ICS 35.040

L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

中华人民共和国国家标准

GB/T 202697-2006

Information security technology- Information system security management requirements

信息安全技术　信息系统安全管理要求

Issued on May 31, 2006　　Implemented on December 01, 2006

Issued by General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China

Standardization Administration of the People's Republic of China

Contents

Foreword

Annex A and Annex B to this Standard are informative annexes.

This Standard is proposed by and under the jurisdiction of National Information Security Standardization Technical Committee.

Drafting organizations of this Standard: Beijing Siyuan Xinchuang Information Security Consulting Co., Ltd., Jiangnan Computing Technology Research Institute Technical Service Center.

Main drafters of this Standard: Chen Guanzhi, Wang Zhiqing, Ji Zengrui, Jing Qianyuan, Song Jianping.

Introduction

Classified Protection of Information Security refers to classified protection of security for information and information system in information security related physical level, network level, system level, application level and management level. Management level is throughout the other levels to guarantee the implementation of classified protection of security in other levels. This Standard proposes classified management of security requirement for security protection of information and information system, elaborates security management factors and the strengths, performs management requirements in five levels on classified protection of information security and is conducive to security management implementation, assessment and inspection. Division of classified protection of security in GB 17859-1999 is determined based on the relationship between security technology and security risk control; division of classified protection of security in Gong Tong Zi [2004] No. 66 is determined based on the extent of damage to national security, social order, economic development and public interest. The common grounds of them is that the higher security level is, the higher incurred safety technical costs and administration costs are, thus the greater expected security threats withstood are, the stronger established security confidence is, the smaller the risk in use of information system is.

This Standard takes security management elements as the basic components of describing security management requirements. Security management factor refers to control methods and measures taken in management view in order to meet the security requirements of information system classified protection of security. In accordance with the division of classified protection of security in GB 17859-1999, different security protection classes have different security management requirements, which are reflected in increase of management elements and strengthening of management strength. For each management element, respectively list different management strengths based on particular circumstances, which are divided into a minimum of five classes or not divided. In the detailed description, unless otherwise specified, description of high-level management strength is generally based on low-grade description.

Information system refers to the system or network that is composed of computer and

related and supporting equipments and stores, transmits or processes information based on certain application objectives and rules; information refers to digitized information stored, transmitted and processed in information system. This Standard involves administrators of information system, including State organs, public institutions, industrial and mining enterprises, companies, groups and other types and sizes of organizations, hereinafter referred to as “organization”.

Security mechanism that information technically adopts shall be determined based on relevant technical standards; this Standard only proposes management requirements that ensure implementation of these security mechanisms. Technically closed management is an integral part of technical implementation; corresponding security managements are not required if information system does not adopt this technology according to specific business and security requirements. Technical requirements Technical requirements difficult to be separated from management description will be included in management requirements, specific implementation of which shall refer to relevant technical standards.

Confidential management of information system that involves State secrets shall follow national management provisions on confidentiality and relevant standards to implement.

Description on correspondence of information system security management elements and the strengths to classified requirements of information system security management is as shown in annex A. In order to help readers understand and use security management requirements of these information systems from the view of security management concept, annex B provides descriptions on information system security management concept.

Information Security Technology—Information System Security Management Requirements

1 Scope

This Standard specifies management requirements of security classes required for information system security based on the division of security classes required by information system security.

This Standard applies to information system security management based on classified requirements.

2 Normative references

The articles contained in the following documents have become this document when they are quoted herein. For the dated documents so quoted, all subsequent modifications (Including all corrections) or revisions made thereafter do not apply to this standard. However, the parties that reach an agreement according to this standard are encouraged to study whether the latest versions of these documents may be used. For the undated documents so quoted, the latest versions (including all modification sheets) apply to this document.

GB 17859-1999 Classified criteria for security protection of computer information system

GB/T 20271-2006 Information security technology Common security techniques requirement for information system

3 Terms and definitions

Following terms and definitions defined in GB 17859—1999 apply to this Standard.

3.1

Integrity

It includes data security and system security. Data security represents all the characteristics of data, i.e. accuracy and consistency of data remain unchanged regardless of any changes of data; system integrity represents the quality that system can fulfill the operation purposes under the circumstance of preventing unauthorized users from modifying or using resources and prevention authorized users from incorrectly modifying or using resources.

3.2

Availability

Security attribute that represents the extent of being accessed or used upon the request of authorized entity.

3.3

Access control

Security mechanism that controls access activities between entities based on a specific rule and can prevent unauthorized use of resources.

3.4

Security audit

Security mechanism audits security-related event, records necessary information in the form of log and properly processes according to the requirements of determined rules.

3.5

Authentication information

Information used to confirm the authenticity of identity information.

3.6

Sensitivity

Characteristics that represent resource value or importance and may also contain the vulnerability of these resources.

3.7

Risk assessment

The process of determining information system security risk through comprehensive analysis of information system asset value/importance, the threats to information system and vulnerability of information system and through scientific identification and assessment of information system and the processing, transmission and the confidentiality, integrity and availability of information stored., etc.

3.8

Security policy

It mainly refers to course of action, routes, work mode, guiding principles or procedures.

4 General requirements of information system security management

北京文心雕语翻译有限公司
Beijing Lancarver Translation Inc.

完整版本请在线下单/Order Checks Online for Full version

联系我们/or Contact:

TEL: 400-678-1309

QQ: 19315219 | Skype: Lancarver

Email：info@lancarver.com

http://www.lancarver.com

线下付款方式：

I. 对公账户：

单位名称：北京文心雕语翻译有限公司

开 户 行：中国工商银行北京学清路支行

账　　号：0200 1486 0900 0006 131

II. 支付宝账户：info@lancarver.com

III. Paypal: info@lancarver.com

注: 付款成功后，请预留电邮，完整版本将在一个工作日内通过电子 PDF 或 Word 形式发送至您的预留邮箱，如需索取发票，下单成功后的三个工作日内安排开具并寄出，预祝合作愉快！

NOTE All documents on the store are in electronic Adobe Acrobat PDF format, there is not sell or ship documents in hard copy. Mail the order and payment information to info@lancarver.com , you will shortly receive an e-mail confirming your order.