Q/BJKB

北京坤标检验认证有限公司企业标准

Q/BJKB 005-2026

个人身份信息保护管理体系 基本要求

Personally Identifiable Information Protection - Basic Requirements

2026-4-1 发布　　2026-4-1 实施

北京坤标检验认证有限公司　　发　布

目　　次

前　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 控制者建立个人身份信息保护管理体系提供了基本要求，并在附件中提供了广泛的信息安全和 PII 保护控制措施方面的指导，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。

本标准主体结构(包括条款标题)反映了 ISO/EC 27001 的主体结构。附件包含一套扩展的 PII 保护特定控制措施，对 ISO/IEC 29151 和 ISO/EC27002 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与 ISO/IEC29100 中的隐私政策和 11 项隐私原则相对应。

本标准按 GB/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》给出的规则起草。

本标准主要起草人：陈刚辉、杨英者、吕晚香、李英华。

个人身份信息保护管理体系 基本要求

1 范围

本标准规定了个人身份信息保护管理体系的术语和定义、基本要求等内容。

本标准适用于采用本标准在企业内部建立个人身份信息保护管理体系，也适用于北京坤标检验认证有限公司作为第三方认证机构对企业进行个人身份信息保护管理体系的评价。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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。

ISO/IEC 27000 信息技术-安全技术-信息安全管理体系-概述和词汇

ISO/IEC 29151 信息技术 - 安全技术 - 个人身份信息保护的实践守则

3 术语和定义

下列术语和定义适用于本文件。

GB/T 27000、ISO/IEC 29151 界定的术语和定义适用于本文件。

4 组织的背景

4.1 了解组织和其背景

组织应确定与其目的相关的、影响其实现个人身份信息保护管理体系预期结果能力的外部和内部问题。

4.2 了解有关各方的需求和期望

组织应确定:

a) 与个人身份信息保护管理体系有关的有关各方。

b) 这些相关方的相关要求。

c) 这些要求中的哪些将通过个人身份信息保护管理体系来解决。

4.3 确定个人身份信息保护管理体系范围

4.1.1 组织应确定个人身份信息保护管理体系的边界和适用性以建立其范围。

4.1.2 当确定范围时，组织应考虑组织实施活动之间及与其他组织间实际活动的接口和依赖关系。

4.1.3 范围应形成文件化信息并可获得。

4.4 个人身份信息保护管理体系

4.2.1 组织应根据本文件要求，建立、实施、维护和持续改进个人身份信息保护管理体系，包括所需过程及其相互作用。

组织应满足 ISO/IEC 29151 第 4 章概述中要求。

5 领导作用

5.1 领导作用和承诺

最高管理者应通过以下方面，证实其对个人身份信息保护管理体系的领导作用和承诺：

a) 确保建立个人身份信息保护方针和个人身份信息保护目标，并与组织的战略方向相一致；
b) 确保将个人身份信息保护管理体系的要求融入组织的过程中；
c) 确保个人身份信息保护管理体系所需的资源是可获得的；
d) 沟通有效的个人身份信息保护管理和符合个人身份信息保护管理体系要求的重要性；
e) 确保个人身份信息保护管理体系实现其预期结果；
f) 促使人员积极参与，指导和支持他们为个人身份信息保护管理体系的有效性作出贡献；
g) 推动改进；
h) 支持其他相关管理者在其职责范围内发挥领导作用。

5.2 方针

最高管理者应制定、实施和保持个人身份信息保护管理体系的方针，方针应：

a) 与组织的宗旨相事宜；
b) 为建立个人身份信息保护管理体系的目标提供框架；
c) 包括满足适用要求的承诺；
d) 包括持续改进个人身份信息保护管理体系的承诺。

方针应：

a) 可获取并保持成文信息；
b) 在组织内得到沟通、理解和应用；
c) 适宜时，可为有关相关方所获取。

5.3 组织的岗位、职责和权限

5.3.1 最高管理者应确保组织相关岗位的职责、权限得到分配、沟通和理解。

5.3.2 最高管理者应分配职责和权限，以：

a) 确保个人身份信息保护管理体系符合本文件的要求；
b) 报告个人身份信息保护管理体系的绩效以及改进机会，特别是向最高管理者报告。

6 策划

6.1 应对风险和机遇的措施

6.1.1 总则

在策划个人身份信息保护管理体系时，组织应确定需要应对的风险和机遇，以：

a) 确保个人身份信息保护管理体系能够实现其预期结果；
b) 预防或减少不利影响；
c) 实现改进。

组织应策划：

a) 应对这些风险和机遇的措施；
b) 如何 ：
    1) 在个人身份信息保护管理体系过程中整合并实施这些措施；
    2) 评价这些措施的有效性。

6.1.2 个人身份信息保护管理体系风险评价

组织应确定和实施个人身份信息保护风险评估过程，以：

a） 建立并维护个人身份信息保护风险准则，包括：

1）风险可接受准则；

2）实施个人身份信息保护风险评估准则。

b） 确保重复的个人身份信息保护风险评估产生一致、有效和可比较的结果。

c） 识别个人身份信息保护风险：

1）实施个人身份信息保护风险评估过程以识别以个人身份信息保护管理体系范围内与数据的保密性、完整性和可用性损失有关的风险；

2）识别风险所有者。

d） 分析个人身份信息保护风险：

1）评估 6.1.2c)1)中所识别的风险发生后，可能导致的潜在后果；

2）评估 6.1.2c)1)中所识别的风险实际发生的可能性；

3）确定风险级别。

e） 评价个人身份信息保护风险：

1）将风险分析的结果与 6.1.2a)中建立的风险准则进行比较；

2）为风险处置排序已分析风险的优先级。

组织应保留有关个人身份信息保护风险评估过程的文件化信息。

6.1.3 个人身份信息保护风险处置

组织应确定并实施个人身份信息保护风险处置过程，以：

a） 在风险评估结果的基础上，选择适当的个人身份信息保护风险处置选项；

b） 确定实现已选的个人身份信息保护风险处置选项所必需的所有控制；

注 1：当需要时，组织可设计控制，或识别来自任何来源的控制。

c） 将 6.1.3b)确定的控制与附录 A 的控制进行比较，并验证没有忽略必要的控制；

注 2：附录 A 包括了可能的个人身份信息保护控制清单，本文件的用户可在附录 A 的指导下，确保所必需的个人身份信息保护控制措施没有被忽视。

注 3：附录 A 的个人身份信息保护控制清单并不是详尽的，如需要，可以附加个人身份信息保护控制。

d） 制定一个适用性声明，包括：

——必要的控制；

——包含这些控制的正当理由；

——是否实施了所必需的控制；

——排除附录 A 控制的正当理由。

e） 制定正式的个人身份信息保护风险处置计划；

f） 获得风险所有者对个人身份信息保护风险处置计划以及对个人身份信息保护残余风险接受的批准。

组织应保留有关个人身份信息保护风险处置过程的文件化信息。

注 4：本文件中的个人身份信息保护风险评估与处置过程与 ISO 31000 中给出的原则和通用指南相匹配。

组织应满足 ISO/IEC 29151 4 概述 4.3 保护 PII 的控制、4.4 选择控制措施、4.5 制定组织特定的准则、4.6 生命周期考虑、4.7 本指南的结构中的要求。

6.2 个人身份信息保护目标及实现的策划

组织应针对相关职能、层次和个人身份信息保护管理体系所需的过程建立个人身份信息保护目标。

个人身份信息保护目标应：

a） 与个人身份信息保护方针保持一致；

b） 可测量；

c） 考虑适用的要求，以及个人身份信息保护评估和个人身份信息保护处置的结果；

d） 予以监视；
e） 予以沟通；
f） 适时更新；
g） 作为文件化信息可获取。

组织应保持有关个人身份信息保护目标的成文信息。

组织应满足 ISO/IEC 29151 4 概述 4.1 保护 PII 的目标、4.2PII 的保护要求中的要求，以及附录 A 中的要求。

策划如何实现个人身份信息保护目标时，组织应确定：

a) 要做什么；
b) 需要什么资源；
c) 由谁负责；
d) 何时完成；
e) 如何评价结果。

6.3 变更的策划

当组织确定需要变更个人身份信息保护管理体系时，变更应按计划的方式实施。

7 支持

7.1 资源

组织应确定并提供建立、实施、保持和持续改进个人身份信息保护管理体系所需的资源。

7.2 能力

组织应：

a） 确定在其控制下工作的人员所需具备的能力，这些人员从事的工作影响个人身份信息保护管理体系绩效和有效性 ；
b） 基于适当的教育、培训或经验，确保这些人员是胜任的；
c） 适用时，采取措施以获得所需的能力，并评价措施的有效性；
d） 保留适当的成文信息，作为人员能力的证据。

注：适用措施可包括对在职人员进行培训、辅导或重新分配工作，或者聘用、外包胜任的人员。

7.3 意识

组织应确保在其控制下工作的人员知晓：

a） 个人身份信息保护方针；
b） 他们对个人身份信息保护管理体系有效性的贡献，包括改进绩效的益处；
c） 不符合个人身份信息保护管理体系要求的后果。

7.4 沟通

组织应确定与个人身份信息保护管理体系相关的内部和外部沟通，包括：

a） 沟通什么；
b） 何时沟通；
c） 与谁沟通；
d） 怎么沟通。

7.5 成文信息

7.5.1 总则

组织的个人身份信息保护管理体系应包括：

a) 本文件要求的成文信息；

b) 组织所确定的、为确保个人身份信息保护管理体系有效性所需的成文信息。

注：对于不同组织，个人身份信息保护管理体系成文信息的多少与详路程度可以不同，取决于：

——组织的规模，以及活动、过程、产品和服务的类型；

——过程及其相互作用的复杂程度；

——人员的能力。

7.5.2 创建和更新

在创建和更新成文信息时，组织应确保适当的：

a) 标识和说明(如标题、日期、作者、索引编号)；

b) 形式(如语言、软件版本、图表)和载体(如纸质的、电子的)；

c) 评审和批准，以保持适宜性和充分性。

7.5.3 成文信息的控制

应控制个人身份信息保护管理体系和本文件所要求的成文信息，以确保：

a) 在需要的场合和时机，均可获得并适用；

b) 予以妥善保护(如防止泄密、不当使用或缺失)。

为控制成文信息，适用时，组织应进行下列活动：

a) 分发、访问、检索和使用；

b) 存储和防护，包括保持可读性；

c) 更改控制(如版本控制)；

d) 保留和处置。

对于组织确定的策划和运行个人身份信息保护管理体系所必需的来自外部的成文信息，组织应进行适当识别，并予以控制。

注：对成文信息的“访问”可能意味着仅允许查阅，或者意味着允许查阅并授权修改。

8 运行

8.1 运行的策划和控制

8.1.1 为满足产品和服务提供的要求，并实施第 6 章所确定的措施，组织应通过以下措施对所需的过程进行策划、实施和控制：

——建立过程准则；

——按照过程准则实施过程控制。

8.1.2 应在必要的范围和程度上提供文件化信息，以确信这些过程按计划得到执行。

8.1.3 组织应控制计划内的变更并评审非预期变更的后果，必要时采取措施减轻任何负面影响。

8.1.4 组织应确保外包过程是确定的和受控的。

8.2 个人身份信息保护风险评估

组织应考虑 6.1.2a)所建立的准则，按计划的时间间隔，或当重大变更提出或发生时，执行个人身份信息保护风险评估。

组织应保留个人身份信息保护风险评估结果的文件化信息。

8.3 个人身份信息保护风险处置

组织应实施个人身份信息保护处置计划。

组织应保留个人身份信息保护风险处置结果的文件化信息。

9 绩效评价

9.1 监视、测量、分析和评价

9.1.1 总则

组织应确定：

a) 需要监视和测量什么，包括个人身份信息保护过程和控制；

b) 适用时的监视、测量、分析和评价的方法，以确保结果有效。选择的方法应能产生可比较与可重现的结果以被认为是有效的；

c) 何时实施监视和测量；

d) 谁应监视和测量；

e) 何时对监视和测量的结果进行分析和评价；

f) 应分析和评价这些结果。

应提供文件化信息以作为结果的证据。

组织应评价个人身份信息保护绩效和个人身份信息保护管理体系的有效性。

9.2 内部审核

9.2.1 总则

组织应按照策划的时间间隔实施内部审核，以提供有关个人身份信息保护管理体系的以下信息，是否：

a) 符合：

1) 组织自身对个人身份信息保护管理体系要求；

2) 本文件的要求；

b) 得到有效的实施和保持。

9.2.2 内部审核

组织应策划、制定、实施和维护审核方案，包括审核频次、方法、职责、策划要求和报告；

制定内部审核方案时，组织应考虑相关过程的重要性和以往审核的结果。

组织应：

a) 规定每次审核的审核准则和范围；

b) 选择审核员并实施审核，确保审核过程的客观公正；

c) 确保将审核结果报告至相关管理者。

应提供文件化信息，作为实施审核方案以及审核结果的证据。

9.3 管理评审

9.3.1 总则

最高管理者应按照策划的时间间隔对组织的个人身份信息保护管理体系进行评审，以确保其持续的适宜性、充分性和有效性。

9.3.2 管理评审输入

策划和实施管理评审时应考虑下列内容：

a) 以往管理评审所采取措施的情况；

b) 与个人身份信息保护管理体系相关的相关方需求和期望的变化；

c） 下列有关个人身份信息保护管理体系绩效和有效性的信息，包括其趋势：
1） 不合格及纠正措施；
2） 监视和测量结果；
3） 审核结果；
4） 个人身份信息保护目标完成情况。
d） 相关方反馈；
e） 风险评估及风险处置计划的情况；
f） 持续改进的机会。

9.3.3 管理评审输出

管理评审的结果应包括与持续改进机会相关的决定以及变更个人身份信息保护管理体系的任何需求。

组织应提供文件化信息，以作为管理评审结果的证据。

10 改进

10.1 持续改进

组织应持续改进个人身份信息保护管理体系的适宜性、充分性和有效性。

10.2 不合格和纠正措施

10.2.1 当发生不符合时，组织应：
a） 对不符合做出应对，适用时：
1） 采取措施，以控制和纠正不符合；
2） 处理后果；
b） 通过下列活动，评价是否需要采取措施，以消除产生不符合的原因，避免其再次发生或在其他场合发生：
1） 评审不符合；
2） 确定不符合的原因；
3） 确定是否存在或可能发生类似的不符合；
c） 实施任何所需的措施；
d） 评审任何所采取纠正措施的有效性；
e） 必要时，对个人身份信息保护管理体系进行变更。

10.2.2 纠正措施应对不符合所产生的影响相适应。

10.2.3 应提供文件化信息以作为下列事项的证据：
a） 不符合的性质以及所采取的任何后续措施；
b） 任何纠正措施的结果。

附录 A

（规范性附录）

个人身份信息保护控制参考

表 A 所列的个人身份信息保护控制应在 6.1.3 环境中被使用。

表 A 个人身份信息保护控制

5 组织控制		
5.1	个人身份信息保护策略	**控制** 个人身份信息保护策略和特定的主题策略应被定义，由管理者批准发布、传递并相关人员和有关相关方所认可，并按照策划的时间间隔或当发生重大变化时实施评审。 组织应满足 ISO/IEC 29151《个人身份信息保护实践指南》5 信息安全政策中的要求。
5.2	个人身份信息保护角色和职责	**控制** 应根据组织的需求定义、分配个人身份信息保护的角色和职责 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》6 信息安全的组织 6.1 内部组织 6.1.1 简介、6.1.2 信息安全角色和责任中的要求。
5.3	职责分离	**控制** 应分离有冲突的职责及其职责范围 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》6 信息安全的组织 6.1 内部组织 6.1.3 职责分离中的要求。
5.4	管理职责	**控制** 管理应要求所有人员按照组织制定的个人身份信息保护策略、特定主题策略和规程实施个人身份信息保护 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》7 人力资源安全 7.2 在任职期间 7.2.1 介绍 7.2.2 管理责任中的要求。
5.5	与职能机构的联系	**控制** 组织应建立和维护与相关职能机构的联系 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》6 信息安全的组织 6.1.4 与主管部门联系中的要求。

5.6	与特定相关方的联系	**控制** 组织应建立和维护与相关职能机构的联系 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》6 信息安全的组织 6.1.5 与特殊利益集团联系中的要求。
5.7	威胁情报	**控制** 应收集和分析与个人身份信息保护威胁相关的信息，以形成威胁情报
5.8	项目管理中的个人身份信息保护	**控制** 个人身份信息保护应整合进项目管理中 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》6 信息安全的组织 6.1.6 项目管理中的信息安全中的要求。
5.9	信息及其他资产清单	**控制** 应当制定和维护信息和其他资产清单，包括其拥有者 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》8 资产管理 8.1 有关资产的责任 8.1.1 介绍、8.1.2 资产清单、8.1.3 资产的所有权中的要求。
5.10	信息和其他相关资产的可接受使用	**控制** 应识别可接受使用的准则、信息及其他相关资产处理规程，形成文件并实施 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》8 资产管理 8.1 有关资产的责任 8.1.4 资产的可接受使用中的要求。
5.11	资产归还	**控制** 人员和其他适当的相关方在任用、合同或协议的变更或终止时，应归还其占用的所有组织资产 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》8 资产管理 8.1 有关资产的责任 8.1.5 资产归还中的要求。
5.12	信息的分级	**控制** 信息应按照组织的个人身份信息保护需求，基于保密性、完整性、可用性和有关相关方的要求进行分级 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》8 资产管理 8.2 信息分类 8.2.1 介绍 8.2.2 信息分类中的要求。

5.13	信息的标记	**控制** 应按照组织采用的信息分级方案，制定并实现一组适当信息标记规程 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》8 资产管理 8.2 信息分类 8.2.1 介绍 8.2.3 信息标记中的要求。
5.14	信息传输	**控制** 在组织内以及与其他各方之间的所有类型传输设备，都应制定信息传输规则、规程或协议 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》13 通信安全 13.2 信息传输 13.2.1 简介、13.2.2 信息传输策略和规程、13.2.3 信息传输协议、13.2.4 电子信息发送中的要求。
5.15	访问控制	**控制** 应基于业务和个人身份信息保护要求，建立和实施控制信息和其他相关资产的物理和逻辑访问控制规则 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》9 访问控制 9.1 访问控制的业务需求中的要求。
5.16	身份管理	**控制** 应对身份的全生命周期实施管理 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》9 访问控制 9.2 用户访问管理 9.2.1 简介、9.2.2 用户注册和注销、9.2.3 用户访问供给中的要求。
5.17	鉴别信息	**控制** 应通过管理过程控制鉴别信息的分配和管理，包括建议员工适当地处理鉴别信息 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》9 访问控制 9.2 用户访问管理 9.2.5 用户的秘密鉴别信息的管理中的要求。 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》9 访问控制 9.3 用户责任中的要求。

5.18	访问权限	**控制** 应根据组织的特定主题策略和访问控制规则，提供、评审、调 整和移除对于信息和其他相关资产的访问权限 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》9 访问控制 9.2 用户访问管理 9.2.6 用户访问权管理、9.2.7 访问权的移除或调整中的要求。
5.19	供应商关系的个人身份信息保护	**控制** 应确定和实施过程和规程，以管理与供应商的产品和服务相关的个人身份信息保护风险 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》15 供应商关系 15.1 供应关系的信息保护 15.1.1 简介、15.1.2 供应商关系信息保护策略中的要求。
5.20	在供应商协议中强调个人身份信息保护	**控制** 应基于供应商关系的类型与每个供应商建立相关的个人身份信息保护要求，并达成一致 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》15 供应商关系 15.1 供应关系的信息保护 15.1.3 在供应商协议中安全的要求。
5.21	ICT（信息与通信技术）供应链中的个人身份信息保护管理	**控制** 应确定和实施过程和规程，以管理与 ICT 产品和服务供应链相关的个人身份信息保护风险 组织应满足 ISO/IEC 29151《个人身份信息保护实践指南》15 供应商关系 15.1 供应关系的信息保护 15.1.4 信息与通讯技术供应链中的要求。
5.22	供应商服务的监视、评审和变更管理	**控制** 组织应定期对供应商的个人身份信息保护履行和服务交付实施监视、评审、评价和管理变更 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》15 供应商关系 15.2 供应商服务交付管理中的要求。
5.23	云服务使用中的个	**控制**

	人身份信息保护	应根据组织个人身份信息保护要求建立云服务的获取、使用管理和退出过程
5.24	个人身份信息保护事件管理的策划和准备	**控制** 组织应通过确定、建立和沟通个人身份信息保护事件管理过程、准则和职责进行个人身份信息保护事件管理的策划和准备 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》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 简介、16.1.2 责任和规程中的要求。
5.25	个人身份信息保护事态的评估和决策	**控制** 组织应评估个人身份信息保护事件并决定其是否归属于个人身份信息保护事件 组织应满足 ISO/IEC 29151《个人身份信息保护实践指南》16 信息安全事件管理 16.1 信息安全事件的管理和改进 16.1.5 信息安全事态的评估和决策中的要求。
5.26	个人身份信息保护事件的响应	**控制** 应按照文件化的规程响应个人身份信息保护事件 组织应满足 ISO/IEC 29151《个人身份信息保护实践指南》16 信息安全事件管理 16.1 信息安全事件的管理和改进 16.1.6 信息安全事件的响应中的要求。
5.27	从个人身份信息保护事件中的学习	**控制** 应利用在个人身份信息保护事件中获得的知识加强和改进个人身份信息保护控制 组织应满足 ISO/IEC 29151《个人身份信息保护实践指南》16 信息安全事件管理 16.1 信息安全事件的管理和改进 16.1.7 从信息安全事件中学习中的要求。
5.28	证据的收集	**控制** 组织应建立、实施规程来识别、收集、获取和保存与个人身份 信息保护事态相关的证据 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》16 信息安全事件管理 16.1 信息安全事件的管理和改进 16.1.8 证据的收集中的要求。

5.29	中断期间的个人身份信息保护	**控制** 组织应策划在中断期间保持适当级别的个人身份信息保护
5.30	关于业务连续性的 ICT 准备	**控制** 应基于业务连续目标和 ICT 连续要求策划、实施、保持和测试 ICT(信息通信技术）的准备情况 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》17 业务连续性管理的信息安全方面 17.1 信息安全的连续性中的要求。
5.31	法律法规、监管和合同要求	**控制** 与个人身份信息保护相关的法律、法规、监管和合同要求，以 及组织为满足这些要求的方法，应得到识别、形成文件和保持 更新 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》18 符合性 18.1 符合法律和合同要求 18.1.1 引言、18.1.2 适用的法律和合同要求的识别中的要求。
5.32	知识产权	**控制** 组织应建立适当的规程来保护知识产权 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》18 符合性 18.1 符合法律和合同要求 18.1.3 知识产权中的要求。
5.33	记录保护控制	**控制** 记录应得到保护以防其丢失、损坏、伪造、未授权访问和未授权发布 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》18 符合性 18.1 符合法律和合同要求 18.1.4 记录保护中的要求。
5.34	隐私和 PII(个人可识别信息）的保护	**控制** 组织应根据适用的法律法规和合同要求，识别并满足有关隐私保护和个人可识别信息的保护 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》18 符合性 18.1 符合法律和合同要求 18.1.5 隐私和个人可识别信息保护、18.1.6 密码控制规则中的要求。

5.35	个人身份信息保护的独立评审	**控制** 应按照计划的时间间隔或在重大变化发生时，对组织的个人身份信息保护管理方法及其实现，包括人员、过程和技术进行独立评审 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》18 符合性 18.2 信息安全评审 18.2.1 介绍、18.2.2 信息安全的独立评审中的要求。
5.36	符合个人身份信息保护的策略、规则和标准	**控制** 应定期评审与组织的个人身份信息保护策略、特定主题策略、规则和标准的符合性 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》18 符合性 18.2 信息安全评审 18.2.3 符合安全策略和标准、18.2.4技术符合性评审中的要求。
5.37	文件化的操作规程	**控制** 信息处理设施的操作规程应当形成文件并对所需用户可用 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》12 运行安全 12.1 运行规则和责任 12.1.1 简介、12.1.2 文件化的操作规程中的要求。
6 人员控制		
6.1	审查	**控制** 在加入组织前，对所有拟任的候选人的背景实施验证核查，并考虑到适用的法律法规和道德规范，以及与业务要求、访问信息的等级和察觉的风险相适宜 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》7 人力资源安全 7.1 聘用前 7.1.1 介绍、7.1.2 审查中的要求。
6.2	任用条款及条件	**控制** 员工合同协议中应声明员工和组织对个人身份信息保护的职责 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》7 人力资源安全 7.1 聘用前 7.1.3 任用条款和条件中的要求。

6.3	个人身份信息保护意识、教育和培训	**控制** 组织员工和有关相关方应按其工作职能，接受适当的个人身份信息保护意识、教育和培训，以及组织个人身份信息保护策略、特定主题策略及规程的定期更新的信息 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》7 人力资源安全 7.2 在任职期间 7.2.3 信息安全意识、教育和培训中的要求。
6.4	违规处理过程	**控制** 违规处理过程应正式地传达，以对违反个人身份信息保护策略的员工和其他有关相关方采取措施 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》7 人力资源安全 7.2 在任职期间 7.2.4 违规处理过程中的要求。
6.5	任用终止或变更后的责任	**控制** 任用终止或变更后仍有效的个人身份信息保护责任及其职责应当得到确定、执行和传达到相关员工和其他相关方 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》7 人力资源安全 7.3 任用的终止或变更中的要求。
6.6	保密和不泄露协议	**控制** 应识别、形成文件、定期评审并与员工和其他有关相关方签署反映信息保护需要的保密性或不泄露协议 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》13 通信安全 13.2 信息传输 13.2.5 保密或不泄露协议中的要求。
6.7	远程工作	**控制** 当员工远程工作时，应当采取措施以保护在组织场所外访问的处理的或存储的信息 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》6 信息安全的组织 6.2 移动设备和远程工作中的要求。
6.8	个人身份信息保护事态报告	**控制** 组织应提供一种让员工通过适当渠道，及时报告观察到的或可疑的个人身份信息保护事态的机制

		组织应满足 ISO/IEC 29151《个人身份信息保护实践指南》16 信息安全事件管理 16.1 信息安全事件的管理和改进 16.1.3 报告信息安全事态、16.1.4 报告信息安全弱点中的要求。
7 物理控制		
7.1	物理安全边界	**控制** 应定义和使用安全边界来保护信息和其他相关资产的区域 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》11 物理和环境安全 11.1 安全区域 11.1.1 简介 11.1.2 物理安全边界中的要求。
7.2	物理入口	**控制** 安全区域应由适当的入口控制和访问点所保护 组织应满足 ISO/IEC 29151《个人身份信息保护实践指南》11 物理和环境安全 11.1 安全区域 11.1.3 物理入口控制中的要求。
7.3	办公室、房间和设备的安全保护	**控制** 应为办公室、房间、设施设计和实施物理安全措施 组织应满足 ISO/IEC 29151《个人身份信息保护实践指南》11 物理和环境安全 11.1 安全区域 11.1.4 办公室、房间和设施的安全保护中的要求。
7.4	物理安全监视	**控制** 应持续监视物理场所，以防止未经授权的物理访问
7.5	物理和环境威胁的安全防护	**控制** 应设计和实施应对物理和环境威胁的安全防护，如自然灾害和其他有意或无意的对基础设施的物理威胁 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》11 物理和环境安全 11.1 安全区域 11.1.5 外部和环境威胁的安全防护中的要求。
7.6	在安全区域工作	**控制** 应设计和实施在安全区域工作的安全措施 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》11 物理和环境安全 11.1 安全区域 11.1.6 安全区域工作、11.1.7 交接区中的要求。

7.7	清理桌面和屏幕	**控制** 应当确定并适当地执行针对纸质和可移动存储介质的清理桌面规则和针对信息处理设施的清理屏幕规则 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》11 物理和环境安全 11.2 设备 11.2.10 清理桌面和屏幕策略中的要求。
7.8	设备安置和保护	**控制** 应安全地安置和保护设备 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》11 物理和环境安全 11.2 设备 11.2.1 简介、11.2.2 设备安置和保护中的要求。 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》11 物理和环境安全 11.2 设备 11.2.9 无人值守的用户设备中的要求。
7.9	组织场所外的资产安全	**控制** 场外的资产应得到保护 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》11 物理和环境安全 11.2 设备 11.2.6 资产移动、11.2.7 组织场外的设备与资产安全中的要求。
7.10	存储介质	**控制** 应根据组织的分级方案和处理要求，对存储介质实施购买、使用、运送和处置的全生命周期管理 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》8 资产管理 8.2 信息分类 8.3 介质处置中的要求。
7.11	支持性设施	**控制** 应保护信息处理设施使其免于由支持性设施的失败而引起的电源故障和其他中断 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》11 物理和环境安全 11.2 设备 11.2.3 支持性设备中的要求。
7.12	布缆安全	**控制**

		应保证输送电力、传输数据或支持信息服务的电缆免受窃听、干扰或损坏 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》11 物理和环境安全 11.2 设备 11.2.4 布缆安全中的要求。
7.13	设备维护	**控制** 设备应予以正确地维护，以确保信息的可用性、完整性和保密性 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》11 物理和环境安全 11.2 设备 11.2.5 设备维护中的要求。
7.14	设备的安全处置或再利用	**控制** 包含储存介质的设备项目应进行核查，以确保在处置或再利用之前，任何敏感信息和注册软件已被删除或安全的重写 组织应满足 ISO/IEC 29151《个人身份信息保护实践指南》8 资产管理 8.2 信息分类 8.2.4 资产处置中的要求。 组织应满足 ISO/IEC 29151《个人身份信息保护实践指南》11 物理和环境安全 11.2 设备 11.2.8 设备的安全处置和再利用中的要求。
8 技术控制		
8.1	用户终端设备	**控制** 应保护用户终端设备上存储、处理或访问的信息
8.2	特许访问权	**控制** 应限制并管理特许访问权的分配和使用 组织应满足 ISO/IEC 29151《个人身份信息保护实践指南》9 访问控制 9.2.4 特殊访问权的管理中的要求。
8.3	信息访问限制	**控制** 应按照建立的特定主题访问控制策略限制对信息和其他相关资产的访问 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》9.4 系统和应用访问控制中的要求。
8.4	对源代码的访问	**控制**

		对源代码、开发工具和软件库的读写访问应得到适当的管理
8.5	身份验证安全	**控制** 应当基于信息访问限制和访问控制的特定主题策略，实施身份验证技术和规程
8.6	容量管理	**控制** 应根据当前和预期的能力要求对资源的使用进行监视和调整 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》12 运行安全 12.1 运行规则和责任 12.1.4 容量管理中的要求。
8.7	恶意软件防范	**控制** 应实施恶意软件防范，并通过适当的用户意识提供支持 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》12 运行安全 12.2 恶意软件防范中的要求。
8.8	技术脆弱性管理	**控制** 应获取在用信息系统的有关技术脆弱性信息，用评价组织对这些脆弱性的暴露状况并采取适当的措施 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》12 运行安全 12.6 技术脆弱性管理中的要求。
8.9	配置管理	**控制** 硬件、软件、服务和网络的配置（包括安全配置）应得到建立、 文件化、实施、维护和评审
8.10	信息删除	**控制** 不再需要时，应删除存储在信息系统、设备或任何其他介质中的信息
8.11	数据屏蔽	**控制** 应当根据组织的访问及其他相关的特定主题策略、业务要求使用数据屏蔽，并考虑到法律要求
8.12	防止数据泄露	**控制** 数据泄露预防措施应用于处理、存储或传输敏感信息的系统、网络和任何其他终端设备
8.13	信息备份	**控制**

		按照既定的备份特定专题策略，对信息、软件和系统进行备份，并定期测试 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》12 运行安全 12.3 备份中的要求。
8.14	信息处理设施的冗余	**控制** 信息处理设施应当实现冗余，以满足可用性要求 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》17 业务连续性管理的信息安全方面 17.2 冗余中的要求。
8.15	日志管理	**控制** 应产生、存储、保护和分析记录活动、异常、错误和其他事态 的日志 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》12 运行安全 12.4 日志和监视中的要求。
8.16	监视活动	**控制** 应监视网络、系统和应用的异常行为，并采取适当的措施评估潜在的个人身份信息保护事件
8.17	时钟同步	**控制** 组织使用的信息处理系统的时钟，应与批准的时间源同步
8.18	特许权使用程序的应用	**控制** 对于可能超越系统和应用控制的使用程序的使用应予以限制并严格控制
8.19	运行系统的软件安装	**控制** 应实施规程和措施，以安全管理运行系统的安装软件 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》12 运行安全 12.5 运行软件控制中的要求。
8.20	网络安全	**控制** 应安全管理和控制网络以及网络设备，以保护系统和应用中的信息 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》13 通信安全 13.1 网络安全管理 13.1.1 简介、13.1.2 网络控制中的要求。

8.21	网络服务安全	**控制** 网络服务的安全机制、服务级别和安全要求应予以确定、实施和维护 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》13 通信安全 13.1 网络安全管理 13.1.3 网络服务安全中的要求。
8.22	网络隔离	**控制** 应在组织的网络中隔离信息服务、用户和信息系统 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》13 通信安全 13.1 网络安全管理 13.1.4 网络隔离中的要求。
8.23	网站过滤	**控制** 应管理对外部网站的访问，以减少对恶意内容的接触
8.24	密码使用	**控制** 应确定和实施有效使用密码的规则，包括密钥管理 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》10 密码学中的要求。
8.25	开发生命周期安全	**控制** 应建立和应用软件和系统的安全开发规则 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》14 系统获取、开发和维护 14.1 信息系统的安全要求、14.2 开发和支持过程的安全性 14.2.1 简介、14.2.2 安全的开发策略、14.2.3 系统变更控制规程、14.2.4 运行平台变更后对应的技术评审、14.2.5 软件包变更的限制中的要求、14.2.7 安全的开发环境中要求。
8.26	应用程序安全要求	**控制** 应开发和获取应用程序时，应识别、规定和批准个人身份信息保护要求
8.27	安全系统架构和工程原则	**控制** 应建立、形成文件、维护系统安全工程原则，并应用到任何信息系统的开发活动

		组织应满足 ISO/IEC 29151《个人身份信息保护实践指南》14 系统获取、开发和维护 14.2 开发和支持过程的安全性 14.2.6 系统安全工程原则中的要求。
8.28	安全编码	**控制** 安全编码原则应用于软件开发
8.29	开发和验收中的安全测试	**控制** 应在开发的生命周期中确定和实施安全测试过程 组织应满足 ISO/IEC 29151《个人身份信息保护实践指南》14 系统获取、开发和维护 14.2 开发和支持过程的安全性 14.2.9 系统安全测试、14.2.10 系统验收测试中的要求。
8.30	外包开发	**控制** 组织应指导、监视和评审与外包系统开发有关的活动 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》14 系统获取、开发和维护 14.2 开发和支持过程的安全性 14.2.8 外包开发中的要求。
8.31	开发、测试与生产环境的隔离	**控制** 应分离并保护开发、测试和生产环境 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》12 运行安全 12.1 运行规则和责任 12.1.5 开发、测试和运行环境的分离中的要求。
8.32	变更管理	**控制** 信息处理设备和信息系统的变更应遵守变更管理规程 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》12 运行安全 12.1 运行规则和责任 12.1.3 变更管理中的要求。
8.33	测试信息	**控制** 测试信息应适当地选择、保护和管理
8.34	审计测试期间的信息系统保护	**控制** 审计测试和其他涉及运行系统验证的评审活动应在测试人员和事宜的管理者之间得到策划和协商一致 组织应满足 ISO/IEC 29151 《个人身份信息保护实践指南》12 运行安全 12.7 信息系统审计控制中的要求。

参 考 文 献

[1] GB/T 19000 质量管理体系 基础和术语

[2] GB/T 19001—2016/ISO 质量管理体系 要求

[3] GB/T 19011 管理体系审核指南

[4] GB/T 27011 合格评定 认可机构要求

[5] GB/T 27021.1 合格评定 管理体系审核认证机构要求 第 1 部分：要求

[6] 国家认证认可监督管理委员会 2006 年第 3 号公告 认证技术规范管理办法

[7] GB/T 22080 网络安全技术 信息安全管理体系 要求

[8] GB/T 22081 网络安全技术 信息安全控制

[9] ISO/IEC 27001 信息安全、网络安全和隐私保护—信息安全管理体系 要求

[10]ISO/IEC 27002 信息安全、网络安全和隐私保护-信息安全控制

[10] ISO/IEC 27003 信息技术 安全技术 信息安全管理体系实施指南

[11] ISO/IEC 27004 信息技术 安全技术 信息安全管理 测量

[12] ISO/IEC 27005 信息技术 安全技术 信息安全风险管理

[13] ISO 31000 风险管理 原则和指南

[14] ISO/IEC 27000 信息技术-安全技术-信息安全管理体系-概述和词汇

[15] ISO/IEC 27018 信息技术-安全技术-作为 PII 处理者的公有云中保护个人可识别信息（PII）的实施规程

[16] ISO/IEC 29151:2017 信息技术 - 安全技术 - 个人身份信息保护的实践守则