ICS 35.020
L 70

DB21

辽　宁　省　地　方　标　准

DB21/T 1628.1—2016
代替 DB21/T 1628.1-2012

信息安全　个人信息保护规范

Information Security-Specification for Personal Information Protection

2016－09－27 发布　　2016－11－27 实施

辽宁省质量技术监督局　发布

目　　次

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实施指南

——信息安全 个人信息数据库管理指南

——信息安全 个人信息管理文档管理指南

——信息安全 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安全技术实施指南

——信息安全 个人信息安全管理体系内审实施指南

——信息安全 个人信息安全管理体系过程管理指南等。

本部分是 DB21/T 1628 的第 1 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。

本部分代替 DB21/T 1628.1-2012《信息安全 个人信息保护规范》。与 DB21/T 1628.1-2012 相比，本部分除编辑性修改外，主要技术变化如下：

——标准结构修改，构建个人信息安全管理框架；

——标准粒度修订，剔除规章制度等部分过细的约束规则；

——适当跟踪新技术的发展，增加部分相关规则，如移动设备等；

——增加个人定义，以使个人信息定义更加严谨，精确地描述个人信息；

——修订个人信息定义；

——增加主体定义，以使个人信息主体定义更加严谨，精确地描述个人信息主体；

——修订个人信息主体定义，更加严谨、规范地描述个人信息主体；

——定义个人信息生命周期，制定基于个人信息生命周期的个人信息安全规则；

——定义个人信息管理者的行为约束；

——建立被动收集的约束规则；

——增加个人安全管理规则，以适应新一代信息技术应用对个人信息主体的安全威胁。

本部分由大连市经济和信息化委员会提出。

本部分由辽宁省经济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、辽宁省信息安全与软件测评认证中心。

本部分主要起草人：郎庆斌、孙鹏、尹宏、丁宗安、孙毅、吕蕾蕾、杨莉、司丹、郭玉梅、杨万清、王小庚、宋悦、王开红、曹剑、李倩。

本部分代替DB21/T 1628.1-2012。

DB21/T 1628.1-2012的历次版本发布情况：

——DB21/T 1628-2008

引 言

DB21/T1628.1-2012已经发布实施近3年，在社会、经济、文化等各个领域的深刻变革中，对辽宁省个人信息安全起到了重要的指导作用。随着科学技术，特别是IT的进步和发展，引发新的个人信息安全危机，需要在新的形势下重新审视个人信息安全标准的普适性。

管理是安全的关键，无论传统的个人信息形态，还是新一代信息技术的应用（如智慧城市、云服务、大数据、物联网等）。本标准再次修订，以管理为主线，以个人信息生命周期，即服务管理过程为导向，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。

信息安全　个人信息保护规范

1　范围

本标准规定了个人信息主体权利、个人信息生命周期、个人信息管理、管理机制、个人信息获取、个人信息处理、安全管理、过程管理等的基本规则和要求。

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、社会团体等组织及个人。

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

DB21/T 1628.2 信息安全 个人信息安全管理体系实施指南

DB21/T 1628.3 信息安全 个人信息数据库管理指南

DB21/T 1628.5 信息安全 个人信息安全风险管理指南

3　术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

个人　personal

基于自然规律出生，具有生物学意义和法理人格，并被赋予民事主体资格的自然人个体。

3.1.2

个人信息 personal information

依附于个人，并可描述个人基本形态的信息，包括：

a）可通过听觉、视觉、触觉等感官直接识别个人的信息，如数字、文字、图像、影像、声音等；

b）可借助各种手段间接识别个人的信息，如与个人相关各种信息对照、参考、分析等。

3.1.3

主体　subject

享受民事权利并承担民事义务的个人。

3.1.4

个人信息主体 personal information subject

可通过个人信息识别的、拥有该个人信息，享有该个人信息权益的个人。

3.1.5

个人信息管理者 personal information controller

获个人信息主体授权，基于特定、明确、合法目的，获取、管理个人信息的机关、企业、事业、社会团体等组织及个人。

3.1.6

个人信息安全 personal information security

以安全为目的、以个人信息资源为核心，以服务管理流程为导向，构建相对稳定、安全的个人信息环境。

3.1.7

个人信息生命周期 personal information life cycle

当个人信息主体同意直接收集个人信息直至个人信息彻底销毁的生命历程，是个人信息管理者向个人信息主体提供服务管理的过程。

注1：个人信息生命周期可以是多重的，如间接收集应是个人信息生命周期内存在的新的生命周期。

3.1.8

个人信息管理 personal information management

在个人信息生命周期内，计划、组织、协调、控制个人信息及相关资源、环境、管理体系等的相关活动或行为。

3.1.9

个人信息安全管理体系 personal information Security management system

个人信息管理活动或行为的结果。基于个人信息管理目标，整合目标、方针、原则、方法、过程、审核、改进等管理要素，及实现要素的方法和过程，提高个人信息管理有效性的系统。

3.1.10

个人信息数据库 personal information database

为实现一定目的，按照某种方式和规则组织的个人信息集合体。包括：

a）可以通过自动处理检索特定的个人信息的集合体，如磁介质、电子、网络媒介等；

b）可以采用非自动处理方式检索、查阅特定的个人信息的集合体，如纸介质、声音、照片等；

c）前述 2 种混合形式；

除前 3 项外，法律规定的可检索特定个人信息的集合体。

注2：个人信息数据库，一般由 a、b 两种形式构成，形成逻辑统一的个人信息集合体。

3.1.11

个人信息收集 personal information collect

基于特定、明确、合法的目的获取个人信息的行为。

3.1.12

个人信息处理 personal information process

自动或非自动处置个人信息的过程，如收集、加工、编辑、存储、检索、交换等及其它使用行为或活动。

3.1.12.1

自动处理 automatic processing

利用计算机及其相关和配套设备、信息网络系统、信息资源系统等，按照一定的应用目的和规则，收集、加工、编辑、存储、检索、交换等相关数据处置行为或活动。

3.1.12.2

非自动处理 non-automatic processing

除自动处理外的其它数据处置行为或活动。

3.1.13

利用 utilize

因某种利益交付第三方使用或因其它某种利益使用个人信息的行为。

3.1.14

个人信息主体同意 personal information subject agreement

个人信息管理活动或行为与个人信息主体意愿一致，个人信息主体明确表示赞成。表达形式包括：

a）个人信息主体以书面形式同意；

b）个人信息主体以可鉴证的、有规范记录的、满足书面形式要求的非书面形式同意。

注3：下述情况视为个人信息主体同意：

1）由监护人代表未成年的或无法做出正确判断的成年个人信息主体表达的意愿；

2）个人信息管理者与个人信息主体签订合同中确认了相关个人信息处理的规定，个人信息主体同意履行合同。

3.2 缩略语

3.2.1

PDCA Plan-Do-Check-Act

GB/T 19001/ISO 9001 确立的全面质量管理应遵循的科学方法。本标准用于个人信息管理相关活动的质量管理。

3.2.2

PISMS personal information security management system

个人信息安全管理体系。

4 个人信息生命周期

个人信息生命周期应包括3个环节：

a）个人信息获取过程：个人信息主体同意，基于特定、明确、合法目的，直接或间接收集个人信息；

b）个人信息处理过程：基于收集目的的个人信息使用、利用过程，可划分4种形式：

1）包括编辑、加工、检索、存储、传输等不同的使用流程；

2）包括提供、委托、交换等不同的利用过程；

3）包括交易、二次开发等不同的利用过程；

4）个人信息的后处理过程；

c）基于生命周期的过程管理：在个人信息生命周期内，采用PDCA模式管理针对个人信息及相关资源、环境、管理体系等的活动或行为。

5 个人信息主体权利

5.1 知情权

个人信息主体知情权应包括：

a）个人信息主体应有权知悉个人信息数据库中与个人信息主体相关的信息；

b）个人信息主体应有权知悉个人信息收集、处理、使用、利用的目的、方式、范围等相关信息；

c）个人信息主体应有权查询个人信息收集、处理、使用、利用情况及个人信息质量等相关信息；

d）个人信息主体应有权知悉个人信息生命周期内个人信息管理质量。

5.2 支配权

个人信息主体支配权应包括：

a）收集、处理、使用、利用个人信息，应经个人信息主体同意，并签字盖章；

b）个人信息主体应有权修改、删除、完善与之相关的个人信息，以保证个人信息的完整、准确和最新状态；

c）个人信息主体应有权决定如何使用与之相关的个人信息；

d）在个人信息生命周期内，个人信息主体应有权提议改进、完善个人信息管理质量。

5.3 质疑权

个人信息主体质疑权应包括：

a）个人信息主体应有权质疑与之相关的个人信息的准确性、完整性和时效性；

b）个人信息主体应有权质疑或反对与之相关的个人信息管理目的、过程等；

c）如果个人信息管理目的、过程违背了个人信息主体意愿或其它正当理由，个人信息主体应有权请求停止个人信息管理活动、行为或提出撤消该个人信息。停止或撤销应经个人信息主体确认；

d）在个人信息生命周期内，个人信息主体应有权质疑个人信息管理质量的可靠性。

6 个人信息管理者

6.1 规则

个人信息管理者规则应包括：

a）个人信息管理者获取、处理、使用、利用、管理个人信息应获得个人信息主体授权，并确定明确、合法的目的；

b）个人信息管理者应基于个人信息生命周期，为个人信息主体提供个人信息的服务管理；

c）个人信息管理者不应因利益、条件等的变化降低个人信息管理质量的可靠性。

6.2 角色

个人信息管理者可根据不同的需要细分不同的角色，如个人信息获取、个人信息消费等，但均应遵循6.1确立的规则，保障个人信息主体的权益。

6.3 服务管理

个人信息管理应是个人信息管理者向个人信息主体提供服务的过程。个人信息管理者应满足：

a）个人信息管理者应具有各类资源的转换能力和相应的管理职能，以保证个人信息管理的有效性；

b）个人信息管理者应建立有效的内部管理机制并形成管理体系，以保证个人信息管理的质量可靠性；

c）个人信息管理者应提供透明的服务管理过程，以保证第5章确立的个人信息主体的权力。

6.4 责任和义务

6.4.1 管理责任

个人信息管理者应对所拥有的个人信息负有管理责任，并征得个人信息主体同意后开展与个人信息相关的管理活动或行为。

6.4.2 权利保障

个人信息管理者应保障个人信息主体的权利。

6.4.3 目的明确

个人信息管理者应保证个人信息管理目的与个人信息主体意愿一致，管理过程或行为不应超目的、超范围。

6.4.4 告知

个人信息管理者应将收集个人信息的目的和方式、不提供个人信息的后果、查询和更正相关个人信息的权利，以及个人信息管理者本身的相关信息等告知个人信息主体。

6.4.5 质量保证

个人信息管理者应在管理活动或行为中保证个人信息的完整性、准确性、可用性，并保持最新状态。

6.4.6 保密性

个人信息管理者应对所管理的个人信息予以保密，并对个人信息管理过程中的安全负责。

7 个人信息管理

7.1 目的

个人信息管理者应依据其责任和义务，协调、组织、转换PISMS和各类相关资源，根据收集目的，采取相应的控制策略和措施，收集、处理、使用、利用个人信息。

7.2 原则

7.2.1 目的明确

收集个人信息应有明确的目的，不应超目的范围处理、利用、使用。

7.2.2 主体权利

个人信息主体应对与个人相关的个人信息享有权利。

7.2.3 信息质量

在管理活动或行为中应保证个人信息的准确性、完整性和最新状态。

7.2.4 合理限制

收集、处理、使用、利用个人信息，应采用合法、合理的手段和方式，并保持公开的形式。

7.2.5 安全保障

应采取必要、合理的管理和技术措施，防止个人信息滥用、篡改、丢失、泄露、损毁等。

7.3 方针

个人信息管理者应制定个人信息管理方针，以指导个人信息管理。方针应遵循国家相关法律、法规规定的原则和措施，符合个人信息管理者实际情况，并应以简洁、明确的语言阐述，公之于众。方针内容宜包括：

a）个人信息主体的权利；
b）个人信息管理者的义务；
c）个人信息管理的目的和原则；
d）个人信息管理的措施和方法；
e）个人信息管理的改进和完善。

7.4 计划

个人信息管理者应根据管理、业务目标，制定基于个人信息生命周期的管理计划。计划应包括：

a）个人信息收集目的、策略；
b）个人信息管理措施、策略；
c）个人信息管理和各类相关资源的组织、协调、转换和沟通；
d）个人信息安全风险评估；
e）计划评估；
f）其它必要的管理策略。

7.5 组织

7.5.1 要求

个人信息管理者应根据管理计划，建立个人信息管理机构，实施个人信息生命周期全过程的符合个人信息相关法规、标准的管理，组织个人信息管理活动或行为。

7.5.2 相关机构及职责

7.5.2.1 最高管理者

个人信息管理者的最高行政领导，应重视个人信息管理，并选择、任命有能力的个人信息管理者代表组建、负责个人信息管理机构，在资金、资源等各个方面提供完全的支持。

7.5.2.2 管理机构

个人信息管理者代表应建立、落实个人信息管理机构，明确责任主体和职责，制定管理计划。个人信息管理机构宜包括宣传教育、安全管理、服务台等责任主体，管理机构的主要职责应包括：

a）个人信息管理计划制定、实施；

b）PISMS 建立、实施、运行；

c）明确个人信息管理相关责任主体和人员职责、责任；

d）个人信息相关活动、行为的管理，包括相关宣传教育、安全管理、服务咨询等；

e）基于个人信息生命周期的过程管理；

f）PISMS运行检查、评估、改进、完善；

g）记录个人信息管理活动，并编制PISMS运行报告。

7.5.2.3 内审机构

个人信息管理者应建立PISMS内审机构，并应由最高管理者指定PISMS内审代表负责。内审代表可以在个人信息管理者内部选聘，或聘请社会人士担任。其职责是：

a）独立、公平、公正地开展 PISMS 监督、检查、调查工作；

b）制定 PISMS 内审制度和内审计划，并按计划实施内审；

c）跟踪、监控、评估PISMS实施、运行；

d）编制内审报告，督促、建议PISMS的改进、完善。

7.5.3 个人信息安全管理体系

个人信息管理者代表应建立基于服务管理的 PISMS，满足个人信息管理的需要。PISMS 应包括以下要素：

a）个人信息安全目标和基本原则；

b）个人信息管理方针；

c）个人信息管理机制；

d）个人信息获取过程；

e）个人信息处理过程；

f）个人信息安全管理；

g）过程管理等。

7.6 控制

个人信息管理者代表应根据管理计划适时评估 PISMS 的效能和个人信息管理效果，检查、修正个人信息管理相关活动、行为，并监督管理计划的实施。

7.7 协调

在个人信息管理活动或行为中，应注意个人信息主体与个人信息管理者、个人信息管理者各部门（从属机构）与PISMS、PISMS内、PISMS与相关资源之间等的协调、沟通。

8 管理机制

8.1 管理制度

8.1.1 基本规章

基本规章是个人信息管理者及其全体工作人员应遵循的行为准则，应使每个工作人员完全理解并遵照执行。基本规章应包括个人信息安全管理体系构成要素和各个环节的管理规则，并应在实施过程中不断改进和完善。基本规章示例，参照DB21/T 1628.2。

8.1.2 管理细则

各从属机构、部门等应根据实际需要制定与基本规章一致，并符合从属机构、部门特点、切实可行的相关管理细则。

8.1.3 其它规定

其它业务开展或有特殊要求的业务，涉及个人信息管理，应制定相应的管理规定。

8.2 人员管理

8.2.1 相关人员

应明确与个人信息管理相关人员的权限、责任，加强监督和管理，防范未经授权的个人信息接触、职责不清、不作为、渎职等管理风险。

8.2.2 工作人员

应加强所有与个人信息管理者相关工作人员的宣传和教育，明确岗位职责，提高保护个人信息主体权益的意识，避免发生个人信息安全事件。

8.2.3 激励

应采取有计划的措施，激发工作人员与个人信息管理机构之间的互动交流、合理诉求，增强工作人员保护个人信息的热情、责任感、积极性和事业心，以实现个人信息管理目标。

8.3 宣传教育

8.3.1 宣传

8.3.1.1 基本宣传

个人信息管理者应在其内部向全体工作人员及其它相关人员说明个人信息管理的重要性和相关管理策略，以得到工作人员及其它相关人员对个人信息管理工作的配合和重视。

8.3.1.2 业务宣传

个人信息管理者处理涉及个人信息的相关业务时，应主动说明收集、处理、使用、利用个人信息的目的、措施、方法和规定，并做出保密承诺。

8.3.1.3 社会宣传

个人信息管理者应在相关媒介（宣传资料、网络媒介（如网站等）及其它相关的面向社会的电子类、纸质等材料）中增加个人信息管理的相关内容。

8.3.2 培训教育

8.3.2.1 计划

应根据人员、机构、业务、需求等实际情况，制定个人信息管理相关的培训和教育制度，适时开展相应的培训教育。

8.3.2.2 对象

培训教育的对象，应包括：

a）全体工作人员；

b）临时员工；

c）其他相关人员。

8.3.2.3 内容

培训教育的主要内容，应包括：

a）个人信息安全相关法律、法规、规范、标准和管理制度；

b）个人信息管理的重要性和必要性；

c）PISMS的构成、实施等；

d）个人信息主体的权利、责任；

e）管理、业务活动中个人信息管理的方式、措施等；

f）违反个人信息安全相关标准可能引起的损害和后果；

g）其它必要的教育。

8.4 数据库管理

8.4.1 要求

个人信息管理者应集中管理各种形式存放的个人信息，规范、建立统一的个人信息数据库。个人信息数据库管理，参照DB21/T1628.3。

8.4.2 保存

个人信息主体应明确确认其个人信息是否以简明、易懂的语言记载、存储在个人信息数据库中，并可以清楚无误地提取、拷贝这些信息。

8.4.3 时限

个人信息管理者应为个人信息的存储、保存设定一个合理的时限，并与目的充分相关。

8.4.4 备案

个人信息数据库的使用、查阅，应建立备案登记制度，并有专人负责。记录应包括责任人、存储（保存）目的、时限、更新时间、获取方法、获取途径、位置、使用目的、使用方法、安全承诺、废弃原因和方法等。

8.4.5 个人管理

个人信息主体保有的可移动设备、媒介等构成了移动的个人信息数据库，个人信息主体应提高安全意识，采取必要的安全措施，防止不正当收集个人信息，避免个人信息泄漏。

8.5 文档管理

8.5.1 记录

应在个人信息管理过程中记录与个人信息相关活动和行为的目的、时间、范围、对象、方式方法、效果、反馈等信息。这些活动和行为包括体系建立、宣传、培训教育、安全管理、过程改进、内审等。

8.5.2 备案

应建立与个人信息管理相关的规章、文件、记录、合同等文档的备案管理制度，并不断改进和完善。

8.6 公示

公开、公示个人信息，应以适当方式通知个人信息主体，并征得个人信息主体同意。通知的内容应包括：

a）个人信息管理者的相关信息；

b）公示的目的、方式、范围和内容；

c）个人信息主体的权利；

d）公示和非公示的结果。

9 个人信息获取

9.1 目的

所有个人信息收集行为，必须具有特定、明确、合法的目的，并应征得个人信息主体同意，限定在收集目的范围内。

9.2 限制

应遵循 7.2、6.4 的规定，基于特定、明确、合法的目的，采用科学、规范、合法、适度、适当的收集方法和手段，以保障个人信息主体的权益：

a）应将收集目的、范围、方法和手段、处理方式等清晰无误的告知个人信息主体，并征得个人信息主体同意；

b）间接或被动收集时，应将收集目的、范围、内容、方法和手段、处理方式等以适当形式公开，如以公告形式发布。如有疑义、反对，应停止收集；

c） 不应以任何目的、方法、手段等收集移动的个人信息数据库的信息。

注4：被动收集，即个人信息主体不知情或不能控制情况下收集。

9.3 类别

9.3.1 直接收集

目的明确，并征得个人信息主体同意，直接经个人信息主体收集个人信息。直接收集应向个人信息主体提供的信息包括：

a）个人信息管理者的相关信息；

b）个人信息收集、处理、使用的目的、方法；

c）接受并管理该个人信息的第三方的相关信息；

d）个人信息主体拒绝提供相关个人信息可能会产生的后果；

e）个人信息主体的查询、修正、反对等相关权利；

f）个人信息安全和保密承诺；

g）后处理方式。

9.3.2 间接收集

非直接地收集个人信息时，应遵循9.2的规定，保证个人信息主体知悉并同意。间接收集应保证个人信息主体权益不受侵害。应保证个人信息主体知悉的信息，参照9.3.1。

9.3.3 被动收集

在个人信息主体不知情或不能控制的情况下收集、处理、使用、利用个人信息，应保证个人信息主体权益不受侵害：

a）应遵循7.2、6.4确定的原则和责任义务；

b）应遵循9.2的限制；

c）通过各种电子媒介（如博客、微博、微信、论坛、云盘、网盘、邮件、即时通讯、网站、网络视频等）、纸媒体获取公开的个人信息，亦应遵循7.2、6.4确定的原则、责任义务，同时应遵循9.2的限制；

d）依据9.2，应采取适宜的方式公告、公示。通过公告、公示保证个人信息主体知悉的信息，参照9.3.1。

9.4 保存

以各种形式、方式收集的个人信息，应保存或存储在统一的个人信息数据库内，并应依据8.4建立相应的个人信息数据库管理机制。

10 个人信息处理

10.1 过程

在个人信息处理过程中，应遵循：

a）应根据第7章、第8章的相关规则，管控个人信息处理过程，以保证个人信息质量和个人信息主体权益；

b）应接受内审机构的检查、监控，随时改进、完善个人信息处理过程，以保证个人信息安全。

10.2 使用

个人信息管理者处理、使用个人信息应基于明确、合法的目的，并遵循以下约束：

a）应征得个人信息主体同意；或为履行与个人信息主体达成的合法协议的需要；

b）应在个人信息收集目的范围内处理、使用个人信息。如需要超目的范围处理、使用个人信息，应征得该个人信息主体同意。通知信息参照 9.3.1；

c）任何处理、使用个人信息的行为，应履行 7.2、6.4 规定的原则和个人信息管理者的责任、义务，征得个人信息主体同意，并限定在个人信息主体同意的范围内，避免随意泄漏、传播和扩散，以保证个人信息安全。通知信息参照 9.3.1。

10.3 提供

10.3.1 合法性

个人信息管理者所拥有的个人信息，应是依特定、明确、合法的目的，经个人信息主体同意，采取适当、合法、有效的方法和手段获得的，并不与收集目的相悖。

10.3.2 权益保障

个人信息管理者合法拥有的个人信息，在向第三方提供时，应履行 6.4 规定的个人信息管理者的责任和义务，保障个人信息主体的合法权益。

10.3.3 授权许可

个人信息管理者向第三方提供个人信息，应获得该个人信息的个人信息主体授权，并在允许的目的范围内，采用合法、适当、适度的方法使用。应向个人信息主体说明的信息，参照 9.3.1。

10.3.4 质量保证

第三方接受个人信息管理者提供的个人信息，应遵循 6.4 关于质量保证的原则。

10.3.5 安全承诺

个人信息管理者向第三方提供个人信息时，应获得第三方以书面形式（或以可见证的、有规范记录的、满足书面形式要求的非书面形式）保证个人信息的完整性、准确性、安全性的明确承诺，避免不正确使用或泄漏。

10.4 委托

10.4.1 范围限定

委托第三方收集个人信息、向第三方委托个人信息处理业务或接受个人信息处理委托业务时，应在个人信息主体明确同意的，或委托方以合同或其它方式要求的使用目的范围内处理，不可超范围、超目的随意处理，并应向个人信息主体提供受托方相关信息。提供的信息可参照 9.3.1。

10.4.2 委托信用

涉及个人信息委托业务时，应选择已建立 PISMS 的个人信息管理者，以建立相应的委托信用机制，保证不会发生个人信息泄漏或个人信息滥用。在委托合同中应包括：

a）委托方和受托方的权利和责任；
b）委托目的和范围；
c）保护个人信息的安全措施和安全承诺；
d）再委托时的相关信息；
e）PISMS 的相关说明；
f）个人信息相关事故的责任认定和报告；
g）合同到期后个人信息的处理方式。

10.5 二次开发

分析、整合、整理、挖掘、加工等个人信息二次开发，应履行 7.2、6.4 规定的原则和个人信息管理者的责任、义务，征得个人信息主体同意，并限定在个人信息主体同意的范围内，避免随意泄漏、传播和扩散。通知的内容应包括：

a）个人信息管理者的相关信息；
b）二次开发的目的、方式、方法和范围；
c）安全措施和安全承诺；
d）事故责任认定和处理方式；
e）开发完成后的处理方式等。

10.6 交易

个人信息交易应保证：

a）应限定在法律许可的范围内；

b）应通知个人信息主体并征得个人信息主体同意，且限定在个人信息主体同意的范围内处理使用，避免随意泄漏、传播和扩散；

c）交易双方均应履行 7.2、6.4 规定的原则和个人信息管理者的责任、义务，保障个人信息主体权益。

通知个人信息主体的内容应包括：

1）个人信息管理者相关信息；

2）个人信息来源的合法性、有效性；

3）个人信息交易的必要性；

4）个人信息交易的目的、方式、方法和范围；

5）安全措施和安全承诺；

6）事故责任认定和处理方式；

7）交易完成后的处理方式等。

10.7 后处理

10.7.1 要求

个人信息处理、利用、使用后，应根据个人信息主体意见或合同约定方式，采取相应的安全措施，避免发生丢失、损毁、泄漏等安全事故。

10.7.2 质量

个人信息处理、使用、利用后，如需继续保存、使用、返还，应保证个人信息的准确性、完整性和最新状态。

10.7.3 销毁

个人信息处理、使用、利用后，如不需继续保存、使用、返还，应彻底销毁与个人信息相关的文档、介质等及其记录的个人信息。

11 安全管理

11.1 风险管理

应在个人信息管理过程或行为中，识别、分析、评估潜在的风险因素，制定风险应对策略，采取风险管理措施，监控风险变化，并将残余风险控制在可接受范围内。风险管理应参照 DB21/T 1628.5 实施。

11.2 物理环境管理

应根据需要采取必要的措施，保证个人信息存储、保存环境的安全，包括防火、防盗及其它自然灾害、意外事故、人为因素等。

11.3 工作环境管理

应注意工作人员工作环境内所有相关的个人信息管理，防止未经授权的、无意的、恶意的使用、泄露、损毁、丢失。工作环境包括：

a）出入管理；

b）工作桌面；
c）计算机桌面；
d）计算机接口；
e）计算机管理（文件、文件夹等）；
f）其它相关管理。

11.4 网络行为管理

应制定网络管理措施，采用相应的技术手段，引导、约束通过网络利用、传播个人信息的行为，构建规范、科学、合理、文明的网络秩序。

11.5 IT 环境安全

应在整体信息安全体系建设中，充分考虑个人信息及相关因素的特点，加强个人信息安全防护，预防安全隐患和安全威胁。如网络基础平台、系统平台、应用系统、安全系统、数据等的安全，及信息交换中的安全防范、病毒预防和恢复、非传统信息安全等。

11.6 个人信息数据库安全

11.6.1 要求

个人信息管理机构应保证个人信息数据库存储、保存的个人信息的准确性、完整性、保密性和可用性，并随时更新，以保证个人信息的最新状态。

11.6.2 管理安全

个人信息管理者应履行 6.4 规定的责任和义务，建立个人信息数据库管理机制。包括：
a）个人信息数据库管理和使用制度；
b）个人信息数据库管理者的职责；
c）维护和记录；
d）事故处理。

11.6.3 使用安全

应根据个人信息自动和非自动处理的特点，制定相应的个人信息数据库管理策略，包括访问/调用控制、权限设置、密钥管理等，防止个人信息的不当使用、毁损、泄漏、删除等。

11.6.4 备份和恢复

应制定个人信息数据库备份和恢复机制，并保证备份、恢复的完整性、可靠性和准确性。

11.7 移动设备安全

11.7.1 管理安全

个人信息管理者应制定与个人信息相关的移动设备、媒介的管理制度，采用管理和技术措施，并建立设备使用追踪回溯机制，防止数据毁损、泄漏、删除、遗失等。

11.7.2 终端安全

个人信息主体对所保有的移动设备，应提高安全意识，根据不同的物理环境和使用环境，采取相应的安全防范措施，避免个人信息泄漏。

11.8 个人安全

在多种情况下，个人信息主体应提高安全意识，采取相应和适当的措施，防止不当收集、使用、利用个人信息，以保护个人信息主体权益。这些情况可包括：

a）各种网络环境下与个人信息相关的各种行为、活动；
b）各种工作环境下与个人信息相关的各种行为、活动；
c）各种生活环境下与个人信息相关的各种行为、活动；
d）各种社会活动中与个人信息相关的各种行为、活动等。

12 过程管理

12.1 PISMS 内审

12.1.1 管理

a）应审核个人信息管理相关活动和行为、PISMS、PISMS 实施和运行过程；
b）内审应由与审核对象无直接关系人实施；
c）内审应提出过程改进和完善建议。

12.1.2 计划

应根据相关法律、规范和实际需求制定 PISMS 内审计划：

a）内审目标和原则；
b）内审策略和控制措施；
c）组织、协调相关资源；
d）内审周期、时间；
e）职责、责任；
f）内审实施；
g）其它必要的措施。

12.1.3 实施

应根据PISMS内审计划，定期独立、公平、公正地实施内审，并形成内审报告。

12.2 过程改进

12.2.1 服务台管理

服务台应接受个人信息主体、各类组织和人员提出的个人信息管理活动、PISMS的相关意见、建议、咨询、投诉等，并采取相应的处理措施，及时反馈。

12.2.2 跟踪和监控

PISMS内审机构应实时跟踪、监控PISMS的实施、运行，及时发现潜在的安全风险、缺陷和存在的问题，提出整改建议。

12.2.3 持续改进

个人信息管理机构应依据相关法规、内审报告、需求变化、服务台反馈、跟踪监控结果等，采用 PDCA 模式，定期评估、分析 PISMS 运行状况，并持续改进和完善：

a）分析、判断 PISMS 实施、运行中的缺陷和漏洞；
b）制定预防和改进措施；
c）实时预防、改进；
d）跟踪改进结果。

12.3 应急管理

个人信息管理者应制定应急预案，评估、分析收集、处理、使用个人信息过程中可能出现的个人信息泄露、丢失、损坏、篡改、不当使用等事故，采取相应的预防措施和处理。预案应包括：
a）事故的评估、分析；
b）事故的处理流程；
c）事故的应急机制；
d）事故的处理方案；
e）事故记录和报告制度；
f）事故的责任认定。

13 例外

13.1 敏感个人信息

敏感的个人信息应包括：
a）有关思想、宗教、信仰、种族、血缘的事项；
b）有关身体障碍、精神障碍、犯罪史及相关可能造成社会歧视的事项；
c）有关政治权利的事项；
d）有关健康、医疗及性生活的相关事项等。

13.2 收集例外

不应收集、处理、使用敏感的个人信息。经个人信息主体同意的例外，但个人信息管理者应遵循以下规则：
a）应合理、合法、适度、目的明确，并经个人信息主体确认同意；
b）应直接收集，不应间接收集、被动收集或违背个人信息主体意愿收集；
c）应采取特别的保护措施，保证敏感个人信息安全和个人信息主体权益；
d）一经处理、使用完毕，立即完全、彻底销毁。

13.3 法律例外

法律特别规定的个人信息收集例外，个人信息管理者应遵循以下规则：
a）应依据相关法规，合理、合法、适度，且目的明确：
1）法律特别规定的；
2）保护国家安全、公共安全、国家利益、制止刑事犯罪；
3）保护个人信息主体或公众的权利、生命、健康、财产等重大利益等；
b）基于明确目的，可不必事先征得个人信息主体同意，但应经由专门机构确定；
c）应保证限于收集目的和使用范围内；
d）应采取特别的保护措施，保证个人信息安全和个人信息主体权益；
e）一经处理、使用完毕，立即完全、彻底销毁，避免个人信息泄漏、转移。

14 认证

为提供个人信息管理、PISMS的质量保证，应评价个人信息管理者实施、运行PISMS的状况，以确定其与个人信息安全相关法律、法规、规范的符合性、一致性和目的有效性，并以此作为颁发PISMS认证证书的依据。

参 考 文 献

[1]个人信息安全-研究与实践　　郎庆斌、孙毅　人民出版社　2012