

ICS 35.40
CCS L 80

GA

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

GA/T 1390.2-2017

**Information security technology-General requirements for
classified protection of cyber security-Part 2: Special security
requirements for cloud computing**

信息安全技术 网络安全等级保护基本要求 第2部分：云计算安全扩展要求
(English Translation)

Issued on: May 8, 2017

Implemented on: May 8, 2017

Issued by: Ministry of Public Security

Table of Contents

Foreword V.
Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Cloud Computing Security Overview
4.1 Cloud computing platform
4.2 Cloud computing platform rating
5 Level 1 safety requirements
5.1 Technical Requirements
5.1.1 Physical and Environmental Safety
5.1.2 Network and Communication Security
5.1.2.1 Network Architecture
5.1.2.2 Access Control
5.1.2.3 Intrusion prevention
5.1.2.4 Security Audit
5.1.3 Equipment and computing security
5.1.3.1 Identification
5.1.3.2 Access Control
5.1.3.3 Security Audit
5.1.3.4 Intrusion prevention
5.1.3.5 Resource Control
5.1.3.6 Mirroring and Snapshot Protection
5.1.4 Application and Data Security
5.1.4.1 Security Audit
5.1.4.2 Resource Control
5.1.4.3 Interface Security
5.1.4.4 Data Integrity
5.1.4.5 Data Confidentiality
5.1.4.6 Data backup and recovery
5.1.4.7 Residual Information Protection
5.2 Management Requirements

5.2.1 Security management agencies and personnel

5.2.1.1 Authorization

5.2.1.2 Personnel recruitment

5.2.2 Safety Construction Management

5.2.2.1 Test and acceptance

5.2.2.2 Cloud service provider choice

5.2.2.3 Supply Chain Management

5.2.3 Safe Operation Management

5.2.3.1 Environmental Management

5.2.3.2 Monitoring and Audit Management

6 Level 2 safety requirements

6.1 Technical Requirements

6.1.1 Physical and Environmental Safety

6.1.2 Network and Communication Security

6.1.2.1 Network Architecture

6.1.2.2 Access Control

6.1.2.3 Intrusion Prevention

6.1.2.4 Security Audit

6.1.3 Equipment and Computing Security

6.1.3.1 Identification

6.1.3.2 Access Control

6.1.3.3 Security Audit

6.1.3.4 Intrusion Prevention

6.1.3.5 Resource Control

6.1.3.6 Mirroring and Snapshot Protection

6.1.4 Application and Data Security

6.1.4.1 Security Audit

6.1.4.2 Resource Control

6.1.4.3 Interface Security

6.1.4.4 Data Integrity

6.1.4.5 Data Confidentiality

6.1.4.6 Data backup and recovery

6.1.4.7 Residual Information Protection

6.2 Management Requirements

6.2.1 Security management agencies and personnel

- 6.2.1.1 Authorization
- 6.2.1.2 Personnel recruitment
- 6.2.2 Safety Construction Management
 - 6.2.2.1 Test acceptance
 - 6.2.2.2 Cloud service provider choice
 - 6.2.2.3 Supply Chain Management
- 6.2.3 Safe Operation Management
 - 6.2.3.1 Environmental Management
 - 6.2.3.2 Monitoring and Audit Management
- 7 Level 3 Safety Requirements
 - 7.1 Technical Requirements
 - 7.1.1 Physical and Environmental Safety
 - 7.1.2 Network and Communication Security
 - 7.1.2.1 Network Architecture
 - 7.1.2.2 Access Control
 - 7.1.2.3 Intrusion Prevention
 - 7.1.2.4 Security Audit
 - 7.1.3 Equipment and Computing Security
 - 7.1.3.1 Identification
 - 7.1.3.2 Access Control
 - 7.1.3.3 Security Audit
 - 7.1.3.4 Intrusion Prevention
 - 7.1.3.5 Malicious Code Prevention
 - 7.1.3.6 Resource Control
 - 7.1.3.7 Mirroring and Snapshot Protection
 - 7.1.4 Application and Data Security
 - 7.1.4.1 Security Audit
 - 7.1.4.2 Resource Control
 - 7.1.4.3 Interface Security
 - 7.1.4.4 Data Integrity
 - 7.1.4.5 Data Confidentiality
 - 7.1.4.6 Data backup and recovery
 - 7.1.4.7 Residual Information Protection
 - 7.2 Management Requirements
 - 7.2.1 Security management agencies and personnel

- 7.2.1.1 Authorization
- 7.2.1.2 Personnel recruitment
- 7.2.2 Security Construction Management
 - 7.2.2.1 Security Program Design
 - 7.2.2.2 Test acceptance
 - 7.2.2.3 Cloud Service Provider Selection
 - 7.2.2.4 Supply Chain Management
- 7.2.3 Safe Operation Management
 - 7.2.3.1 Environmental Management
 - 7.2.3.2 Configuration Management
 - 7.2.3.3 Monitoring and Audit Management
- Level 4 Safety Requirements
- 8.1 Technical Requirements
 - 8.1.1 Physical and Environmental Safety
 - 8.1.2 Network and Communication Security
 - 8.1.2.1 Network Architecture
 - 8.1.2.2 Access Control
 - 8.1.2.3 Intrusion Prevention
 - 8.1.2.4 Security Audit
 - 8.1.3 Equipment and Computing Security
 - 8.1.3.1 Identification
 - 8.1.3.2 Access Control
 - 8.1.3.3 Security Audit
 - 8.1.3.4 Intrusion Prevention
 - 8.1.3.5 Malicious Code Prevention
 - 8.1.3.6 Resource Control
 - 8.1.3.7 Mirroring and Snapshot Protection
 - 8.1.4 Application and Data Security
 - 8.1.4.1 Security Audit
 - 8.1.4.2 Resource Control
 - 8.1.4.3 Interface Security
 - 8.1.4.4 Data Integrity
 - 8.1.4.5 Data Confidentiality
 - 8.1.4.6 Data backup and recovery
 - 8.1.4.7 Residual Information Protection