个人数据隐私保护管理体系

认证技术规范

文件编号：CTS TBGL136-2026

版本号：B/2

受控状态： （ 受控 ）

编写：技术部

审核：张辉根

批准：周春阳

首次发布：2022-12-20 **首次实施：2022-12-20** **修订实施日期：20260423**

江西腾标认证有限公司

目录

1. 范围 4
2. 规范性引用文件 4
3. 术语和定义 4
4. 组织环境 5
4.1. 理解组织及其环境 5
4.2. 理解相关方的需求和期望 5
4.3. 确定 个人数据隐私保护管理体系 范围 5
4.4. 个人数据隐私保护管理体系 及其过程 6
5. 领导作用 6
5.1. 领导作用和承诺 6
5.2. 方针 7
5.3. 组织的岗位、职责和权限 7
6. 策划 7
6.1. 应对风险和机遇的措施 7
6.2. 个人数据隐私保护管理体系 目标及其实现的策划 8
6.3. 变更的策划 8
7. 支持 9
7.1. 资源 9
7.2. 能力 9
7.3. 意识 9
7.4. 沟通 10
7.5. 成文信息 10
8. 运行 10
8.1. 运行策划和控制 11
8.2. 隐私风险评估 11
8.3. 隐私风险处置 11
8.4. 个人数据隐私保护特定控制措施（依据ISO/IEC 29151:2017） 11
9. 绩效评价 13
9.1. 监视、测量、分析和评价 13
9.2. 内部审核 13
9.3. 管理评审 14
10. 改进 14
10.1. 不合格与纠正措施 14
10.2. 持续改进 15
11. 其他 15

前言

本文件旨在为组织（以下简称“组织”）建立、实施、维护和持续改进个人数据隐私保护管理体系（PIPMS）提供要求和指南。本文件采用PDCA（策划-实施-检查-改进）循环模式，与ISO/IEC 27001:2022《信息安全、网络安全和隐私保护 — 信息安全管理体系 — 要求》 的高阶结构保持一致，并充分融合了 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》 的特定行业控制要求。

本文件旨在为组织在基于ISO/IEC 27001:2022建立和实施信息安全管理体系的过程中，提供一套专门的个人数据隐私保护控制选择和实施指南。本文件的核心架构与ISO/IEC 27001:2022完全一致，组织可通过实施本文件，建立一个同时满足ISO/IEC 27001和ISO/IEC 29151:2017要求的整合性管理体系。组织应首先建立满足ISO/IEC 27001要求的信息安全管理体系（ISMS），并在此基础上扩展个人数据隐私保护管理要求。

1. 范围

本文件规定了组织建立、实施、保持和持续改进 个人数据隐私保护管理体系（简称：PIPMS） 的要求。本文件适用于：

1) 组织建立、实施、保持和改进 个人数据隐私保护管理体系 ；

2) 认证机构对组织进行 个人数据隐私保护管理体系 认证。

2. 规范性引用文件

下列文件对于本文件的应用必不可少。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
- GB/T 22080-2025/ISO/IEC 27001:2022 网络安全技术 信息安全管理体系 要求
- ISO/IEC 27002:2022 信息安全、网络安全和隐私保护-信息安全控制
- 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
- ISO/IEC 29100:2024 信息技术-安全技术-隐私框架

注：认证审核时引用文件的有效性以审核实施时现行有效的最新版本为准。

3. 术语和定义

ISO/IEC 27000、ISO/IEC 27001:2022界定的以及下列术语和定义适用于本文件。ISO和IEC在以下地址维护用于标准化的术语数据库：

- ISO在线浏览平台-信息技术及相关技术行业 https://www.iso.org/sectors/it-technologies
- IEC电子百科 https://www.iec.ch/homepage

3.1. 个人身份信息（PII）

(a) 可用于识别与该信息相关的PII主体的任何信息，或(b) 与PII主体直接或间接相关的信息。

[来源：ISO/IEC 29100:2011, 2.9]

3.2. PII主体

PII所关联的个人。

[来源：ISO/IEC 29100:2011, 2.12]

3.3. PII控制者

决定PII处理的目的和方式的组织。

[来源：ISO/IEC 29100:2011, 2.10]

3.4. PII处理者

根据PII控制者的指示处理PII的组织。

[来源：ISO/IEC 29100:2011, 2.11]

3.5. 隐私

个人对其个人身份信息（PII）的控制权，包括收集、使用、披露、存储和销毁的方式。

3.6. 同意

PII主体在充分知情的情况下，自愿、明确地同意对其PII进行特定处理的意愿表示。

3.7. 数据泄露

对PII的未经授权的访问、披露、更改或丢失。

3.8. 数据最小化

将PII的处理限制在实现特定目的所必需的最小范围内。

3.9. 数据主体权利

PII主体依法享有的对其PII的权利，包括访问权、更正权、删除权、限制处理权、数据可携带权和反对权等。

4. 组织环境

4.1. 理解组织及其环境

组织应建立并保持程序，以确定与其宗旨和战略方向相关并影响其实现 个人数据隐私保护管理体系 预期结果的能力的各种外部和内部因素。组织应对这些外部和内部因素的相关信息进行监视和评审，并保留成文信息。

1) 外部因素：适用的PII保护法律和法规（如《个人信息保护法》、欧盟GDPR等）、监管机构要求（如网信办、工信部、数据局等）、行业标准与最佳实践、PII泄露的监管和声誉风险、客户对隐私保护的关注度、分包商所在国家的法律等。
2) 内部因素： 组织的规模、治理结构、作为PII控制者或处理者的角色、处理的PII类型和数量、人员隐私意识与技能水平、以往PII安全事件记录等。

注：

① 这些因素可能包括需要考虑的正面和负面要素或条件。
② 考虑来自于国际、国内、地区或当地的各种法律法规、技术、竞争、市场、文化、社会和经济环境的因素，有助于理解外部环境。
③ 考虑与组织的价值观、文化、知识和绩效等有关的因素，有助于理解内部环境。

4.2. 理解相关方的需求和期望

4.2.1. 由于相关方对组织稳定提供符合顾客要求及适用法律法规要求的产品和服务的能力具有影响或潜在影响，组织应确定：

1) 与PIPMS有关的相关方；
2) 这些相关方的有关要求；
3) 哪些要求将通过PIPMS予以解决。

4.2.2. 相关方包括但不限于：PII主体、PII控制者/处理者、监管机构、员工、客户、合作伙伴、供应商、认证机构、公众。

4.2.3. 组织应建立、实施并保持程序，以识别相关方，并促其参与到与 个人数据隐私保护管理体系 相关的已识别的议题中。组织应保留促进相关方参与所产生的输出作为成文信息。与相关方的沟通应为一个持续的过程，而组织应保留沟通记录。

4.3. 确定 个人数据隐私保护管理体系 范围

4.3.1. 组织应确定 个人数据隐私保护管理体系 的边界和适用性，以确定其范围。

4.3.2. 在确定范围时，组织应考虑：

1) 在4.1.理解组织及其环境中提及的各种外部和内部因素；
2) 在4.2理解相关方的需求和期望中提及的相关方的要求；
3) 组织实施的活动与其他组织实施的活动之间的接口和依赖关系（特别是与PII控制者、处理者、

分包商之间的接口）。

4.3.3. 如果本标准的全部要求适用于组织确定的 个人数据隐私保护管理体系 范围，组织应实施本标准的全部要求。

4.3.4. 组织应编制并保持 个人数据隐私保护管理体系 范围的成文信息。该范围应明确界定管理体系覆盖的边界和适用性，经最高管理者批准后生效。该范围应描述所覆盖的产品和服务类型，如果组织确定本标准的某些要求不适用于其 个人数据隐私保护管理体系 范围，应说明理由。

4.3.5. 只有当所确定的不适用的要求不影响组织确保其产品和服务合格的能力或责任，对增强顾客满意也不会产生影响时，方可声称符合本标准的要求。

4.4. 个人数据隐私保护管理体系 及其过程

4.4.1. 组织应按照本技术规范的要求，建立、形成文件、实施、保持和持续改进 个人数据隐私保护管理体系 ，包括所需过程及其相互作用。组织应保留管理体系成文信息（如管理手册）。

4.4.2. 组织应确定 个人数据隐私保护管理体系 所需的过程及其在整个组织中的应用，且应：

1) 确定这些过程所需的输入和期望的输出；
2) 确定这些过程的顺序和相互作用；
3) 确定和应用所需的准则和方法(包括监视、测量和相关绩效指标),以确保这些过程的有效运行和控制；
4) 确定这些过程所需的资源并确保其可获得；
5) 分配这些过程的职责和权限；
6) 按照6.1条款的要求应对风险和机遇；
7) 评价这些过程，实施所需的变更，以确保实现这些过程的预期结果；
8) 改进过程和 个人数据隐私保护管理体系 。

4.4.3. 在必要的范围和程度上，组织应：

1) 保持成文信息以支持过程运行；
2) 保留成文信息以确信其过程按策划进行。

5. 领导作用

5.1. 领导作用和承诺

5.1.1. 总则

最高管理者应通过以下方面，提供证据以证实其对 个人数据隐私保护管理体系 的领导作用和承诺。最高管理者应保留履行上述职责的记录（如会议纪要、批准文件等）：

1) 对 个人数据隐私保护管理体系 的有效性负责；
2) 确保制定 个人数据隐私保护管理体系 的方针和目标，并与组织环境相适应，与战略方向相一致；
3) 确保 个人数据隐私保护管理体系 要求融入组织的业务过程；
4) 促进使用过程方法和基于 个人数据隐私保护管理体系 的思维；
5) 确保 个人数据隐私保护管理体系 所需的资源是可获得的；
6) 沟通有效的培训管理和符合 个人数据隐私保护管理体系 要求的重要性；
7) 确保 个人数据隐私保护管理体系 实现其预期结果（如PII安全、合规、客户信任）；
8) 促使人员积极参与，指导和支持他们为 个人数据隐私保护管理体系 的有效性作出贡献；
9) 推动改进；
10) 支持其他相关管理者在其职责范围内发挥领导作用。

注：本标准使用的“业务”一词可广义地理解为涉及组织存在目的的核心活动，无论是公有、私有、营利或非营利组织。

5.1.2. 以顾客为关注焦点

最高管理者应通过确保以下方面，证实其以顾客为关注焦点的领导作用和承诺：

1) 确定、理解并持续地满足顾客要求以及适用的法律法规要求；
2) 确定和应对风险和机遇，这些风险和机遇可能影响产品和服务合格以及增强顾客满意的能力；
3) 始终致力于增强顾客满意。

5.2. 方针

5.2.1. 制定 个人数据隐私保护管理体系 方针

最高管理者应制定、形成文件、实施和保持 个人数据隐私保护管理体系 方针应经最高管理者批准，并保留批准记录：

1) 适应组织的宗旨和环境并支持其战略方向；
2) 为建立 个人数据隐私保护管理体系 目标提供框架；
3) 包括满足适用 个人数据隐私保护管理体系 要求（如法律法规、监管要求、相关方要求）的承诺；
4) 包括持续改进 个人数据隐私保护管理体系 的承诺；
5) 包括预防 安全事故、保护人员安全和健康的承诺。

5.2.2. 沟通 个人数据隐私保护管理体系 方针应：

1) 可获取 个人数据隐私保护管理体系 并保持成文信息；
2) 个人数据隐私保护管理体系 在组织内得到沟通、理解和应用；
3) 适宜时， 个人数据隐私保护管理体系 可为有关相关方所获取（如PII主体、监管机构）。

5.3. 组织的岗位、职责和权限

5.3.1. 最高管理者应以文件形式明确并分配 个人数据隐私保护管理体系 相关岗位的职责、权限。组织应保留岗位职责分配表，并确保相关人员知晓。

5.3.2. 最高管理者应指定一名或多名管理者，不论其是否负有其他职责，应使其具有以下方面的岗位、职责和权限，以确保：

1) 个人数据隐私保护管理体系 符合本技术规范的要求；
2) 协调与 个人数据隐私保护管理体系 有关的内部和外部沟通，确保各过程获得其预期输出；
3) 报告 个人数据隐私保护管理体系 的绩效以及改进机会(见9.1.监视、测量、分析和评价),特别是向最高管理者报告；
4) 确保在整个组织中提高对 个人数据隐私保护管理体系 重要性的意识；
5) 协调与 个人数据隐私保护管理体系 有关的内部和外部沟通（特别是与PII主体和监管机构），并作为监管机构的联络点。
6) 确保在策划和实施 个人数据隐私保护管理体系 变更时保持其完整性。

6. 策划

6.1. 应对风险和机遇的措施

6.1.1. 在策划 个人数据隐私保护管理体系 时，组织应考虑到4.1和4.2所提及的因素和要求，并确定需要应对的风险和机遇，以：

1) 确保 个人数据隐私保护管理体系 能够实现其预期结果；
2) 增强有利影响；
3) 预防或减少不利影响（如I泄露、合规处罚、客户流失、声誉损害）；
4) 实现持续改进。

6.1.2. 组织应建立并保持合规义务登记册，以识别和跟踪与 个人数据隐私保护管理体系 相关的法律法规、标准及其他要求；

6.1.3. 组织应策划：

1) 应对这些风险和机遇的措施；
2) 在 个人数据隐私保护管理体系 过程中整合并实施这些措施(见4.4.条款)；
3) 评价这些措施的有效性。

6.1.4. 隐私风险评估

1) 组织应定义并应用风险评估过程，以建立并维护风险准则（包括风险接受准则和评估实施准则）；
2) 识别与PII处理相关的隐私风险（如未经授权的访问、数据泄露、数据滥用、合规风险、数据主体权利无法实现）；分析并评价风险。
3) 风险评估应特别考虑PII泄露对PII主体权利和自由的影响。
4) 组织应保留有关风险评估过程的文件化信息。

6.1.5. 应对措施应与风险和机遇对产品和服务符合性的潜在影响相适应。

1) 应对风险可选择规避风险，为寻求机遇承担风险，消除风险源，改变风险的可能性或后果，分担风险，或通过信息充分的决策而保留风险。
2) 机遇可能导致采用新实践、推出新产品、开辟新市场、赢得新顾客，建立合作伙伴关系、利用新技术和其他可行之处，以应对组织或其顾客的需求。

6.2. 个人数据隐私保护管理体系 目标及其实现的策划

6.2.1. 组织应针对相关职能、层次和 个人数据隐私保护管理体系 所需的过程建立 个人数据隐私保护管理体系 的目标。

1) 个人数据隐私保护管理体系 目标应：
   ① 与 个人数据隐私保护管理体系 方针保持一致；
   ② 可测量（如PII泄露事件数、投诉率、培训完成率、审计发现项关闭率、数据主体请求响应时间）；
   ③ 考虑适用的要求；
   ④ 予以监视；
   ⑤ 予以沟通；
   ⑥ 视情况予以适时更新。
2) 组织应保持有关 个人数据隐私保护管理体系 目标的成文信息。

6.2.2. 策划如何实现 个人数据隐私保护管理体系 目标时，组织应确定：

1) 要做什么；
2) 需要什么资源；
3) 由谁负责；
4) 何时完成；
5) 如何评价结果。

6.3. 变更的策划

当组织确定需要对 个人数据隐私保护管理体系 进行变更时（如如引入新的PII处理活动、外包PII处理、法律法规重大变更、新增PII类型），变更应按所策划的方式实施。组织应考虑：

1) 变更目的及其潜在后果；
2) 个人数据隐私保护管理体系 的完整性；

3) 资源的可获得性；
4) 职责和权限的分配或再分配。

7. 支持

7.1. 资源

7.1.1. 总则

1) 组织应确定并提供所需的资源，以建立、实施、保持和持续改进 个人数据隐私保护管理体系 。组织应保留资源评估与配置的记录。
2) 组织资源包括：具备相应能力的人员（数据保护官、隐私保护专家等）、技术基础设施（加密工具、访问控制系统、日志审计系统、数据防泄露系统等）、过程运行环境、监视和测量资源、财务资源、技术资源、信息等。
3) 组织应考虑：
   ① 现有内部资源的能力和局限；
   ② 需要从外部供方获得的资源。

7.1.2. 人员

组织应确定并配备所需的人员，以有效实施 个人数据隐私保护管理体系 ，并运行和控制其过程。关键岗位应明确任职要求并保留人员资质证明。

7.2. 能力

7.2.1. 组织必须：

1) 确定在其控制下工作的人员所需具备的能力（如隐私法规、数据保护技术、数据主体权利响应流程），这些人员从事的工作影响 个人数据隐私保护管理体系 绩效和有效性；
2) 基于适当的教育、培训或经验，确保这些人员是具备所需的能力；
3) 适用时，采取措施以获得所需的能力，并评价措施的有效性；
4) 保留适当的成文信息作为人员能力的证据；
5) 每年至少一次对能力需求进行评审。

7.2.2. 适用措施可包括：

1) 建立并维护全面的培训与意识策略，确保人员理解其隐私保护责任和程序。
2) 实施定期（如年度） 的、有针对性的、基于角色的隐私保护培训。
3) 在发生隐私事件后，实施针对性的强化培训。
4) 确保人员签字确认（手动或电子） 接受隐私保护责任的承诺。
5) 保留适当的文件化信息作为能力的证据（如培训记录、认证证书、签字确认记录）。

注：能够访问PII的个人应承担保密义务（根据ISO/IEC 29151:2017附录A.10.1）。

7.3. 意识

组织应通过培训、宣传、会议等方式，确保在其控制下工作的人员知晓以下内容。组织应保留培训记录和培训签到表。

1) 个人数据隐私保护管理体系 的培训方针
2) 与 个人数据隐私保护管理体系 相关的培训目标；
3) 组织对 个人数据隐私保护管理体系 有效性的贡献，包括改进绩效的益处；
4) 不符合 个人数据隐私保护管理体系 认证技术规范要求的后果；
5) 在 个人数据隐私保护管理体系 过程中个人的角色和职责；

6) 报告 个人数据隐私保护管理体系 和潜在危险相关的程序（尤其是对PII主体和组织的风险）。

7.4. 沟通

7.4.1. 组织应确定与 个人数据隐私保护管理体系 相关的内部和外部沟通，包括但不限于：

1) 沟通什么（如隐私政策、PII处理信息、数据泄露通知、数据主体请求）；
2) 何时沟通；
3) 与谁沟通；
4) 如何沟通；
5) 谁来沟通。

7.4.2. 组织应建立、实施和保持程序，建立与PII主体关于其PII处理的沟通机制，以及向监管机构报告数据泄露的机制。组织应保留沟通记录（如通知、报告、会议纪要）。

7.5. 成文信息

7.5.1. 总则

1) 组织的管理体系成文信息必须包括 个人数据隐私保护管理体系 认证技术规范要求的文件（如PIPMS手册、风险评估报告、风险处置计划、适用性声明、隐私政策、同意记录、数据主体请求处理记录等）及组织确定的 个人数据隐私保护管理体系 有效运行所需的文件（如PII处理活动记录、数据保护影响评估报告）。
2) 对于不同组织， 个人数据隐私保护管理体系 成文信息的多少与详略程度可以不同，取决于：
   ① 组织的规模，以及活动、过程、产品和服务的类型；
   ② 过程及其相互作用的复杂程度；
   ③ 人员的能力。

7.5.2. 创建和更新

在创建和更新成文信息时，组织应确保适当的标识和说明(如标题、日期、作者、索引编号)、格式(如语言、软件版本、图表)、载体(如纸质的、电子的)以及评审和批准，以保持适宜性和充分性。

7.5.3. 成文信息的控制

组织应建立并保持成文信息控制程序，以确保：在需要的场合和时机，均可获得并适用；予以妥善保护。组织应保留成文信息分发、变更、处置的记录。

1) 应控制 个人数据隐私保护管理体系 所要求的成文信息，以确保：
   ① 在需要的场合和时机，均可获得并适用；
   ② 予以妥善保护(如防止泄密、不当使用或缺失)。
2) 为控制成文信息，适用时，组织应进行下列活动：
   ① 分发、访问、检索和使用；
   ② 存储和防护，包括保持可读性；
   ③ 更改控制(如版本控制)；
   ④ 保留和处置（PII相关的文件化信息的保留期限应符合法规要求）。
3) 对于组织确定的策划和运行 个人数据隐私保护管理体系 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。
4) 对所保留的、作为符合性证据的成文信息应予以保护，防止非预期的更改。

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. 运行策划和控制

8.1.1. 组织应策划、实施和控制满足 个人数据隐私保护管理体系 所需的全过程，并实施第6章所确定的措施，组织必须通过以下措施对所需的过程进行策划、实施和控制。组织应保留运行策划的输出。

1) 确定 个人数据隐私保护管理体系 的工作要求，建立下列内容的准则：
   ① 过程准则（如数据处理准则、隐私保护要求、信息记录要求）；
   ② 个人数据隐私保护管理体系 工作的接收准则；
      a. 确定 个人数据隐私保护管理体系 所需的资源；
      b. 按照 个人数据隐私保护管理体系 准则实施过程控制；
   ③ 在必要的范围和程度上，确定并保持、保留成文信息
   ④ 确信过程已经按策划进行；
   ⑤ 证实 个人数据隐私保护管理体系 工作符合要求。

8.1.2. 策划的输出应适合于组织的运行。

8.1.3. 组织应控制策划的变更，评审非预期变更的后果，必要时，采取措施减轻不利影响。组织应确保外包过程受控。

8.2. 隐私风险评估

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发生时（如新PII处理活动上线、法律法规更新），执行隐私风险评估。应保留风险评估结果的文件化信息。

8.3. 隐私风险处置

组织应实现隐私风险处置计划。应保留风险处置结果的文件化信息。

8.4. 个人数据隐私保护特定控制措施（依据ISO/IEC 29151:2017）

组织应按本章节要求实施和运行特定的隐私保护控制措施，这些措施补充和细化了ISO/IEC 27001:2022附录A中的相关控制。

8.4.1. 隐私保护策略（依据ISO/IEC 29151:2017第5章）

1) 控制：应制定和维护隐私保护策略，以管理组织的PII保护。
2) 实施要求：
   ① 制定并维护文件化的《隐私保护策略》，该策略应由最高管理层批准。
   ② 该策略应涵盖：PII保护的目标和原则；PII收集和处理的透明度；数据最小化原则；数据主体权利；数据保留与销毁；数据泄露响应；合规要求。
   ③ 隐私保护负责人应定期评估并向最高管理层报告隐私保护策略和PIPMS的绩效，包括合规状态、风险状况和改进机会。
   ④ 该策略应定期评审和更新（至少每年一次）。

8.4.2. PII的识别与分类（依据ISO/IEC 29151:2017第6章）

1) 控制：应识别和分类组织处理的所有PII。
2) 实施要求：
   ① 建立并维护PII处理活动记录（ROPA），记录所有PII处理活动。ROPA应包含但不限于：
      a. 处理目的
      b. PII类别（如个人基本信息、敏感信息）
      c. PII主体类别（如员工、客户、供应商）
      d. PII接收方或接收方类别

e. PII保留期限

f. 所采取的技术和组织安全措施的一般描述

② 对PII进行分类（如一般PII、敏感PII），并根据分类实施不同的保护措施。

8.4.3. 同意管理（依据ISO/IEC 29151:2017第7.2.3条及附录A.3.1）

1) 控制：应在处理PII前获得PII主体的有效同意。

2) 实施要求：

① 确定何时以及如何获得PII主体的同意。

② 以清晰、明确的方式向PII主体提供同意请求，确保其充分知情。

③ 记录并保存PII主体的同意记录，包括同意的时间、方式和内容。

④ 提供修改或撤销同意的机制。

8.4.4. 数据主体权利响应（依据ISO/IEC 29151:2017第7.3条及附录A.9, A.10）

1) 控制：应建立机制以响应PII主体行使权利（访问、更正、删除、限制处理、数据可携带、反对）的请求。

2) 实施要求：

① 建立《数据主体权利响应程序》，明确处理请求的流程、时限和责任人。

② 在法律规定的时间内响应PII主体的请求。

③ 验证请求者的身份。

④ 记录所有数据主体请求及其处理结果。

8.4.5. 数据最小化与保留（依据ISO/IEC 29151:2017第7.4条及附录A.5, A.7）

1) 控制：应仅收集和处理实现特定目的所必需的PII，并在不再需要时安全删除。

2) 实施要求：

① 限制收集：仅收集实现明确目的所必需的PII。

② 限制处理：仅根据已声明的目的处理PII。

③ 数据最小化目标：设定数据最小化目标，定期审查PII收集的必要性。

④ 保留：制定并实施PII保留策略，明确不同类型PII的保留期限。

⑤ 处置：当PII不再需要时，应安全地删除或匿名化处理。

8.4.6. 访问控制——PII（依据ISO/IEC 29151:2017第8章及附录A.10.10）

1) 控制：应实施访问控制措施，防止对PII的未授权访问。

2) 实施要求：

① 对所有经授权可访问PII的用户，维护其用户配置文件。

② 严格执行最小权限原则，确保用户仅获得执行其职责所必需的访问权限。

③ 实施用户ID的独立使用，每个有权访问PII的个人应拥有唯一的用户ID。

④ 已停用或过期的用户ID不得重新分配给其他个人。

8.4.7. 加密与密钥管理（依据ISO/IEC 29151:2017第10章及附录A.11.4, A.11.5）

1) 控制：应使用加密技术保护PII的保密性。

2) 实施要求：

① 应实施静态数据加密：对存储PII的数据库、文件系统或存储介质进行加密。

② 应实施传输中数据加密：对通过网络传输的PII进行加密（如TLS/SSL）。

③ 应管理加密密钥：使用企业级密钥管理系统（KMS）；密钥生成、存储、分发、轮换和销毁应遵循安全策略。

8.4.8. 数据泄露事件管理（依据ISO/IEC 29151:2017第16章及附录A.10.1）

1) 控制：应建立机制以管理PII数据泄露事件。

2) 实施要求：

① 建立《PII数据泄露响应与通知程序》。

② 在发生涉及PII的数据泄露时，应及时通知相关PII控制者（如适用）和监管机构。

③ 通知应包含泄露的性质、涉及的PII类型、已采取或拟采取的补救措施等。

④ 信息安全事件应触发以确定是否涉及PII数据泄露的审查。

8.4.9. 分包商与第三方管理（依据ISO/IEC 29151:2017第15章及附录A.11.2, A.11.3）

1) 控制：应确保分包商具有足够能力保护PII。

2) 实施要求：

① 披露与同意：在使用分包商处理PII之前，应向相关PII控制者（如适用）披露分包商的使用情况。

② 合同约束：与处理PII的任何分包商签订的合同，应规定满足本组织隐私保护义务的最低技术和组织措施。

③ 监控与审计：对分包商的PII处理活动进行监控和定期审计，确保其满足合同要求。

8.4.10. 隐私影响评估（PIA）（依据ISO/IEC 29151:2017第7.2.5条）

1) 控制：应在引入新的PII处理活动或对现有处理活动进行重大变更时，进行隐私影响评估。

2) 实施要求：

① 建立《隐私影响评估程序》。

② 在启动新的PII处理项目或对现有处理进行重大变更时，执行PIA。

③ PIA应识别和评估隐私风险，并提出风险处置措施。

④ 保留PIA报告作为文件化信息。

9. 绩效评价

9.1. 监视、测量、分析和评价

9.1.1. 总则

1) 组织应建立并保持监视、测量、分析和评价的程序，明确：

① 需要监视和测量什么（如包括隐私保护过程绩效、PII安全事件、数据主体请求处理时效、培训完成率、合规性偏差等）；

② 需要用什么方法进行监视、测量、分析和评价的方法，以确保结果有效；

③ 确保用于监视与测量的资源（如审计工具、日志分析系统）的准确性；

④ 何时实施监视和测量；

⑤ 何时对监视和测量的结果进行分析和评价。

2) 组织应保留监视和测量记录。

3) 组织应评价 个人数据隐私保护管理体系 的绩效和有效性，并保留适当的成文信息，以作为结果的证据。

9.1.2. 合规性评价

1) 组织应根据法规要求和相关方对 个人数据隐私保护管理体系 的要求，建立、实施并保持程序，以定期评价组织对适用法律法规、标准及其他要求的遵守情况。

2) 合规性评价应至少每年进行一次，并保留合规性评价报告作为成文信息。

3) 合规性评价应由指定部门或人员组织实施，评价结果应报告最高管理者。

9.2. 内部审核

9.2.1. 组织应按照策划的时间间隔（至少每年一次） 进行内部审核。

9.2.2. 组织应建立并保持内部审核方案，审核员应具备相应能力且不得审核自己的工作。以提供有关 个人数据隐私保护管理体系 是否符合本技术规范的要求，以及是否得到有效实施和保持的信息：

9.2.3. 在进行内部审核时，组织应：

1) 依据有关过程的重要性、对组织产生影响的变化和以往的审核结果，策划、制定、实施和保持审核方案，审核方案包括频次、方法、职责、策划要求和报告；
2) 规定每次审核的审核准则和范围；
3) 选择审核员并实施审核，以确保审核过程客观公正；
4) 确保将审核结果报告给相关管理者；
5) 及时采取适当的纠正和纠正措施；
6) 保留成文信息，作为实施审核方案以及审核结果的证据。

注：相关指南参见 GB/T 19011。

9.3. 管理评审

最高管理者应按照策划的时间间隔（至少每年一次）对组织的 个人数据隐私保护管理体系 进行评审。以确保其持续的适宜性、充分 性和有效性，并与组织的战略方向保持一致。组织应保留管理评审会议纪要和输出的决定。

9.3.1. 管理评审输入

策划和实施管理评审时应考虑下列内容：

1) 以往管理评审所采取措施的情况；
2) 与 个人数据隐私保护管理体系 相关的内外部因素的变化（如新的隐私法规、PII处理活动变更）；
3) 有关 个人数据隐私保护管理体系 绩效和有效性的信息，包括：
   ① PII泄露事件趋势；
   ② 数据主体投诉率；
   ③ 外部供方（如分包商）的绩效；
   ④ 合规性偏差；
   ⑤ 风险评估与处置状态；
   ⑥ 改进机会等。
4) 资源的充分性；
5) 应对风险和机遇所采取措施的有效性；
6) 持续改进的机会。

9.3.2. 管理评审的输出应包括与下列事项相关的决定和措施：

1) 改进的机会；
2) 个人数据隐私保护管理体系 所需的变更；
3) 资源需求。
4) 组织应保留成文信息，作为管理评审结果的证据。

10. 改进

10.1. 不合格与纠正措施

10.1.1. 当发生不合格项时（如通过定期隐私影响评估，预防新处理活动带来的隐私风险），组织应在规定时限内：

1) 对不符合项做出应对，并在适用时：
   ① 采取措施以控制和纠正不符合项；
   ② 处置后果。
2) 通过下列活动，评价是否需要采取措施，以消除产生不符合项的原因，避免其再次发生或者在其 他场合发生：
   ① 评审和分析不符合项；
   ② 确定不符合项的原因；
   ③ 确定是否存在或可能发生类似的不符合项。
3) 实施所需的措施；
4) 评审所采取的纠正措施的有效性；
5) 需要时，更新在策划期间确定的风险和机遇；
6) 需要时，变更 个人数据隐私保护管理体系 。

10.1.2. 组织应基于管理评审输出、内审结果、合规性评价等，制定改进计划并跟踪落实。

10.1.3. 纠正措施应与不符合项所产生的影响相适应，组织应保留成文信息，作为下列事项的证据：

1) 不符合项的性质以及随后所采取的措施；
2) 纠正措施的结果。

10.2. 持续改进

10.2.1. 组织应持续改进 个人数据隐私保护管理体系 的适宜性、充分性和有效性。

10.2.2. 组织应考虑分析和评价的结果以及管理评审的输出，确定是否存在持续改进的需求或机遇，并将其作为持续改进变更管理的一部分加以实施。

11. 其他

11.1. 建立并保持程序

组织应形成文件化的程序文件，明确活动的目的、范围、职责、流程和要求。

11.2. 保留成文信息

组织应保存记录（如纸质或电子），以证明活动已按策划实施。记录应清晰、可追溯、便于检索。

11.3. 指定责任人

组织应在相关文件中明确具体岗位或人员的职责，并确保其知晓。

11.4. 时限要求

本文件中“定期”如无特别说明，默认为“至少每年一次”；“及时”指在合理可行的情况下尽快处理，最长不超过30日。

————————————————