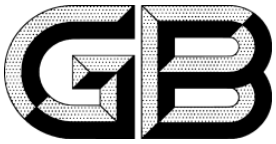

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

GB/T 25068.1-2020

Information technology. Security techniques. Network security - Part 1: Overview and concepts

Issued on: November 19, 2020 **Implemented on: June 1, 2021**

Issued by: SAMR; SAC

Table of Contents

Foreword

GB/T 25068-2020 "Information technology - Security techniques - Network security" is currently divided into the following 5 parts.

- Part 1.Overview and concepts;
- Part 2.Guidelines for the design and implementation of network security;
- Part 3.Securing communications between networks using security gateways;
- Part 4.Securing remote access;
- Part 5.Securing communications across networks using virtual private networks.

This is Part 1 of GB/T 25068.

This Part was drafted in accordance with the rules given in GB/T 1.1-2009.

This Part replaces GB/T 25068.1-2012 "Information technology. Security techniques. Network security -- Part 1.Overview and concepts". Compared with GB/T 25068.1-2012, the main technical changes in this Part are as follows.

- Add the contents such as "Supporting controls", " Reference network scenarios - Risks, design, techniques and control issues" and "Develop and test security solution". Delete contents such as "Target" and "Crypto-based services in public infrastructure" (see Chapter 8, Chapter 10, Chapter 12 of this Edition; Chapter 2, Chapter 13 of Edition 2012);

- Add the contents such as "Supporting controls", "Reference network scenarios - Risks, design, techniques and control issues" and "Develop and test security solution". Delete contents such as "Target" and "Crypto-based services in public infrastructure" (see Chapter 8, Chapter 10, Chapter 12 of this Edition; Chapter 2, Chapter 13 of Edition 2012);

- Delete the dated references to GB/T 22081-2008, GB/T 25068.2-2012, and GB/T 25068.3-2010.Add the undated references to ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 (see Chapter 2 of this Edition; Chapter 2 of Edition 2012);

- Delete the terms and definitions such as "security dimension" and "spam". Add the terms and definitions such as "architecture" and "information security policy" (see Chapter 3 of this Edition; Chapter 3 of Edition 2012);

- Delete the abbreviations such as "Telnet" and "TETRA". Add the abbreviations such as "BPL", "CA" and "DPNSS" (see Chapter 4 of this Edition; Chapter 4 of Edition 2012);

- Delete network connection types, identification of trust relationships, trust relationship references, and potential vulnerability types. Add the conceptual model of network security risk areas, network security risk assessment and management process (see Chapter 5 ~ Chapter 8 of this Edition; Chapter 7, Chapter 10 ~ Chapter 12 of Edition 2012);

- Add cross-references between the security control section in this Part and the relevant provisions in ISO/IEC 27001 and ISO/IEC 27002 and the SecOPs document sample template (see Annex A and Annex B of this Edition).

This Part uses translation method to identically adopts ISO/IEC 27033-1.2015 "Information technology - Security techniques - Network security - Part 1.Overview and concepts".

The Chinese documents which have consistency with the international normative reference in this Part are as follows.

- GB/T 9387 (all parts), Information technology. Open Systems Interconnection. Basic Reference Model [ISO/IEC 7498 (all parts)];
- GB/T 22080-2016, Information technology -- Security techniques -- Information security management systems -- Requirements (ISO/IEC 27001.2013, IDT);
- GB/T 22081-2016, Information technology -- Security techniques -- Code of practice for information security controls (ISO/IEC27002.2013, IDT);
- GB/T 29246-2017, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary (ISO/IEC 27000.2016, IDT);
- GB/T 31722-2015, Information technology -- Security techniques -- Information security risk management (ISO/IEC 27005.2008, IDT).

This Part made the following editorial modifications.

- In Chapter 2, add the international document ISO/IEC 27000 which is used as a normative reference in the text.

This Part was proposed by and shall be under the jurisdiction of National Technical Committee on Information Security of Standardization Administration of China (SAC/TC 260).

The drafting organizations of this Part. Heilongjiang Provincial Cyberspace Research Center, China Electronics Technology Standardization Institute, Beijing Antian Network Security Technology Co., Ltd., Hangzhou Anheng Information Technology Co., Ltd., Harbin University of Science and Technology, Xi'an Xidian Jietong Wireless Network Communications Co., Ltd.

Main drafters of this Part. Fang Zhou, Qu Jiaxing, Ma Chao, Gu Juntao, Shubin, Liu