

ICS 35.240
CCS A 90

GA

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GA/T 1141-2014

**Information security technology-Computer configuration
requirements for security classified protection**

信息安全技术 主机安全等级保护配置要求

(English Translation)

Issued on: March 14, 2014

Implemented on: March 14, 2014

Issued by: Ministry of Public Security

Table of Contents

Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Second stage host security configuration requirements
4.1 Windows host security configuration
4.1.1 Authentication security configuration
4.1.2 Access Control Security Configuration
4.1.3 Security Audit Security Configuration
4.1.4 Intrusion Prevention Security Configuration
4.1.5 Malicious code prevention Security Configuration
4.1.6 Resource Control Security Configuration
4.2 Unix-Host Security Configuration
4.2.1 Authentication Security Configuration
4.2.2 Access Control Security Configuration
4.2.3 Security Audit Security Configuration
4.2.4 Intrusion Prevention Security Configuration
4.2.5 Malicious code prevention Security Configuration
4.2.6 Resource Control Security Configuration
5 Third-level host security configuration requirements
5.1 Windows Host Security Configuration
5.1.1 Authentication security configuration
5.1.2 Security marker
5.1.3 Access Control Security Configuration
5.1.4 Security Audit Security Configuration
5.1.5 Remaining Information Protection Security Configuration
5.1.6 Intrusion Prevention Security Configuration
5.1.7 Malicious code prevention security configuration
5.1.8 Resource Control Security Configuration
5.2 Unix-8 Host Security Configuration
5.2.1 Authentication security configuration
5.2.2 Security marker

- 5.2.3 Access Control Security Configuration
- 5.2.4 Security Audit Security Configuration
- 5.2.5 Remaining information protection security configuration
- 5.2.6 Intrusion Prevention Security Configuration
- 5.2.7 Security Configuration 10 malicious code prevention
- 5.2.8 Resource Control Security Configuration
- 6 Fourth stage host security configuration requirements
 - 6.1 Windows Host Security Configuration
 - 6.1.1 Authentication security configuration
 - 6.1.2 Security marker
 - 6.1.3 Access control security configuration
 - 6.1.4 Trusted Path
 - 6.1.5 Security Audit Security Configuration
 - 6.1.6 Remaining information protection security configuration
 - 6.1.7 Intrusion Prevention Security Configuration
 - 6.1.8 Security Configuration 14 malicious code prevention
 - 6.1.9 Resource Control Security Configuration
 - 6.2 Unix-host security configuration
 - 6.2.1 Authentication security configuration
 - 6.2.2 Security marker
 - 6.2.3 Access control security configuration
 - 6.2.4 Trusted Path
 - 6.2.5 Security Audit Security Configuration
 - 6.2.6 Remaining information protection security configuration
 - 6.2.7 Intrusion Prevention Security Configuration
 - 6.2.8 Security Configuration 17 malicious code prevention
 - 6.2.9 Resource Control Security Configuration

Foreword

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

This standard was proposed by the Ministry of Public Security Network Security Protection Agency.

This standard is under the jurisdiction of the Ministry of Public Security Information System Standardization Technical Committee.

This standard was drafted. Ministry of Public Security of Computer Information System Security Product Quality Supervision and Inspection Center, Ministry of Public Security Network Security Protection Agency, public Third Institute Abe.

1 Scope

This standard specifies the second level to the fourth level information systems, various types of host operating system security configuration requirements.

This standard applies to the second level to the fourth level information system security configuration of all types of the host operating system.

2 Normative references

The following documents for the application of this document is essential. For dated references, only the dated version suitable for use herein Member. For undated references, the latest edition (including any amendments) applies to this document.

GB/T 22239-2008 Information security technology information system security protection essential requirements
GB/T 25069-2010 Information security technology terms

3 Terms and Definitions

Terms and definitions GB/T 22239-2008 and GB/T 25069-2010 defined apply to this document.

4.1.1.1 Identity Security Configuration

The host response settings for each account login password, the password should not be empty.

4.1.1.2 Identification of information security configuration

Should enable the host password security policies and set the following.

- a) Minimum password length;
- b) password complexity;
- c) the maximum password age.

4.1.1.3 Identification Process Security Configuration

Should enable the host account lockout policy, and set the following.

- a) Account lockout threshold;
- b) to reset the account lockout count time;

c) account lockout time.