ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 31496-2023

Information technology - Security techniques - Information security management systems - Guidance

信息技术 安全技术 信息安全管理体系 指南

Issued on: May 23, 2023 **Implemented on: December 1, 2023**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1:1-2020 "Guidelines for Standardization Work Part 1: Structure and Drafting Rules for Standardization Documents" drafting: This document replaces GB/T 31496-2015 "Information Technology Security Technology Information Security Management System Implementation Guide", and Compared with GB/T 31496-2015, except for structural adjustment and editorial changes, the main technical changes are as follows:

---Changed the scope, explained and provided guidance in accordance with the requirements of GB/T 22080-2016;

---The previous edition adopted a project approach, and each project contained a series of activities: The project method is no longer adopted in the revised version, but instead Guidance is provided for each requirement, regardless of the order in which the requirements are implemented: This document is equivalent to ISO /IEC 27003:2017 "Information Technology Security Technology Information Security Management System Guidelines": The following minimal editorial changes have been made to this document:

--- Added note to 4:2: Please note that some contents of this document may refer to patents: The issuing agency of this document assumes no responsibility for identifying patents: This document is proposed and managed by the National Information Security Standardization Technical Committee (SAC/TC260): This document was drafted by: China Electronics Standardization Research Institute, China Network Security Review Technology and Certification Center, China Conformity Assessment National Accreditation Center, Hangzhou Anheng Information Technology Co:, Ltd:, PetroChina Changqing Petrochemical Branch, Tencent Cloud Computing (Beijing) Co:, Ltd:, China Power Great Wall Internet System Application Co:, Ltd:, Shanghai

30 Guardian Information Security Co:, Ltd:, Beijing Saixi Certification Co:, Ltd:, Xidian University, Heilongjiang Cyberspace Research Center, Beijing Information Security

Evaluation Center, China Institute of Software, Academy of Sciences, Chongqing University of Posts and Telecommunications, Anhui Institute of Science and Technology, Beijing Shenzhou NSFOCUS Technology Co:, Ltd:, China Comservice Consulting Design Institute Co:, Ltd:, Beijing Zhongke Weilan Technology Co:, Ltd: The main drafters of this document: Wang Huili, Shangguan Xiaoli, Xu Yuna, Fu Zhigao, Ren Zejun, You Qi, Zhou Yachao, Zhao Lihua, Fan Bo, Min Jinghua, Zhang Dongju, Ma Wenping, Gan Lu, Li Yuan, Fang Zhou, Zhang Liwu, Liang Wei, Huang Yonghong, Zhang Heng, Cao Hao, Yin Xiaopeng, Song Xue, Gao Lifen, Chen Hong, Yang Mutian, Pei Xinping: The release status of previous versions of this document and the documents it replaces are as follows:

---First published as GB/T 31496-2015 in:2015;

--- This is the first revision:

This document provides guidance on the information security management system (ISMS) requirements specified in GB/T 22080, and provides relevant recommendations ("should"), possibilities ("may") and permissibility ("may"): It is not the purpose of this document to provide a general overview of all aspects of information security guide: Chapters 4 to 10 of this document reflect the structure of GB/T 22080-2016: This document does not add any new requirements for ISMS and its related terms and definitions: Organizations should refer to the requirements of GB/T 22080 and Definition of GB/T 29246: Organizations implementing an ISMS are under no obligation to follow the guidance in this document: The ISMS emphasizes the importance of the following stages:

--- Understand the needs of the organization and the necessity of establishing information security policy and information security objectives;

--- Assess the organization's risks related to information security;

---Implement and operate information security processes, controls and other risk treatment measures;

--- Monitor and review the performance and effectiveness of the ISMS;

---Continuous improvement: Similar to other types of management systems, an ISMS includes the following key components:

b) Personnel with defined responsibilities:

1 Scope

GB/T 31496-2023 is the Chinese guidance on implementing an information security management system. The requirements standard says what an ISMS must contain; it does not say how an organisation that has never had one gets from nothing to a working system, and the common failure is a set of policies written to pass an audit that nobody in the business recognises. This document walks through the clauses in implementation terms. It

covers the organisational context, leadership, planning, support with its resources, competence, awareness, communication and documented information, operation including operational planning and control, the information security risk assessment and risk treatment, performance evaluation with monitoring, measurement, internal audit and management review, and improvement. It replaces GB/T 31496-2015 and took effect on 1 December 2023.

This document provides explanations and guidance for GB/T 22080-2016:

2 Normative references

The contents of the following documents constitute the essential provisions of this document through normative references in the text: Among them, dated references For documents, only the version corresponding to the date is applicable to this document; for undated reference documents, the latest version (including all amendments) is applicable to this document:

GB/T 22080-2016 Information Technology Security Technology Information Security Management System Requirements (ISO / IEC 27001:2013, IDT)

GB/T 29246-2017 Information Technology Security Technical Information Security Management System Overview and Vocabulary (ISO /

IEC 27000: 2016, IDT) ISO /

IEC 27001 Information technology, network security and privacy protection information security management system requirements (Information ments)

3 Terms and Definitions

The terms and definitions defined in GB/T 29246-2017 apply to this document:

4 Organizational context

1 Understanding the organization and its context required activity The organization determines those external and internal factors that are relevant to its intentions and affect its ability to achieve the intended outcomes of its information security management system (ISMS): question: explain As a component function of an ISMS, an organization continuously analyzes itself and its environment: This analysis focuses on internal and external issues, which These issues affect information security and how it is managed in some way, and are relevant to the objectives of the organization: Analyzing these questions serves three purposes:

--- Understand the context to determine the scope of the ISMS;

---Analyze the context to determine risks and opportunities;