ICS 35.020
L70

DB21

辽 宁 省 地 方 标 准

DB 21/ T1628.1—2012
代替 DB21/T1628-2008

信息安全 个人信息保护规范

Information Security-Specification for Personal Information Protection

2012－2－7 发布　　2012 - 03 - 07 实施

辽宁省质量技术监督局　发布

目　　次

前　言

本标准代替 DB21/T 1628—2008《个人信息保护规范》。与 DB21/T 1628—2008 相比，本标准除编辑性修改外，主要技术变化如下：

——个人信息保护体系修订为个人信息安全管理体系；

——个人信息保护监察修订为个人信息安全管理体系内审；

——个人信息安全管理体系要素划分调整为个人信息管理方针、个人信息管理机构和职责、个人信息管理机制、个人信息管理过程、个人信息安全管理、个人信息安全管理体系内审、过程改进和应急管理；

——个人信息保护管理机构调整为个人信息管理机构；

——个人信息保护是针对个人信息及相关资源、环境、管理体系的管理活动或行为之一，因而将个人信息保护修订为个人信息管理，增加了个人信息管理相关规则，标准各章节依据这一规则修订；

——修订个人信息交易相关条款；

——原13、16章合并，并修订为过程改进；

——个人信息保护负责人调整为个人信息管理者代表；个人信息保护监察负责人调整为个人信息安全管理体系内审代表。

——本部分的修订，充分考虑其它管理体系，如 GB/T19001—2000、GB/T 24405.1—2009、GB/T 24405.2—2010、GB/T 22080—2008、GB/T 22081—2008 等的特点，为多种管理体系的融和实施，奠定适宜的基础。

本标准是依据 GB/T1.1—2009《标准化工作导则　第 1 部分：标准的结构与编写》制定的。

本标准由大连市经济和信息化委员会提出。

本标准由辽宁省经济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、辽宁省信息安全与软件测评认证中心。

本标准主要起草人：郎庆斌、孙鹏、曹剑、孙毅、吕蕾蕾、王开红、郭玉梅、李倩。

DB21/T 1628—2008《个人信息保护规范》于 2008 年 6 月首次发布，本次修订为第一次修订。

引言

DB21/T1628已经实施近3年，对辽宁省个人信息保护工作起到了重要的指导作用。个人信息安全领域相关研究、实践，随着社会、经济、文化等各个领域的深刻变革不断深入，个人信息安全事件的特征发生变化，对个人信息相关安全法规、标准的认识不断进步、发展，有必要调整DB21/T1628的结构，修订DB21/T1628的内容，建立规范的个人信息安全标准体系。

本标准修订以个人信息管理为主线、个人信息安全为目的，规定普适的个人信息管理过程中各要素的约束条件。在管理过程中，管理活动或行为可以视为要素。在个人信息管理过程中，个人信息保护是针对个人信息及相关资源、环境、管理体系等的管理活动或行为之一。

本标准修订后，将陆续编制个人信息安全标准体系其它标准，主要包括：

——个人信息安全管理体系实施指南

——个人信息数据库管理指南

——个人信息管理文档管理指南

——个人信息安全风险管理指南

——个人信息安全管理体系安全技术实施指南

——个人信息安全管理体系内审实施指南等。

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管理原则、个人信息主体权利、个人信息管理者的义务、个人信息管理、个人信息安全管理体系建立、个人信息管理过程、个人信息安全管理、个人信息安全管理体系内审、过程改进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　术语、定义和缩略语

2.1 术语和定义

下列术语和定义适用于本文件。

2.1.1

个人信息 personal information

与特定个人相关、并可识别该个人的信息，如数据、图像、声音等，包括不能直接确认，但与其它相关信息对照、参考、分析仍可间接识别特定个人的信息。

2.1.2

个人信息数据库 personal information database

为实现一定的目的，按照某种规则组织的个人信息的集合体。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、电子及网络媒介等；

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）除前 2 项外，法律规定的可检索特定个人信息的集合体。

2.1.3

个人信息主体 personal information subject

可通过个人信息识别的特定的自然人。

2.1.4

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，管理个人信息的机关、企业、事业、社会团体等组织及个人。

2.1.5

个人信息管理 personal information management

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。

2.1.6

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。

2.1.7

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。

2.1.8

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。

2.1.8.1

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。

2.1.8.2

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。

2.1.9

利用 utilize

基于特定、明确、合法目的，提供、委托第三方使用个人信息及其它因某种利益使用个人信息的行为。

2.1.10

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：下述情况视为个人信息主体同意：

a）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；

b）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。

2.2 缩略语

2.2.1

PDCA Plan-Do-Check-Act

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。

2.2.2

PISMS personal information Security management system

个人信息安全管理体系。

3 个人信息管理原则

3.1 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。

3.2 主体权利

个人信息主体对与个人相关的个人信息享有权利。

3.3 信息质量

在管理活动或行为中保证个人信息的准确性、完整性和最新状态。

3.4 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。

3.5 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。

4 个人信息主体权利

4.1 知情权

a）确认个人信息数据库中与个人信息主体相关的信息；
b）确认个人信息收集、处理、使用、利用的目的、方式、范围等相关信息；
c）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。

4.2 支配权

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）个人信息主体有权决定如何使用与之相关的个人信息。

4.3 质疑权

a）个人信息主体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。

5 个人信息管理者义务

5.1 管理责任

个人信息管理者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个人信息管理相关活动或行为。

5.2 权利保障

个人信息管理者必须保障个人信息主体的权利。

5.3 目的明确

个人信息管理者必须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。

5.4 告知

个人信息管理者应将个人信息管理目的、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。

5.5 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。

5.6 保密性

个人信息管理者必须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。

6 个人信息管理

6.1 目的

个人信息管理者应依据 5.1，协调、组织 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，处理、使用、利用个人信息。

6.2 计划

个人信息管理者应根据管理、业务目标，制定个人信息管理计划。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、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。

6.3 组织

个人信息管理者应根据管理计划，组织个人信息管理活动或行为，主要包括：

a）建立 PISMS，保证管理、业务需要；

b）明确个人信息管理职责和行为准则；

c）实施、运行 PISMS；
d）评估 PISMS 效能；
e）评估个人信息管理效果；
f）其它相关管理。

6.4 控制

个人信息管理者应根据管理计划，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。

6.5 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。

7 个人信息安全管理体系（PISMS）

PISMS 应包括以下要素：
a）目标和基本原则；
b）方针；
c）机构及职责；
d）管理机制；
e）管理过程；
f）安全管理；
g）内审；
h）过程改进；
i）应急管理。

8 个人信息管理方针

应是指导个人信息管理，保障个人信息安全，符合个人信息管理者实际情况，遵守国家相关法律、法规的原则和措施。应以简洁、明确的语言阐述，并公之于众。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。

9 个人信息管理相关机构及职责

9.1 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。

9.2 个人信息管理机构

个人信息管理机构主要包括宣传教育、个人信息安全、服务台等责任主体，其主要职责包括：

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机构和人员职责、责任；

d）个人信息相关活动、行为的管理；

e）PISMS 运行检查、评估、改进、完善；

f）记录个人信息管理活动，并编制 PISMS 运行报告。

9.2.1 宣传教育

宣传教育宜指定责任主体，在个人信息管理者代表领导下开展工作。宣传教育的主要职责是：

a）组织、实施 PISMS 宣传、教育；

b）制定 PISMS 宣传、教育制度、计划；

c）制定 PISMS 宣传策略和方法；

d）个人信息相关知识、管理和安全技术等的宣传、教育；

e）改进、完善宣传、教育措施、方法。

9.2.2 个人信息安全

个人信息安全宜指定信息安全责任主体负责，在个人信息管理者代表指导下开展个人信息安全管理工作。其主要职责应包括：

a）个人信息安全风险管理；

b）制定个人信息安全管理策略、措施；

c）实施个人信息安全管理措施；

d）改进、完善个人信息安全管理。

9.2.3 服务台

服务台宜指定责任主体，在个人信息管理者代表领导下提供个人信息相关的服务。服务台的主要职责包括：

a）提供个人信息管理、安全的相关咨询和服务；

b）提供个人信息处理、使用建议和意见；

c）接受有关个人信息管理、安全的意见，并落实和反馈；

d）沟通、交流；

e）个人信息管理、安全相关事项、问题处理等的发布；

f）其它应处理的问题。

9.3 PISMS 内审机构

PISMS 内审机构应由最高管理者指定的 PISMS 内审代表负责，该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。

10 个人信息管理机制

10.1 管理制度

应制定个人信息管理的相关规章和制度，包括基本的管理规章和适用于各从属机构、部门特点的管理细则，并使每个工作人员完全理解并遵照执行。

10.1.1 基本规章

基本规章是个人信息管理者及其工作人员应遵循的行为准则，应在实施过程中不断改进和完善。基本规章宜包括以下各项：

a）个人信息管理相关机构职能及职责；
b）个人信息管理；
c）个人信息安全风险和安全管理措施；
d）个人信息数据库管理；
e）个人信息管理文档管理；
f）PISMS 宣传、教育；
g）PISMS 内审；
h）过程管理；
i）服务台管理；
j）应急管理；
k）违反相关规章的处理；
l）其它必要的管理制度。

10.1.2 管理细则

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

10.1.3 其它管理规定

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。

10.2 宣传

10.2.1 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。

10.2.2 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。

10.2.3 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。

10.3 培训教育

10.3.1 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。

10.3.2 对象

培训教育的对象，应包括：

a）工作人员；

b）临时员工；

c）其他相关人员。

10.3.3 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。

10.4 公示

公开、公示个人信息，应通知个人信息主体，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。

10.5 个人信息数据库管理

10.5.1 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。

10.5.2 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。

10.5.3 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。

10.6 个人信息管理文档

10.6.1 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。

10.6.2 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。

10.7 人员管理

10.7.1 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、职责不清等风险。

10.7.2 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。

10.7.3 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。

11 个人信息管理过程

11.1 收集

11.1.1 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。

11.1.2 限制

应基于特定、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）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）个人信息主体应采用适当的措施，防止不正当收集个人信息。

11.1.3 类别

11.1.3.1 直接收集

征得个人信息主体同意，直接从个人信息主体收集个人信息。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。

11.1.3.2 间接收集

非直接地收集个人信息时，也应保证个人信息主体知悉并同意。间接收集必须保证个人信息主体利益不受侵害。应保证个人信息主体知悉的信息参照 11.1.3.1。

11.2 处理

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 11.1.3.1。

c）在处理、使用个人信息时，应履行第 5 章规定的相关义务，保证个人信息安全。

11.3 利用

11.3.1 提供

11.3.1.1 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。

11.3.1.2 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，应履行第 5 章个人信息管理者的义务，保障个人信息主体的合法权益。

11.3.1.3 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 11.1.3.1。

11.3.1.4 质量保证

第三方接受个人信息管理者提供的个人信息，应履行 5.5 节的规定。

11.3.1.5 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露。

11.3.2 委托

11.3.2.1 范围限定

委托第三方收集个人信息、或向第三方委托个人信息处理业务时，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，并将受托方相

关信息提供给个人信息主体。提供的信息可参照 11.1.3.1。

11.3.2.2 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露或个人信息滥用。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。

11.3.3 其它

11.3.3.1 二次开发

分析、整合、整理、挖掘、加工等个人信息二次开发，应履行第 5 章个人信息管理者的义务，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，避免随意泄露、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。

11.3.3.2 交易

个人信息交易应履行第 5 章个人信息管理者的义务，征得个人信息主体同意，并限制在个人信息主体同意的范围内处理使用，避免随意泄露、传播和扩散。通知的内容应包括：

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。

11.4 使用

任何使用个人信息的行为，应履行第 5 章个人信息管理者的义务，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，避免随意泄露、传播和扩散。通知信息参照 11.1.3.1。

11.5 后处理

个人信息处理、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。

11.5.1 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。

11.5.2 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。

12 个人信息安全管理

12.1 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。

12.2 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。

12.3 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。

12.4 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。

12.5 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。

12.6 个人信息数据库安全

个人信息管理者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。

12.6.1 管理安全

个人信息管理者应履行第 5 章规定的义务，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。

12.6.2 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、泄露、删除等。

12.6.3 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。

13 PISMS 内审

13.1 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。

13.2 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。

13.3 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。

14 过程改进

14.1 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。

14.2 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。

14.3 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。

15 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。

16 例外

16.1 收集例外

不允许收集、处理、使用敏感的个人信息。经个人信息主体同意，或法律特别规定的例外，但应采取特别的保护措施。敏感的个人信息包括：

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。

16.2 法律例外

基于以下目的的例外，可以不必事先征得个人信息主体同意，但应依据相关法规，或经由专门机构确定：

a）法律特别规定的；

b）保护国家安全、公共安全、国家利益、制止刑事犯罪；

c）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。

17 评价

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。