ICS 35.020
L70

DB21

辽　宁　省　地　方　标　准

DB 21/ T XXXX—XXXX

信息安全 个人信息安全管理体系 附则

Information security-Personal information security management system-Annex

（征求意见稿）

（本稿完成日期：2017-5-20）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

辽宁省质量技术监督局　发布

目　　次

前　言

本标准按照 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。

本标准由大连市经济和信息化委员会提出。

本标准由辽宁省工业和信息化委员会归口。

本标准主要起草单位：大连软件行业协会、大连交通大学、大连市计算机学会。

本标准主要起草人：郎庆斌、孙鹏、尹宏、丁宗安、董晶、杨万清、杨莉、郭玉梅、曹剑、司丹、孙毅、王小庚。

引　言

在个人信息管理者的管理生态中，寄生多体系管理要素，互相制约、影响，造成资源浪费、管理交叉，冗余、繁复。然因标准框架、管理痼疾……多因素限制，尚无法形成管理体系的一体化。

本标准旨在说明PISMS与QMS、SMS、ISMS的异同，以期在个人信息安全实践中建立同一性规范，在个人信息安全标准体系实施中，兼顾体系间的共性和个性。

本标准是DB21/T 1628系列标准实施的附加说明。本标准涵盖DB21/T 1628标准体系，为标准实施提供参考和指导。与标准体系构成框架是平行的。

信息安全 个人信息安全管理体系 附则

1 范围

本标准为个人信息安全管理体系兼容质量管理体系、服务管理体系、信息安全管理体系提供借鉴和指导。

本标准适用于自动或非自动处理全部或部分个人信息的机关、企业、事业、社会团体等组织。

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 质量管理体系 要求

GB/T 24405.1 信息技术 服务管理 第1部分：规范

GB/T 24405.2 信息技术 服务管理 第2部分：实践规则

GBT 22080 信息技术 安全技术 信息安全管理体系 要求

GBT 22081 信息技术 安全技术 信息安全控制实用规则

3 术语和定义

GB/T 19001、GB/T 24405、GB/T 22080、GB/T 22081、DB21/T 1628界定的术语和定义适用于本文件。

4 概述

DB21/T 1628个人信息安全标准系列，兼容GB/T 19001（等同采用ISO/IEC 9001）、GB/T 24405.1、GB/T 24405.2（等同采用ISO/IEC 20000.1、ISO/IEC 20000.2）、及GB/T 22080、GB/T 22081（等同采用ISO/IEC 27001、ISO/IEC 27002）的思想和方法，为多种管理体系的融和实施，奠定适宜的基础。

个人信息安全标准系列，以管理为主线，以个人信息生命周期为导向，以个人信息安全和个人信息管理质量为目标，规定个人信息生命周期内管理要素的约束规则。因而，个人信息安全标准系列与GB/T 19001、GB/T 24405.1、GB/T 24405.2、GB/T 22080、GB/T 22081具有类同的管理、服务和安全管理要素。

本标准建立PISMS与QMS、SMS、ISMS的同一性规范。

5 同一性设计

5.1 PISMS 设计

5.1.1 目的

个人信息安全管理体系是个人信息管理的结果，其基本目的应是满足个人信息管理的需要，指导各类组织建立健全各类管理机制，协调各类资源，充分保障个人信息主体的权利，保障个人信息管理业务的稳定运行。

5.1.2 要素

5.1.2.1 综述

PISMS构成要素的基础：

a）PISMS是基于个人信息生命周期展开的；

b）个人信息生命周期是个人信息管理者向个人信息主体提供个人信息相关的服务管理的过程；

c）在服务管理过程中，个人信息主体感知服务能力和服务质量；

d）通过服务能力和服务质量的管控，实现个人信息安全。

5.1.2.2 构成要素

基于GB/T 24405.1、GB/T 24405.2和GB/T 19001，PISMS构成要素，主要包括：

a）目标和基本原则：明确管理的目标和管理的基本原则；

b）管理策略：方针、责任、能力等；

c）组织机构：明确管理机构、组织方式、职能、职责、权限等；

d）管理机制：角色、制度、培训、文档等；

e）人员管理：可调配、使用的相关人员管理；

f）资源管理：体系相关、可协调、调配资源管理；

g）过程管理：体系建立、实施过程管理；

h）过程改进：体系建立、实施过程监控、内审、改进等。

5.2 体系综述

5.2.1 GB/T 19001

5.2.1.1 特征

GB/T 19001等同采用ISO/IEC 9001，其特征主要包括：

a）广泛适用：可适用于所有产品类别、不同规模和各种类型的组织，并可根据实际需要剪裁某些质量管理体系要求；

b）管理模式：质量管理体系模式，以过程为基础，强调过程间的联系和相互作用，逻辑性更强，相关性更好；

c）兼容性：强调质量管理体系与其它管理体系保持一致或融合，便于与其它管理体系相互兼容；

d）过程改进：更注重质量管理体系的有效性和持续改进等。

5.2.1.2 质量管理原则

GB/T 19001等同采用ISO/IEC 9001，明确在实施质量管理中必须遵循7项原则。

5.2.1.3 过程管理

在质量管理体系和质量管理过程中应用PDCA过程管理模式：

a）风险管理：应用PDCA管理模式中运用风险管理策略，实现过程和体系的有效管理和改进；

b）过程和要素：应用PDCA管理模式管理过程及过程中相互作用的要素，实现质量管理体系的目标。

5.2.1.4 构成要素

质量管理体系的构成要素，主要包括：

a）管理策略：包括质量方针、质量目标、管理承诺、职责与权限、策划、顾客需求、质量管理体系和管理评审等项内容；

b）资源管理：包括人力资源、信息资源、设施设备和工作环境等项内容；

c）过程管理：包括顾客需求转换、设计、采购、产品生产与服务提供的管理等项内容；

d）测量、分析与改进：包括资源评测、质量管理体系内审、产品监测和测量、过程监测和测量、不合格品控制、持续改进、纠正和预防措施等项内容等。

注1：产品，具有双重含义，可以表示有形的实物产品，也可以表示“服务”。

5.2.2 GB/T 24405

GB/T 24405（等同采用ISO/IEC 20000）以流程为中心、以用户满意和服务质量为核心，整合IT服务与业务流程，提高信息服务提供和支持的能力和水平：

a）引入GB/T 19001的质量管理思想，与QMS更协调、融合；

b）引入GBT 22080的信息安全管理思想，与ISMS更协调、融合；

c）引入GB/T 19001的术语、定义和构成要素，并依据服务管理的特征定义等。

5.2.3 综述

5.2.3.1 一般意义

GB/T 19001所规制的质量管理体系、质量管理思想和方法具有普适性，在遵从GB/T 24405实施服务管理中，规范SMS并融入质量管理思想和方法，可通过服务能力感知服务质量，亦为DB/T 1628的设计提供借鉴。

5.2.3.2 DB/T 1628

基于GB/T 19001、 GB/T 24405的规则设计，DB21/T 1628系列标准为PISMS设计了相应的可实施的规则：

a）遵从GB/T 24405 IT服务管理的基本思想和GB/T 19001质量管理原则，以服务管理为导向，关注个人信息生命周期内服务管理能力、服务管理质量；

b）依据GB/T 19001、 GB/T 24405，DB21/T 1628系列标准建构了PISMS的各项要素、过程等；

c）依据GB/T 19001、 GB/T 24405，DB21/T 1628系列标准规范了PISMS构成要素、过程的管理活动和行为，细粒度地建立了要素对应的各项管理规则。

5.2.4 GB/T 22080

5.2.4.1 综述

GB/T 22080等同采用ISO/IEC 27001，其特征应包括：

a）集成性：ISMS与组织（个人信息管理者）整体管理结构、管理过程集成一致，并构成关键要素；

b）兼容性：标准结构、体例、核心定义等与GB/T 19001对应，ISMS与GMS具有兼容性；

c）风险管理：基于风险管理过程的应用，降低潜在的安全风险，保证信息资产、业务等的安全等。

5.2.4.2 差异

DB21/T 1628系列遵从GB/T 19001、 GB/T 24405的思想和方法，融合GB/T 22080信息安全管理思想，因此，PISMS与ISMS是相似的，但二者存在差异：

a）基点不同：ISMS是基于信息资产的安全管理活动，GB/T 22080规范了基于信息资产安全的管理规则；PISMS是基于保障个人信息主体权益展开的相应管理活动或行为，DB21/T 1628系列规范了个人信息管理的相关规则；

b）资产相关性：个人信息安全亦与信息资产安全相关，但相关性体现个人信息的存在特征，及对信息资产的影响、变化；

c）复杂性：个人信息安全的复杂性表现为：

1）个人信息环境复杂、多变，呈现多样性；

2）个人信息存在形态多样化；

3）个人信息风险随环境、形态的多样化变化。

5.2.5 总论

个人信息管理者内可存在多种管理体系，与PISMS的关系可描述为：

a）GMS、SMS、ISMS和PISMS可并存（标准制定的现实）；

b）PISMS兼容了质量管理、服务管理和信息安全管理；

c）ISMS可以包容PISMS，但GB/T 22080、GB/T 22081不能完全包容个人信息管理；

d）GB/T 19001、 GB/T 24405亦不能包容个人信息管理；

e）若依据GB/T 19001、GB/T 24405、GB/T 22080、GB/T 22081等相关标准，分散个人信息管理，将增加个人信息存在风险、管理风险和管理成本；

f）可在ISMS认证中，兼顾DB21/T 1628系列的标准特征，实施统一认证管理。

附 录 A
（资料性附录）
管理体系标准条款对照表

DB21/T 1628		ISO9001	ISO20000.1	ISO27001	ISO27002
标准系列	章节	章节	章节	章节	章节
1 2	3.1.2 个人信息 6 个人信息				
1 2	3.1.4 个人信息主体 7 个人信息主体				
1 2	4 个人信息生命周期 8 个人信息生命周期		4.2 其它方运行过程的治理		
1 2	5 个人信息主体权利 7.4 权利				
1 2	6 个人信息管理者 9 个人信息管理者				
1	7 个人信息管理				
	7.2 原则				
	7.3 方针	5.2 质量方针	4.1.2 服务管理方针	5.2 方针	5 信息安全方针
	7.4 计划	6.2 质量目标和实现计划	6.6.1 信息安全方针		
	7.5 组织	5.1 领导力和承诺	4.1.1 管理承诺	5.1 领导与承诺	6 信息安全组织
		5.3 组织的角色职责和权限	4.1.3 权限职责沟通	5.3 组织的角色职责和权力	7.2.1 管理者职责
					7.3 任用的终止和变化
		7.4 沟通	4.1.4 管理者代表	7.4 沟通	
2	10 个人信息管理 10.3 管理边界	4 组织情境		4 组织的环境	
	10.5.4 相关团体的联系				6.1.3 与监管机构的联系 6.1.4 与特定利益集团的联系

1 2	7.5.3 个人信息安全管理体系 10.5.2 构建和管理PISMS	4.4 质量管理体系及其过程	4.5 建立和改进服务管理体系		
2	11 资源管理	7.1 资源	4.4 资源管理	7.1 资源	8 资产管理
1 2	8 管理机制 8.1 管理制度 8.2 人员管理 8.3 宣传教育 12 管理机制	 7.2 能力 7.3 意识	 4.4.2 人力资源	 7.2 能力 7.3 意识	 7 人力资源安全 7.2.2 信息安全意识、教育和培训
1 3	8.4 数据库管理 个人信息数据库管理指南				
1 4	8.5 文档管理 个人信息管理文档管理指南	7.5 文件化信息	4.3 文件管理	7.5 文档信息	
1 2	9 个人信息获取 13 获取过程				14 信息系统获取、开发和维护
1 2	10 个人信息处理 14 处理过程				6.1.5 项目管理中的信息安全 6.2.1 移动设备策略 6.2.2 远程工作 15.1 供应商关系中的信息安全

15	11.1 风险管理 风险管理指南	0.3.3 基于风险的思维 6.1 应对风险和机会的措施		6 计划 8.2 信息安全风险评估 8.3 信息安全风险处置
16	11 安全管理 安全技术实施指南		7 信息安全	9 访问控制 11 物理和环境安全 12 操作安全 13 通信安全
18	12 过程管理 12.3 应急管理 过程管理指南	0.3 过程方法	引言	16 信息安全事件管理
17	12.1 PISMS 内审 内审实施指南	9.2 内部审核 9.3 管理评审	4.5.4 监视和评审服务管理体系	9 绩效评价
12	12.2 过程改进 18 过程改进	10 改进	4.5.5 维护和改进服务管理体系	10 改进
2	管理和业务的连续性管理		6.3 服务连续性和可用性管理	17 信息安全与业务连续性管理