ICS 35.020
L70

DB21

辽　宁　省　地　方　标　准

DB 21/T 1628.6—2018

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

Information security-Personal information security management system-Part6: Security technical implementation guide

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

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 6 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6部分：安全技术实施指南

1　范围

本标准为个人信息管理者构建、实施、运行个人信息安全管理体系采用安全技术提供指导和通用准则。

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 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 1628.3 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

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

3　术语、定义和缩略语

3.1　术语和定义

GB/T 22080、GB/T 22081、DB21/T 1628.1和DB21/T 1628.2界定的术语和定义适用于本文件。

3.2　缩略语

ISMS information security management system

信息安全管理体系

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采用信息安全技术的约束规则。

构建、实施和运行PISMS过程中，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。

使用本指南，应同时遵循、融合信息安全相关国际、国内（或等同采用）标准。

5　综述

5.1 概述

个人信息管理中采用的信息安全技术，适用一般意义的信息安全技术，但应考虑个人信息的存在形态、管理特征。特别是新一代信息技术逐渐成熟和应用，如云计算、物联网、大数据、移动终端及新的应用模式等，增加了个人隐私的安全风险，个人信息管理风险等级提高，要求信息安全技术适应科学、技术、社会的进步和发展。

5.2 技术应用

5.2.1 要求

PISMS构建、实施和运行中采用的信息安全技术，应包括安全管理和安全技术。

5.2.2 关于安全管理

应遵循GB/T 22080、GB/T 22081的一般方法，基于PISMS和个人信息形态、分布、管理特征等，构建个人信息安全机制、策略，并与ISMS融合。

5.2.3 关于安全技术

5.2.3.1 安全边界

个人信息安全与一般意义的信息安全的边界基本一致，主要包括：

a）实体安全：IT系统的场地、环境等的安全；

b）基础平台安全：承载个人信息的各种基础平台安全：

1）网络及相关设备构成的基础平台安全；

2）承载各种应用、业务系统运行的底层系统平台安全；

3）应用系统支撑平台安全（数据库、中间件等）；

4）各种安全产品、技术等构成的安全平台安全等；

c）应用系统安全：各种管理、业务等应用系统安全；

d）个人信息数据库安全：个人信息数据库及各种相关资源安全；

e）数据传输安全：个人信息在传输过程中的安全；

f）接口安全：各种接入设备、终端安全；

g）运行安全：承载个人信息（及相关数据资源）系统运行的安全。

5.2.3.2 安全技术应用

个人信息安全与一般意义的信息安全采用的安全技术策略基本一致：

a）应依据DB21/T 1628.3，综合规划个人信息数据库相关信息安全；

b）应基于5.2.3.1描述的安全边界，结合个人信息管理者的整体信息安全，统一、系统规划、模块化设计信息安全体系，特别考虑新技术应用可能产生的新的个人信息安全威胁；

c）应在统一、系统规划、模块化设计基础上，基于个人信息管理者的实际需求，运用先进、成熟、安全、可靠的产品、技术、知识，构建信息安全体系，保证个人信息安全。

6 风险管理

应遵循DB21/T 1628.5确立的规则实施风险管理。

7 安全技术

7.1 实体安全

7.1.1 内容

实体安全应包括：场地、监控、门禁、布线、工作环境、设备、媒介等的安全及灾害预防。

7.1.2 场地安全

场地安全应考虑供电系统、配电系统、接地系统、场地环境（通风、温度、湿度等）等。应符合国家相关场地标准。

7.1.3 出入安全

7.1.3.1 监控

工作场地宜安装监控系统，并考虑其安全：

a）监控系统的运行状态、参数变化、提示信息等；

b）监控设备的安全性、监控系统部署等。

7.1.3.2 门禁

个人信息管理者内部宜安装门禁系统，并考虑其安全：

a）门禁系统的部署、控制；

b）门禁卡的发放、权限，门禁卡涉及个人信息的安全措施等：

1）门禁卡发放记录的管理措施；

2）门禁卡权限设置和管理措施；

3）门禁卡时效管理；

4）门禁卡回收、失效处理等。

7.1.4 布线系统

监控设备间、弱电井、机房等区域配线设备、信息插座等设施及线缆状态，以及网络通信线路的工作状态和可能的故障状态。

7.1.5 工作环境

7.1.5.1 出入管理

出入管理的保障措施，主要应包括：

a）应建立出入管理制度：

1）建立出入登记制度；

2）所涉及个人信息的安全措施和管理；

3）出入登记文档的保存、管理措施；

4）出入登记文档的时效；

5）出入登记文档的失效、销毁管理等；

b）明确相关管理人员的责任：

1）相关管理人员的职责；

2）事故责任追究和处理等。

7.1.5.2 个人环境

应保证个人工作环境的安全：

a）个人工作桌面无个人信息、商业数据相关文档；

b）个人工作环境内个人信息、商业数据保存、管理措施；

c）个人工作环境内各种个人信息相关的移动设备使用、管理措施等。

7.1.5.3 计算机系统

应保证个人工作环境内个人计算机的安全：

a）涉及个人信息的个人计算机，应采取相应的技术和管理措施，保证计算机桌面的安全；

b）存储个人信息的个人计算机，应采取相应的技术和管理措施，保证相关文件、文件夹等相关文件存储的安全等。

7.1.6 设备和媒介

各类设备、媒介的安全，主要包括：

a）宜考虑承载个人信息相关设备管理，防电磁信息辐射泄漏、防电磁干扰、防线路截获、电源保护等；

b）各类媒介和移动设备管理，参看DB21/T 1628.3。

7.1.7 灾害预防

应考虑物理和自然灾害发生的可能性，制定应急预案；考虑设备防火、防盗、防毁等。

7.2 基础平台安全

应遵循DB21/T 1628.1 11.5确立的规则，依据信息技术、信息安全相关标准、法规，并考虑个人信息及相关因素的特点，规划、建设基础平台。

a）网络及相关设备构成的基础平台的架构、配置、部署和管理等；

b）底层系统平台的安全性、可靠性和可用性；

c）数据库、中间件、虚拟平台等应用系统支撑平台的安全性、可靠性和可用性；

d）各种安全产品、技术等构成的安全平台的配置、部署、安全特征及可靠性和可用性等。

7.3 应用系统安全

与个人信息处理相关的各类管理、业务等应用系统应遵循DB21/T 1628.1 11.5确立的规则，保证应用系统的安全性、可靠性：

a）与个人信息处理相关的各类管理类应用系统安全：

1）应用系统可靠性、安全性；

2）应用系统访问控制策略；

3）应用系统访问终端的安全性等；

b）与个人信息处理相关的各类业务系统安全：

1）业务系统的安全性、可靠性；

2）业务系统应用模式、方法等（如本地应用、远程应用等）；

3）业务系统应用的管理方式（如团队管理、权限管理等）；

4）业务系统应用的控制方式等等。

7.4 个人信息数据库安全

依据DB21/T 1628.3和DB21/T 1628.2 11章确立的规则，识别个人信息数据库及相关资源，采取相应的安全措施，保证安全性、可用性：

a）存储（保存）设备：服务器设备、集群系统、存储阵列、存储网络、移动存储等及其它存储设备，非自动处理个人信息保存设施，以及支撑数据存储设施运行的软件平台等数据存储（保存）设施和相关资源的安全性、可靠性和可用性；

b）应遵循DB21/T 1628.1 11.6和DB21/T 1628.3确立的规则，保证个人信息数据库的安全性、可靠性和可用性。

7.5 传输安全

7.5.1 管理

个人信息管理者应在管理过程中保证个人信息传输、交换的安全：

a）数据传输线路和网络基础设施的安全性；

b）管理过程中个人信息相关业务的数据传输、交换：

1）管理业务采用的方式；

2）相关责任主体、责任人的职能、职责；

3）个人信息相关数据传输、交换的安全策略；

4）所涉及个人信息的管理、处理策略（如权限、授权等）；

5）数据交换后的个人信息处理方式；

6）安全承诺等。

7.5.2 业务

个人信息管理者应在业务处理中保证个人信息传输、交换的安全：

a）数据传输线路和网络基础设施的安全性；

b）个人信息传输、交换的方式；

c）相关责任主体、责任人的工作职责、权限；

d）所涉及个人信息的管理、处理策略（如本地化处理的管理方式、远程处理的管理方式等）；

e）个人信息完整性、可用性保证（琐碎的个人信息的一致性保证）；

f）备份、恢复策略；

g）安全事件处理等。

7.6 接口安全

个人信息管理者应完善各种设备接口和终端接入的管理，避免个人信息泄漏威胁：

a）与个人信息相关的个人终端设备外置接口的管理、使用策略；

b）各种终端设备、移动终端设备接入管理策略；

c）（外网、公网）接入的管理策略、管理机制、技术手段；

d）开放网站的管理策略、访问控制、权限管理、非授权访问处理策略；

e）制度建设和相关责任主体、责任人职能、职责；

f）事故追责、处理策略等。

7.7 运行安全

应融合信息安全体系，监控个人信息相关系统的整体安全状况：

a）承载个人信息的管理、业务系统运行状况监测、预警和管理；

b）个人信息数据库结构、事务、状态监测、评估；

c）工作环境管理，包括工作场地、个人计算机终端、移动终端、其它接入设备等的安全性等；

d）系统性能评估，包括系统整体架构、系统平台、应用系统、数据管理、系统安全平台等的整体安全性、可用性，及业务融合度评估等（适用的信息安全体系安全运行）；

e）运行日志审计、工作制度、职能、职责；

f）应急管理和灾难预防恢复机制；

g）系统更新、升级管理等。

8 安全管理

8.1 风险评估

8.1.1 安全技术

应针对前述各节各个层面可能的风险因素，遵循DB21/T 1628.5确立的规则，系统评估各个层面的安全隐患。

8.1.2 体系风险

应针对前述各节安全技术的应用，系统评估PISMS的安全等级、安全技术应用的风险隐患等。

8.2 管理机制

8.2.1 策略

应遵循DB21/T 1628.1第8章和DB21/T 1628.2第12章确立的规则，建立安全管理策略和机制：

a）遵循信息安全管理相关国家标准，完善信息安全管理机制；

b）建立、完善安全技术相关规则、制度；

c）建立、完善人员管理相关制度（如系统管理人员的管理策略等）；

d）其它相关管理机制等。

8.2.2 制度

应遵循DB21/T 1628.1第8章和DB21/T 1628.2第12章确立的规则，建立、完善相关制度，使日常管理规范化、标准化。

8.3 整体安全

应融合信息安全体系，评估、优化、提高系统基础架构（包括硬件基础平台、系统平台、安全平台、数据管理平台等）的可用性、可靠性和安全性。

8.4 文档管理

应遵循DB21/T 1628.4确立的规则，完善安全技术相关文档的管理。

9 内审

PISMS内审时，应基于个人信息管理者的实际，审计安全技术的合理性、适用性、安全性和可靠性，发现安全风险、缺陷，提出整改建议。

10 持续改进

应参照DB21/T 1628.1 12.2.3，根据技术、社会、个人需求、知识更新等，持续改进安全技术。