

ICS 35.040
CCS L 80



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

GB/T 31168-2014

**Information security technology -- Security capability
requirements of cloud computing services**

信息安全技术 云计算服务安全能力要求

(English Translation)

Issued on: September 3, 2014

Implemented on: April 1, 2015

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

Table of Contents

Foreword...	6
Introduction...	7
1 Scope...	8
2 Normative References...	8
3 Terms and Definitions...	8
4 Overview...	9
4.1 Implementation Responsibilities for the Security Measures of Cloud Computing...	9
4.2 Action Range for the Security Measures of Cloud Computing...	11
4.3 Classification of Security Requirements...	11
4.4 Expression Form of Security Requirements...	13
4.5 Adjustment of Security Requirements...	13
4.6 Security Plan...	14
4.7 Structure of This Standard...	15
5 Security of System Development and Supply Chain...	15
5.1 Strategies and Procedures...	15
5.2 Resource Distribution...	15
5.3 System Life Cycle...	16
5.4 Procurement Process...	16
5.5 System Documentation...	17
5.6 Security Engineering Principle...	17
5.7 Critical Analysis...	18
5.8 External Information System Service and Relevant Service...	18
5.9 Security System Framework of Developer...	19
5.10 Development Process, Standards and Tools...	19
5.11 Developer Configuration Management...	20
5.12 Security Test and Assessment of Developer...	21
5.13 Training Provided by the Developer...	22
5.14 Tamper Resistance...	22
5.15 Module Factuality...	22
5.16 Unsupported System Module...	23
5.17 Supply Chain Protection...	23
6 Protection of System and Communication...	25

6.1 Strategies and Procedures...	25
6.2 Boundary Protection...	25
6.3 Transmission Security and Integrity...	26
6.4 Network Interruption...	26
6.5 Trusted Path...	27
6.6 Password Usage and Management...	27
6.7 Coordinated Computing Device...	27
6.8 Mobile Code...	27
6.9 Session Certification...	27
6.10 Physical Connection of Mobile Device...	28
6.11 Malicious Code Protection...	28
6.12 Memory Protection...	28
6.13 System Virtualization Security...	28
6.14 Network Virtualization Security...	29
6.15 Storage Virtualization Security...	30
7 Access Control...	30
7.1 Strategies and Procedures...	30
7.2 User Identification and Authentication...	31
7.3 Device Identification and Authentication...	31
7.4 Identifier Management...	31
7.5 Authentication Certificate Management...	32
7.6 Feedback of Authentication Certificate...	33
7.7 Authentication of Cryptographic Module...	33
7.8 Account Management...	33
7.9 Implementation of Access Control...	34
7.10 Control of Information Flow...	34
7.11 Minimum Privilege...	35
7.12 Unsuccessful Log-in Try...	36
7.13 Notice on Use of System...	36
7.14 Notice on Last Visit...	36
7.15 Concurrent Session Control...	36
7.16 Session Lock-in...	37
7.17 Actions May be Taken in Case of Lacking Identification and Authentication...	37
7.18 Security Attribute...	37
7.19 Remote Access...	37

7.20 Wireless Access...	38
7.21 Use of External Information System...	38
7.22 Information Sharing...	39
7.23 Content accessible to the Public...	39
7.24 Data Excavation Protection...	39
7.25 Medium Access and Use...	39
7.26 Service Closure and Data Migration...	40
8 Configuration Management...	40
8.1 Strategies and Procedures...	40
8.2 Configuration Management Plan...	40
8.3 Base Line Configuration...	41
8.4 Change Control...	41
8.5 Setting of Configuration Parameters...	42
8.6 Minimum Functional Principle...	42
8.7 Information System Module List...	43
9 Maintenance...	44
9.1 Strategies and Procedures...	44
9.2 Controlled Maintenance...	44
9.3 Maintenance Tool...	44
9.4 Remote Maintenance...	45
9.5 Maintenance Personnel...	45
9.6 Timely Maintenance...	45
9.7 Defect Repair...	46
9.8 Security Function Verification...	46
9.9 Integrity of Software, Firmware and Information...	46
10 Emergency Response and Disaster Preparation...	47
10.1 Strategies and Procedures...	47
10.2 Event Handling Plan...	47
10.3 Event Handling...	47
10.4 Event Report...	48
10.5 Event Handling Support...	48
10.6 Security Alarm...	48
10.7 Error Handling...	49
10.8 Emergency Response Plan...	49
10.9 Emergency Training...	50

10.10 Emergency Drilling...	50
10.11 Information System Backup...	50
10.12 Supporting the Service Continuity Plan of the Customer...	51
10.13 Telecommunication Service...	51
11 Audit...	51
11.1 Strategies and Procedures...	51
11.2 Auditable Event...	52
11.3 Audit Record Contents...	52
11.4 Storage Capacity of Audit Record...	52
11.5 Response upon Audit Process Failure...	53
11.6 Examination, Analysis and Report of Audit...	53
11.7 Audit Treatment and Report Generation...	53
11.8 Time Stamp...	54
11.9 Audit Information Protection...	54
11.10 Non-repudiation...	54
11.11 Audit Record Retention...	54
12 Risk Assessment and Persistent Monitoring...	54
12.1 Strategies and Procedures...	54
12.2 Risk Assessment...	55
12.3 Vulnerability Scanning...	55
12.4 Persistent Monitoring...	56
12.5 Information System Monitoring...	56
12.6 Junk Information Monitoring...	57
13 Security Organization and Personnel...	57
13.1 Strategies and Procedures...	57
13.2 Security Organization...	58
13.3 Security Resource...	58
13.4 Security Regulations System...	58
13.5 Post Risks and Responsibilities...	59
13.6 Personnel Screening...	59
13.7 Personnel resignation...	59
13.8 Personnel Deployment...	60
13.9 Access Protocol...	60
13.10 Third Party Personnel Security...	60
13.11 Personnel Punishment...	61