定期监控和审核隐私控制措施和内部隐私政策的有效性。

### 个人信息保护实施指南

各组织应

a) 定期监控和审计PII 处理操作，尤其是涉及敏感PII 的操作，以确保其符合适用的法律、法规和合同条款；

b) 定期监控和审核PII 保护控制措施和政策，确保其符合适用的法律法规和合同条款；

c) 确保由合格的独立方(组织内部或外部)进行审计；以及

d) 如果使用内部资源进行审计，则定期请外部人员进行审计，以进行独立评估。

## A.11.5 PII 保护意识和培训

| |
|---|
| 目标：为PII 控制人员中接触PII 的人员提供适当的培训，提高他们对保护PII 的认识。 |

### 控制

各组织应采取适当措施，为PII 控制人员提供适当的培训。

### 个人信息保护实施指南

各组织应

a) 实施并维护一项全面的培训和提高认识战略，旨在确保工作人员了解他们的PII 保护责任和程序；

b) 建立机制，让负责保护个人信息安全的人员随时了解监管、合同和技术环境中可能影响组织隐私合规的最新发展；

c) 定期(如每年)或根据需要(如发生事故后)开展以角色为基础的基本和有针对性的PII 保护培训-这对于只是不经常处理PII 的活动尤为重要；以及

d) 确保工作人员定期对接受PII保护要求的责任进行认证(手动或电子认证)。

### A.11.6 PII 保护报告

目标：编制、传播和更新个人信息保护报告。

#### 控制

各组织应编制、酌情分发并更新报告(例如，关于违规、调查、审计的报告),提交给高级管理人员和其他负责 监 督PII 保护的人员，以表明对特定法定和监管PII 保护计划任务的责任。

#### 个人信息保护实施指南

通过外部和内部的PII 保护报告，组织应促进组织PII 保护操作的问责制和透明度。报告还有助于组织确定在满足PII 保护合规要求和PII 保护控制措施方面取得的进展，比较整个组织的绩效，找出政策和实施方面的漏洞和差距，并确定成功模式。

## A.12 信息安全

目标：确保根据风险评估结果适当保护PII。

#### 控制

应根据威胁风险评估或PIA的结果，通过适当的控制措施保护由组织照管和保管的PII。

#### 个人信息保护实施指南

各组织应

a) 在操作、功能和战略层面采取适当的控制措施保护个人信息安全，确保个人信息安全的完整性、保密性和可用性，并在其整个生命周期内防范未经授权的访问、销毁、使用、修改、披露或丢失等风险；

b) 选 择PII 处理者，签订适当的合同，在处理PII 的组织、物理和技术控制方面提供足够的保证，并确保遵守这些控制措施；

c) 根据适用的法律要求、安全标准、ISO 31000中描述的系统安全风险评估结果以及成本效益分析结果来制定安全控制措施；

d) 限制那些需要访问PII 以履行职责的个人访问PII, 并限制这些个人只能访问他们为履行职责而需要访问的PII;

e) 解决通过隐私风险评估和审计过程发现的风险和漏洞；以及

f) 在持续的安全风险管理过程中，对控制措施进行定期审查和重新评估。

某些数据隐私法有时会规定安全要求，在这种情况下，应将这些要求传达给数据安全职能部门，以便实施。

在设计和实施安全控制时应尽职尽责。

## A.13 隐私合规

### A.13.1 合规性

目标：避免违反与隐私相关的法律、法定、监管、隐私政策或合同义务以及任何隐私要求。

#### 控制

各组织应采取适当措施，确保PII 处理符合合规要求。

**个人信息保护实施指南**

各组织应

a) 编制一份年度报告，详细说明现有风险，说明合规情况，包括未采取的行动摘要；以及

b) 遵循定义明确的违规响应流程，在某些司法管辖区，该流程可能包括通知PII 委托人和其他机构（如数据保护机构）的要求。

### A.13.2 某些司法管辖区的跨境数据传输限制

| |
|---|
| 目标：保护跨境传输的PII。 |

**控制**

组织应采取适当措施，确保任何跨境PII 转移都符合相关合规要求。

**个人信息保护实施指南**

当需要将PII 转移到PII 目前所在地区以外的国家时，某些司法管辖区的数据隐私法规可能会施加限制，通常可能是以下一种或多种限制：

a) 通知数据保护机构；

b) 数据保护机构的批准，尤其是敏感数据；

c) 开展适当的尽职调查，确保跨境传输的个人信息安全得到与原籍国同等的保护；以及

d) 实施具体的数据传输文书，如标准合同条款或具有约束力的公司规则(BCR)。

各组织应采取措施，检查特定限制是否适用于任何计划中的转移，并在进行转移前遵守这些限制。

# 参考书目

*BSI 10012,个人信息管理系统规范。*

- *欧盟委员会，数据保留指令(第2006/24/EC 号指令)评估报告，2011年。*
- *ISO/IEC27000:2016, 信息技术--安全技术--信息安全管理系统--概述和词汇。*
- *ISO/IEC27001, 信息技术--安全技术--信息安全管理系统--要求。*
  *ISO/IEC27005, 信息技术--安全技术--信息安全风险管理。*
- *ISO/IEC27009, 信息技术--安全技术--针对特定行业的ISO/IEC27001 应用--要求。*
- *ISO/IEC27018, 信息技术--安全技术--在作为PII 处理程序的公共云中保护个人身份信息(PII) 的操作规范。*

  *ISO/IEC29134, 信息技术--安全技术--隐私影响评估指南。*

- IEC Electropedia。可访问(2017-07-06查看):http://www.electropedia.org/。
- ISO 在线浏览平台。可访问(2017-07-06查看):http://www.iso.org/obp。
- 国际电联术语和定义。可访问(2017-07-07查看):http://www.itu.int/ITU-R/go/terminologv-数据库。
- *KCS, 个人信息管理系统，2011年12月。*
- NIST 特别出版物800-53附录J, 联邦信息系统和组织的安全和隐私控制，2011年7月。
- NIST 特别出版物800-122,《个人身份信息(PII) 保密性保护指南》,2010年4月。

ISO/IEC 29151:2017(E)

**ICS35.030**

价格按39页计算