

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

Information security-Personal information security management system-Part4: Guide
for management of personal information management documentation

2018-01-22 发布

2018-02-22 实施

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 综述	1
6 文档管理计划	1
7 文档管理	2
7.1 责任主体	2
7.2 管理制度	2
7.3 管理边界	2
7.4 管理目录	2
7.5 备案管理	3
7.6 文档规范	3
7.7 文档质量	3
8 改进	3

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体系
- 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 4 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、司丹、王小庚。

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

1 范围

本标准个人信息管理者在个人信息生命周期内，建立完善的个人信息管理文档的管理机制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。

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

3 术语和定义

DB21/T 1628.1、DB21/T 1628.2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，重点描述和指导个人信息管理相关文档管理的约束规则。

个人信息管理相关文档的管理，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 综述

本标准个人信息管理及负有个人信息管理相关职能、责任的相关责任主体提供个人信息管理文档的管理指南。本标准指导个人信息管理者在个人信息相关管理活动、行为中管理所产生的与个人信息主体权益相关的任何文档。本标准涉及个人信息管理文档，包括组织、管理机制、管理策略、内审、过程管理及个人信息安全管理体系相关的各类材料等与个人信息生命周期相关联的所有文档等。

在个人信息管理过程中，在个人信息安全管理体系构建、实施、运行中，负有个人信息管理相关职能、责任的相关责任主体，应遵从DB21/T 1628.1 8.5，特别关注管理活动和行为相关的记录、文件等，以便有效管理文档。

6 文档管理计划

应在制定个人信息管理计划时制定相应的文档管理计划：

- a) 明确个人信息管理文档的类型、分布、存在形态、存储（保存）方式等物理形式；
- b) 明确个人信息管理相关文档的管理形式、策略、方法等；
- c) 明确个人信息管理文档管理的基础准备，包括相关资源等；
- d) 识别、组织个人信息管理相关文档的策略；
- e) 评估个人信息管理文档的管理风险及措施、方法；
- f) 评估个人信息管理文档的管理效果；
- g) 评估个人信息管理文档的管理计划实施效果等。

注1：个人信息管理文档管理计划应由个人信息管理机构制定。

7 文档管理

7.1 责任主体

个人信息管理者代表应指定个人信息管理相关文档的管理责任主体：

- a) 责任主体应明确个人信息管理相关文档的管理职责，参见DB21/T 1628.2 12.1.1；
- b) 责任主体应确定对个人信息管理相关文档实施管理所需资源的可靠性、安全性、可用性；
- c) 责任主体应确定所管理的个人信息管理相关文档质量的可靠性、可用性；
- d) 责任主体应做出安全承诺，避免个人信息管理相关文档遗失等责任事故等。

7.2 管理制度

应建立个人信息管理相关文档的管理制度，主要应包括：

- a) 责任主体的职责；
 - b) 个人信息管理文档存储（保存）规定；
 - c) 个人信息管理文档质量要求；
 - d) 个人信息管理文档使用规定；
 - e) 备案管理；
 - f) 责任事故处理等。
- 及其它必要的规定。

7.3 管理边界

应确定个人信息管理文档的管理边界：

- a) 纵向：个人信息管理者最高管理层与管理、业务层相关的个人信息管理文档；
- b) 纵向：管理、业务层与全体员工相关的个人信息管理文档；
- c) 横向：部门之间涉及个人信息的所有文档；
- d) 外部：与客户、社会组织之间相关的所有个人信息文档；
- e) 个人：员工个人保有的自身个人信息或他人个人信息相关文档等。

7.4 管理目录

7.4.1 内容

依据DB21/T 1628.1 8.5，个人信息管理相关文档主要应包括：

- a) 最高管理者签发的各种个人信息管理相关的文件，如任命书、执行计划等；
- b) 个人信息管理机构发布的各种文件，如计划、规章、方针、职能等；

- c) 个人信息管理活动、行为的各种记录；
- d) PISMS构建、实施、运行的各种相关文档等。

7.4.2 分类

建立个人信息管理相关文档的管理目录，应确定文档的类别，便于管理：

a) 应根据个人信息的分布、存在形态、存储（保存）方式、管理特征、风险因子等个人信息管理者实际，确定个人信息管理相关文档管理的分类原则和标准；

b) 个人信息管理相关文档应包括自动处理文档和非自动处理文档，分类原则和标准应统一考虑。

注2：DB21/T 1628.3 确定了个人信息数据库形式，本部分确定了个人信息管理相关文档的管理形式。

7.4.3 识别

应根据文档管理边界，识别并组织、整理所有个人信息管理相关文档，并根据分类原则和标准，分门别类管理个人信息管理相关文档。

7.4.4 目录

确定个人信息管理相关文档的分类原则和标准，并识别所有个人信息管理相关文档后，应建立相应的个人信息管理相关文档的管理目录。

7.5 备案管理

应遵从DB21/T 1628.1 8.5的规定，建立备案管理制度。

7.6 文档规范

个人信息管理机构发布的各种文件、PISMS构建、实施、运行的各种相关文档等，应规范文档格式，主要应包括：

a) 封面：应含名称、文件编号、版本号、制定日期、审批人、制作人、编制单位等；

b) 首页：应设置修改控制页，记录相应文件的修订情况，包括版本号、制定/修改日期、修改原因、修改人、审批人等；

c) 排版格式：应统一、规范。标题宜采用3号黑体、正文宜采用4号宋体；

d) 附录：引用或对应的相关文档、记录，应作为附录列出，附在相应文件后。

7.7 文档质量

应保证个人信息管理相关文档的质量：

a) 文档应清晰、明确；

b) 文档应简明、易读；

c) 文档无涂抹、污损等。

8 改进

根据DB21/T 1628.1 12章和DB21/T 1628.2 18章，应在过程管理、改进中持续改进、完善文档管理。