JIS

JAPANESE
INDUSTRIAL
STANDARD

Translated and Published by
Japanese Standards Association

JIS Q 15001 : 2017

Personal information protection management systems—Requirements

ICS 35.080

Reference number : JIS Q 15001 : 2017 (E)

Date of Establishment: 1999-03-20
Date of Revision: 2017-12-20
Date of Public Notice in Official Gazette: 2017-12-20
Investigated by: Japanese Industrial Standards Committee
Standards Board for IEC area
Technical Committee on Information

JIS Q 15001:2017, First English edition published in 2018-05

Translated and published by: Japanese Standards Association
Mita MT Building, 3-13-12, Mita, Minato-ku, Tokyo, 108-0073 JAPAN

In the event of any doubts arising as to the contents,
the original JIS is to be the final authority.

Printed in Japan

HT/AT

Contents

Page

Foreword

This Japanese Industrial Standard has been revised by the Minister of Economy, Trade and Industry, through deliberations at the Japanese Industrial Standards Committee in accordance with the Industrial Standardization Law. Consequently **JIS Q 15001** : 2006 is replaced with this Standard.

Attention is drawn to the possibility that some parts of this Standard may conflict with patent rights, applications for a patent after opening to the public or utility model rights. The relevant Minister and the Japanese Industrial Standards Committee are not responsible for identifying any of such patent rights, applications for a patent after opening to the public or utility model rights.

Personal information protection management systems—Requirements

0 Introduction

This Japanese Industrial Standard was first established in 1999, then revised once (this revised edition hereafter referred to as the previous edition) in 2006. The revision at this time has been made to bring the contents of this Standard into conformance with the revised stipulations in the laws related to protection of personal information.

No corresponding International Standard has been established at this point. Tables of correspondence between this Standard and the previous edition are shown in Annex D.

0.1 Summary

This Standard has been prepared to provide the requirements for establishing, implementing, maintaining and continually improving personal information protection management systems. Adoption of a personal information protection management system is an organizational strategic decision. The establishment and implementation of a personal information protection management system of an organization are affected by the needs and objectives of the organization, the requirements for personal information protection, the process used by the organization, and the size and structure of the organization. All of these factors are expected to change with time.

The personal information protection management system brings a feeling of trust to the interested parties that, by applying a risk management process, personal information protection is maintained and the risks are appropriately controlled.

It is important to regard a personal information protection management system as a part of the whole organizational process and management structure and to incorporate it into the structure, and to take into consideration the personal information protection in designing the processes, information systems and controls. The personal information protection management system is expected to be introduced on a scale matching the needs of the organization.

This Standard may be used by an organization to evaluate internally its own capability of meeting the personal information protection requirements or by external parties to make such evaluation on the organization.

The sequence of the requirements in this Standard neither reflects the order of their importance nor reflects the order of implementation. The list item symbols in this Standard, such as **a**), **b**) or **1**), **2**), are provided only for the purpose of easy reference.

0.2 Relevance to other management system standards

This Standard refers to Annex SL of Consolidated **ISO** Supplement of **ISO/IEC** Directives Part 1 for the High Level Structure (HLS), common sub-clause titles, identical core text and common terms and core definitions, thereby ensuring relevance to other management system standards adopting Annex SL.

These common efforts specified in Annex SL are useful for an organization operating two or more management systems.

1 Scope

This Standard specifies the requirements for establishing, implementing, maintaining and improving a personal information protection management system regarding the personal information which the organization uses for its own business. The requirements specified in this Standard are intended to be applicable to all organizations independent of type or size of their businesses. The organizations here mean the personal information handling business operators as specified by the Act on Protection of Personal Information (Act No. 57, 2003) (hereafter referred to as Personal Information Protection Act).

NOTE : The term "business" in "the organization uses for its business" means what is accepted as a business by socially accepted norms and does not necessarily refer to profit-making businesses only. Therefore, personal information of a worker is the information used for the business.

2 Normative references

This Standard has no normative references.

3 Terms and definitions

For the purpose of this Standard, the terms and definitions provided in the Personal Information Protection Act, as well as the following apply.

3.1 organization

person or group of people containing a responsible and authoritative top management, which has its own functions with responsibilities, authorities and relationships to achieve its objectives (**3.8**)

3.2 interested party

person or organization (**3.1**) that can affect, be affected by, or perceive themselves to be affected by a decision or activity

(see **2.41** of **JIS Q 27000**:2014)

3.3 requirement

need or expectation that is stated explicitly, generally implied or obligatory

(see **2.63** of **JIS Q 27000**:2014)

NOTE : "Generally implied" means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied.

3.4 management system

set of interrelated or interacting elements of an organization (**3.1**) to establish policies (**3.7**) and objectives (**3.8**) and processes (**3.12**) to achieve those objectives

NOTE 1 A management system can address a single discipline or several disciplines.