ICS 35.020
L70

DB21

辽　宁　省　地　方　标　准

DB 21/T 1628.8—2018

信息安全 个人信息安全管理体系 第8部分：过程管理指南

Information security-Personal information security management system-Part8: Process management guidelines

2018－01－22 发布　　2018－02－22 实施

辽宁省质量技术监督局　发布

目　　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　要求 1
5　过程管理 1
5.1　方法 1
5.2　计划（P） 1
5.3　实施（D） 3
6　过程改进 4
6.1　监控和内审（C） 4
6.2　完善和改进（A） 4
7　文档管理 5

前　言

DB21/T 1628 分为 8 部分：

——信息安全 个人信息保护规范（信息安全 个人信息安全管理体系 第 1 部分：通用要求）

——信息安全 个人信息安全管理体系 第 2 部分：实施指南

——信息安全 个人信息安全管理体系 第 3 部分：个人信息数据库管理指南

——信息安全 个人信息安全管理体系 第 4 部分：个人信息管理文档管理指南

——信息安全 个人信息安全管理体系 第 5 部分：个人信息安全风险管理指南

——信息安全 个人信息安全管理体系 第 6 部分：安全技术实施指南

——信息安全 个人信息安全管理体系 第 7 部分：内审实施指南

——信息安全 个人信息安全管理体系 第 8 部分：过程管理指南等。

本部分是 DB21/T 1628 的第 8 部分。

本部分按照 GB/T 1.1—2009《标准化工作导则　第 1 部分：标准的结构与编写》给出的规则起草。

本部分由大连市质量技术监督局提出。

本部分由辽宁省工业和信息化委员会归口。

本部分主要起草单位：大连软件行业协会、大连交通大学、大连市计算机学会。

本部分主要起草人：郎庆斌、孙鹏、尹宏、丁宗安、董晶、杨万清、杨莉、郭玉梅、曹剑、孙毅、王小庚。

信息安全 个人信息安全管理体系 第8部分：过程管理指南

1 范围

本标准为个人信息安全管理体系构建、实施、运行的过程管理提供指导和通用规则。

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，仅所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。

GB/T 19001/ISO 9001 质量管理体系 要求

GB/T 22080 信息技术 安全技术 信息安全管理体系 要求

GB/T 22081 信息技术 安全技术 信息安全管理实用规则

DB21/T 1628.1 信息安全 个人信息保护规范

DB21/T 1628.2 信息安全 个人信息安全管理体系 第2部分：实施指南

DB21/T 1628.4 信息安全 个人信息安全管理体系 第4部分：个人信息管理文档管理指南

DB21/T 1628.5 信息安全 个人信息安全管理体系 第5部分：个人信息安全风险管理指南

DB21/T 1628.6 信息安全 个人信息安全管理体系 第6部分：安全技术实施指南

DB21/T 1628.7 信息安全 个人信息安全管理体系 第7部分：内审实施指南

3 术语和定义

GB/T 19001/ISO 9001、DB21/T 1628界定的术语和定义适用于本文件。

4 要求

本指南遵循DB21/T 1628.1确立的个人信息管理原则和要求，亦遵循DB21/T 1628.2确立的实施细则，重点描述和指导PISMS过程管理的约束规则。

PISMS过程管理，应同时使用DB21/T 1628.1、DB21/T 1628.2和本指南，并参照DB21/T 1628系列其它标准。

5 过程管理

5.1 方法

应遵循DB21/T 1628.2 5描述的PISMS过程管理方法，采用PDCA模式管理、控制PISMS过程、活动和行为。

5.2 计划（P）

5.2.1 要求

遵循DB21/T 1628.2 5.2，应在这一阶段根据个人信息管理者的整体目标，确立个人信息管理目标和方针，实施个人信息管理计划，构建PISMS。

5.2.2 最高管理者

遵循DB21/T 1628.2 10.5.1.2：

a）最高管理者的认知，应是PISMS持续、稳定运行的关键；

b）最高管理者的认知，应是PISMS实施并持续过程改进的决策者；

c）最高管理者应提供资金、管理、资源等各个方面的切实支持；

d）最高管理者应在适合的情况下理解、参与PISMS实施、运行，创造全员参与的环境；

e）最高管理者应选择有能力、务实的个人信息管理者代表，并赋予相应权限等。

5.2.3 目标和方针

应确立个人信息管理目标和管理方针：

a）明确构建PISMS的方向和应实现的状态；

b）宜将目标分解为PISMS相关的组织、计划和各项活动，实施目标管理；

c）应明确个人信息管理方针和策略，确定简便易行的行动计划；

d）应保证个人信息管理目标的实用性、可用性；

e）应保证个人信息管理方针的易用性、可操作性和有效性等。

5.2.4 机制设计

PISMS内各个相互关联的功能机制设计，应保证：

a）约束个人信息管理者的日常管理、业务活动和员工与个人信息安全相关的行为；

b）激励个人信息管理者的日常管理、业务活动和员工保证个人信息安全的行为；

c）机制设计应合理、适宜，符合个人信息管理者的实际；

d）机制设计应保证约束、激励的有效性等。

5.2.5 质量保证

PISMS设计应包括相应的质量管理活动：

a）质量目标：设定质量管理目标，保证PISMS的可靠性、有效性；

b）质量控制：通过监控、跟踪等手段，监督PISMS构建、实施和运行，及时消除质量隐患；

c）质量保证：提供保证PISMS符合个人信息安全相关法规、标准和安全承诺的保证措施；

d）质量改进：为提高个人信息管理相关过程、活动的个人信息安全可信度所提供的提高PISM效能的措施等。

5.2.6 资源配置

应保证实现个人信息安全所需相关资源，遵循DB21/T 1628.2：

a）应识别PISMS所需相关资源；

b）应识别这些资源的风险；

c）应确定相关资源的范围；

d）应根据PISM构建、实施、运行的需要，合理配置资源；

e）应确定相关资源的范围、风险识别充分、适宜；

f）应确定资源配置、利用的合理性、安全性等。

5.3 实施（D）

5.3.1 要求

遵循DB21/T 1628.2 5.2，应在这一阶段实施和运行PISMS，是保证PISMS各项机制有效运行，满足质量目标的过程保证。

5.3.2 风险管理

风险管理的有效性，应是个人信息安全的关键。应遵循DB21/T 1628.5：

a）识别、分析、评估与个人信息安全相关的所有风险，包括资源、管理、业务、环境、行为等；

b）采取适宜的风险应对措施，降低、规避或弱化风险，保证风险的可控、可接受；

c）确定风险评估、风险应对措施是充分、适宜、有效的。

5.3.3 管理机制

管理机制的有效性，应是保证PISMS约束机制的关键：

a）管理机制应包括PISMS的结构、功能、作用、约束规则、行为等；

b）应在PISMS机制设计、建设中，遵循DB21/T 1628.1、DB21/T 1628.2及相关标准，采取适宜的质量保证措施；

c）应确定管理机制所有功能适宜、可用、有效和易用。

5.3.4 保护机制

保护机制的有效性，应是保证个人信息安全和个人信息主体权益的关键：

a）个人信息的关联因素，主要包括：

1）个人信息管理者内部的各种因素；

2）个人信息管理者外部各种因素的作用和影响；

3）个人信息管理者的各种环境制约等；

b）应在个人信息全生命周期各个关键环节，如收集、处理、使用、利用等环节，依据DB21/T 1628.1及相关法规、标准，针对不同因素采取相应的管理、保护措施；

c）应确定保护机制各项功能有效、可用、安全、可靠。

5.3.5 安全机制

安全机制的有效性，应是保证PISMS安全、可靠运行的关键：

a）应确定个人信息安全风险评估的结果；

b）应分析、判断个人信息管理者的现状和需求、个人信息特征等；

c）应依据GB/T 22080、GB/T 22081（等同采用ISO/IEC 27001、ISO/IEC 27002）、DB21/T 1628.1、DB21/T 1628.6等标准，对环境、物理、行为、技术、管理等的安全，采取相应的管理措施；

d）应确定安全机制合理、有效、可用和安全。

5.3.6 效果评估

应评估实施、运行阶段的效果，以保证PISMS的充分和有效。评估主要应包括：

a）最高管理者和管理者代表的认知、行为；

b）风险管理效能评估；

c）管理机制效能评估；

d）保护机制效能评估；

e）PISMS的相关活动、行为评估；
f）安全机制效能评估等等。

6 过程改进

6.1 监控和内审（C）

6.1.1 要求

依据DB21/T 1628.1 第12章、DB/T 1628.7 6.2.5，内审机构应全程监控、检查PISMS的构建、实施、运行过程。监控和内审（C）应参与PDCA各个阶段的循环。

a）PISMS构建、实施、运行相应的管理、技术等充分、有效；
b）PISMS构建、实施、运行相应的活动、行为规范；
c）过程管理方法规范、科学、有效。

6.1.2 跟踪、监控

应依据DB21/T 1628.1第12章、DB/T 1628.2第18章，跟踪、监控PISMS构建、实施、运行过程中安全风险变化。

a）已识别风险的变化：已识别风险可因条件、环境、影响、资源、管理等的变化发生变化，应采取相应的控制措施；

b）潜在风险的发生：可能存在的潜在风险可在满足一定条件、环境或在激励下发生，应制定应急预案并采取相应的应对和控制措施；

c）新的风险：管理、业务、资源、环境等的变化可引发新的风险，应及时识别、分析、评估，并采取相应的应对和控制措施。

6.1.3 内审

应依据DB/T 1628.7，建立有效的内部审计监控机制。应确定内审的合理性、有效性和充分性。

6.1.4 符合性

应确定PISMS设计、构建与PISMS实施、运行的符合性、一致性：

a）PISMS设计、构建与个人信息管理者的实际需求的符合性；
b）PISMS设计、构建与个人信息管理者的管理、业务发展的一致性；
c）PISMS设计、构建与个人信息管理者的员工权益的一致性；
d）PISMS设计、构建与个人信息管理者管理、业务相关的个人信息主体的期望的一致性。

6.2 完善和改进（A）

6.2.1 要求

应依据DB21/T 1628.1第12章、DB/T 1628.2第18章，改进、完善PISMS，并在P、D、C各个阶段的自循环中，实时改进、消除缺陷、漏洞和问题。

6.2.2 改进机制

过程改进应是保证PISMS持续改进、完善的有效机制：

a）过程的主要元素应包括人、资源、工具、方法、流程等及相关因素；

b）应根据个人信息安全目标和个人信息管理者的实际，采用PDCA模式，持续改进过程的主要元素。

6.2.3 意见和反馈

在PISMS构建、实施和运行中，应认真接受个人信息主体、个人信息管理者内外部的意见、建议，选择、应用有益的部分，并反馈意见、建议的应用、效果等，以推进PISMS的改进和完善。

6.2.4 沟通和交流

在PISMS构建、实施和运行中，应对个人信息管理及PISMS相关的体系建设、机制功能、保护措施、安全措施、改进措施等，与个人信息管理者内部及内、外部之间，及时沟通、交流，以改进、完善PISMS。

6.2.5 持续改进

PISMS应随着管理、业务、环境、外部因素等的变化，应用PDCA模式，适时改进、完善，保证PISMS的适用性、科学性。

7 文档管理

应根据DB21/T 1628.1 8.5和DB21/T 1628.4，建立个人信息安全管理体系过程管理相关文档的管理机制。