

SINGAPORE STANDARD  
**Specification for multi-tiered cloud computing  
security**

~~Incorporating Corrigendum No. 1~~

Published by



Enterprise  
Singapore

**SS 584 : ~~2015+C1:2016~~2020**

(ICS 35.020; 35.040; 35.240.01)

---

SINGAPORE STANDARD

**Specification for multi-tiered cloud  
computing security**

---

~~All rights reserved. Unless otherwise specified, no part of this Singapore Standard may be reproduced or utilised in any form or by any means, electronic or mechanical, including photocopying and microfilming, without permission in writing from Enterprise Singapore. Request for permission can be sent to: [standards@enterprisesg.gov.sg](mailto:standards@enterprisesg.gov.sg).~~

Published by Enterprise Singapore

All rights reserved. Unless otherwise specified, no part of this Singapore Standard may be reproduced or utilised in any form or by any means, electronic or mechanical, including photocopying and microfilming, without permission in writing from Enterprise Singapore. Request for permission can be sent to: [standards@enterprisesg.gov.sg](mailto:standards@enterprisesg.gov.sg).

© Enterprise Singapore 2020

ISBN 978-981-~~4726-00-9~~49-2515-0

~~This~~The content of this Singapore Standard was approved on 4 September 2020 by the Information Technology Standards Committee (ITSC) ~~on behalf~~ under the purview of the Singapore Standards Council ~~of Singapore on 31 July 2015~~.

First published, 2013  
 First revision, 2015  
 Second revision, 2020

The ITSC, ~~appointed by the Standards Council~~, consists of the following members:

	<b>Name</b>	<b>Representation</b>
<b>Chairman</b>	: Mr Chak Kong Soon	<i>Individual Capacity</i>
<b>Deputy Chairman</b>	: Mr Harish Pillay	<i>Individual Capacity</i>
<b>Advisor</b>	: Mr Yap Chee Yuen	<i>Individual Capacity</i>
<b>Secretary</b>	: Mr Tao Yao Sing	<i>Infocomm Media Development Authority of Singapore</i>
<b>Members</b>	: Assoc Prof Benjamin Gan	<i>Singapore Management University</i>
	Mr Hong Tse Min	<i>Infocomm Media Development Authority of Singapore</i>
	Assoc Prof Huang Zhiyong	<i>National University of Singapore</i>
	Prof Li Xiaoli	<i>Institute for Infocomm Research</i>
	Mr Sam Liew	<i>Singapore Computer Society</i>
	Ms Lim Bee Kwan	<i>Government Technology Agency</i>
	Mr Lim Soon Chia	<i>Cyber Security Agency</i>
	Mr Kelvin Ng	<i>Nanyang Polytechnic</i>
	Mr Ong Hian Leong	<i>Individual Capacity</i>
Mr Andy Sim	<i>SGTech</i>	

	<b>Name</b>	<b>Capacity</b>
Chairman	∴ Mr Yap Chee Yuen	<del>Member, Standards Council</del>
Deputy Chairman	∴ Mr Chak Kong Soon	<del>Singapore Computer Society</del>
Secretary	∴ Ms Ho Buay Qui	<del>Infocomm Development Authority of Singapore</del>
Members	∴ Assoc Prof Chan Mun Choon	<del>National University of Singapore</del>
	Mr Cheong Tak Leong	<del>SPRING Singapore</del>
	Mr Robert Chew	<del>Individual Capacity</del>
	Assoc Prof Benjamin Gan	<del>Singapore Management University</del>
	Dr Derek Kiong	<del>Individual Capacity</del>
	Mr Karl Kwan	<del>Singapore Polytechnic</del>
	Mr Lee Kee Siang	<del>Information Technology Management Association</del>
	Mr Kelvin Ng	<del>Nanyang Polytechnic</del>
	Mr Patrick Pang	<del>National Research Foundation</del>
	Mr Harish Pillay	<del>Internet Society (Singapore Chapter)</del>
	Mr Victor Tan	<del>Defence Science Technology Agency</del>
	Prof Tham Jo Yew	<del>Institute for Infocomm Research</del>
	Mr Thomas Ting	<del>Association of Small and Medium Enterprises</del>
	Mr Yow Tau Keon	<del>Singapore Infocomm Technology Federation</del>

	<b>Name</b>	<b>Capacity</b>
<b>Chairman</b>	∴ Mr Robert Chew	<del>Member, Standards Council</del>
<b>Secretary</b>	∴ Ms Ho Buay Qui	<del>Infocomm Development Authority of Singapore</del>
<b>Members</b>	∴ Ms Suria R Asai	<del>Institute of Systems Science</del>
	Dr Calvin Chan	<del>SIM University</del>
	Mr Chan Kin Chong	<del>Chairman, Security and Privacy Standards</del>
	Mr Francis Fan	<del>Integrated Health Information Systems Pte Ltd</del>
	Mr Kwa Kim Chiong	<del>Information Technology Management Association</del>
	Dr Lee Hing Yan	<del>Infocomm Development Authority of Singapore</del>
	Mr James Lee	<del>Information Technology Management Association</del>
	Mr Kelvin Ng	<del>Member, ITSG</del>
	Ms Ng Lay Ngan	<del>Chairman, IT Governance Technical Committee</del>
	Mr Harish Pillay	<del>Member, ITSG</del>

The ITSC set up the Technical Committee on Cloud Computing Standards ~~Coordinating Task Force, appointed by the ITSC and responsible for~~ to oversee the preparation of this standard. The Technical Committee consists of ~~representatives from~~ the following ~~organisations~~ members:

	<b>Name</b>	<b>Capacity</b>
<b>Chairman</b>	: Mr Robert Chew	<i>Individual Capacity</i>
<del><b>Members</b></del> <b>Secretary</b>	: Mr <del>Hammad Rajjoub</del> Steven Tan	<i>Infocomm Media Development Authority of Singapore</i> <del><i>Infocomm Technology Federation</i></del>
<b>Members</b>	: Dr Anton Ravindran	<i>Singapore Computer Society</i>
	Mr <del>Martin Yates</del> Chan Kin Chong	<i>Individual Capacity</i>
	Dr Calvin Chan Meng Lai	<i>Singapore University of Social Sciences</i>
	Mr Chew Weiqiang	<i>Accenture</i>
	Mr Hammad Rajjoub	<i>Individual Capacity</i>
	Dr Kang Meng Chow	<i>SGTech</i>
	Dr Ryan Ko	<i>Individual Capacity</i>
	Mr Kwa Kim Chiong	<i>Information Technology Management Association</i>
	: Mr James Loo	<i>Information Technology Management Association</i>
	Mr Kelvin Ng	<i>Nanyang Polytechnic</i>
	Ms Ng Lay Ngan	<i>Institute of Systems Science</i>
	Mr Harish Pillay	<i>Individual Capacity</i>
	Mr Raju Chellam	<i>SGTech</i>
	Dr Suria P Asai	<i>Institute of Systems Science</i>
	Mr Tao Yao Sing	<i>Infocomm Media Development Authority of Singapore</i>
	Mr Wong Onn Chee	<i>Resolvo Systems</i>
	Mr Martin Yates	<i>Singapore Computer Society</i>

The ~~Multi-tiered Cloud Security Working Group, appointed by the Cloud Computing Standards Coordinating Task Force to assist in the preparation of this standard, comprises the following experts who contribute in their individual capacity:~~

<del><b>Convener</b></del>	<del>Dr Kang Meng Chow</del> <del>Dr Suria P Asai</del>	<del>Institute of Systems Science</del>
	<del>Mr Tao Yao Sing</del>	<del>Infocomm Media Development Authority of Singapore</del>
	<del>Mr Wong Onn Chee</del>	<del>Resolvo Systems</del>
	<del>Mr Martin Yates</del>	<del>Singapore Computer Society</del>

The Technical Committee set up the Multi-tiered Cloud Security Working Group to prepare this standard. The Working Group consists of the following experts who contribute in their individual capacity:

	Name
Convenor	: Dr Kang Meng Chow
Deputy Convenor	: Mr Lim Soon Chia
Members	: Dr Anton Ravindran Mr Mandar Bale Dr Ken Baylor Mr Chai Chin Loon Mr Chan Meng Fai Mr Dave Cheng Mr Chetan Sansare Mr Chong Jian Yi Mr Patrick Choong Wee Meng Ms Dhana Lakshmi Mr Gajun Ganendran Mr Hong Jian Hui Mr Lucas Kauffman Mr Richard Koh Prof Lam Kwok Yan Dr Lee Hing Yan Ms Lim May Ann Mr Loh Chee Keong Mr Manoj Wadhwa Mr Mok Boon Poh Mr Chris Ng Khee Soon Mr Raju Chellam Mr Sanjeev Gupta Mr Andrew Seit Mr Sim Bak Chor Mr Suresh Agarwal Mr Tao Yao Sing Ms Irene Wang Mr Wong Onn Chee Mr Xiang Bin Mr Zhuang Haojie

The organisations in which the experts of the Working Group are involved are:

~~Cisco Systems, INC~~

AliCloud

Amazon Web Services

Asia Cloud Computing Association

Association of Information Security Professionals

BSI Group Singapore Pte. Ltd.

Certification Partner Global

Cloud Security Alliance APAC

Cyber Security Agency

Ernst & Young CertifyPoint B.V.

Google Cloud

Government Technology Agency

IBM Softlayer Cloud

Infocomm Media Development Authority of Singapore

~~MOH Holdings Pte Ltd PrivyLink~~Microsoft Cloud Services

Salesforce.com

SCS Cloud Chapter

SGTech, Cloud and Data Chapter

Singapore Chinese Chamber of Commerce and Industry

SOCOTEC Certification Singapore

TÜV SÜD PSB Pte Ltd

~~Resolve Systems Pte Ltd~~

(blank page)



## Contents

	<b>Page</b>
Foreword .....	10
0 Introduction .....	11
0.1 General.....	11
0.2 Cloud computing risks.....	11
0.3 Structure.....	14
0.4 Framework.....	16
0.5 Alignment of user requirements to CSP level .....	16
1 Scope.....	19
1.1 General.....	19
1.2 Exclusions .....	19
1.3 Audience .....	19
1.4 Certification .....	19
2 Normative references .....	20
<del>3 Definitions and abbreviated terms .....</del>	<del>19</del>
<del>3.1 Definitions.....</del>	<del>19</del>
<del>3.2 Abbreviated terms.....</del>	<del>22</del>
3 Terms, definitions and abbreviations .....	20
3.1 Terms and definitions .....	20
3.2 Abbreviations.....	23
4 Cloud computing fundamentals .....	24
4.1 Cloud computing characteristics .....	24
4.2 Cloud computing service models.....	24
4.3 Cloud computing deployment models.....	25
5 Other considerations .....	25
5.1 Applicability and compensatory controls.....	25
5.2 Cloud service provider disclosure .....	26
5.3 Considerations of emerging technologies.....	26
6 Information security management.....	28
6.1 Information security management controls .....	28
6.2 Information security management system (ISMS) .....	28
6.23 Management of information security .....	30
6.34 Management oversight of information security .....	31
6.45 Information security policy .....	33
6.56 Review of information security policy .....	34

6.67	Information security audits .....	35
6.78	Information security liaisons (ISL) .....	36
6.89	Acceptable usage .....	37
7	Human resources .....	38
7.1	Human resources security controls .....	38
7.2	Background screening .....	38
7.23	Continuous personnel evaluation .....	39
7.34	Employment and contract terms and conditions .....	40
7.4	<del>Disciplinary process .....</del>	<del>36</del>
7.5	<del>Asset returns .....</del>	<del>37</del>
7.6	<del>Information security training and awareness .....</del>	<del>37</del>
8	<del>Risk management .....</del>	<del>39</del>
8.1	<del>Risk management programme .....</del>	<del>39</del>
8.2	<del>Risk assessment .....</del>	<del>40</del>
8.3	<del>Risk management .....</del>	<del>41</del>
8.4	<del>Risk register .....</del>	<del>42</del>
9	<del>Third-party .....</del>	<del>43</del>
9.1	<del>Third party due diligence .....</del>	<del>43</del>
9.2	<del>Identification of risks related to third parties .....</del>	<del>44</del>
9.3	<del>Third party agreement .....</del>	<del>45</del>
9.4	<del>Third party delivery management .....</del>	<del>46</del>
7.5	Disciplinary process .....	42
7.6	Asset returns .....	42
7.7	Information security training and awareness .....	43
8	Risk management .....	45
8.1	Risk management controls .....	45
8.2	Risk management programme .....	45
8.3	Risk assessment .....	47
8.4	Risk management .....	48
8.5	Risk register .....	49
9	Third-party .....	50
9.1	Third-party security controls .....	50
9.2	Third-party due diligence .....	50
9.3	Identification of risks related to third parties .....	51
9.4	Third-party agreement .....	52
9.5	Third-party delivery management .....	53

10	Legal and compliance .....	55
10.1	Legal and compliance controls.....	55
10.2	Compliance with regulatory and contractual requirements.....	56
10.23	Compliance with policies and standards.....	57
10.34	Prevention of misuse of cloud facilities .....	58
10.45	Use of compliant cryptography cryptographic controls.....	59
10.56	Third-party compliance .....	60
10.67	Continuous compliance monitoring.....	60
11	Incident management .....	62
11.1	Incident management controls .....	62
11.2	Information security incident response plan and procedures .....	62
11.23	Information security incident response plan testing and updates.....	65
11.34	Information security incident reporting .....	66
11.45	Problem management.....	66
12	Data governance .....	67
12.1	Data governance controls .....	67
12.2	Data classification.....	68
12.23	Data ownership.....	68
12.34	Data integrity .....	69
12.45	Data labelling/handling.....	70
12.56	Data protection .....	70
12.67	Data retention .....	72
12.78	Data backups.....	73
12.89	Secure disposal and decommissioning of hardcopy, media and equipment.....	74
12.9	Secure disposal verification of live instances and backups .....	75
12.10		
12.10	<del>Tracking of data.....</del>	<del>76</del>
12.11	<del>Production data .....</del>	<del>76</del>
12.11	Tracking of data.....	76
12.12	Production data .....	76
13	Audit logging and monitoring .....	77
13.1	Audit logging and monitoring controls .....	77
13.2	Logging and monitoring process .....	77
13.23	Log review .....	79
13.34	Audit trails .....	80
13.45	Backup and retention of audit trails.....	81
13.56	Usage logs .....	82

14	Secure configuration .....	83
14.1	Secure configuration controls.....	83
14.2	Server and network device configuration standards .....	83
14.23	Malicious code prevention.....	84
14.34	Portable code .....	85
14.45	Physical port protection .....	86
14.56	Restrictions to system utilities.....	87
14.67	System and network session management .....	87
14.78	Unnecessary services and protocols.....	88
14.89	Unauthorised software .....	89
14.9	Enforcement checks .....	89
14.10		
15	Security testing and monitoring .....	90
15.1	Security testing and monitoring controls.....	90
15.2	Vulnerability scanning.....	91
15.23	Penetration testing.....	92
15.34	Security monitoring .....	92
16	System acquisitions and development.....	94
16.1	System acquisitions and development security controls.....	94
16.2	Development, acquisition and release management.....	94
16.23	Web application security .....	96
16.34	System testing .....	96
16.45	Source code security .....	97
16.56	Outsourced software development.....	98
17	Encryption.....	99
17.1	Encryption and secure cryptographic key management.....	99
17.2	Encryption policies and procedures.....	99
17.23	Channel encryption.....	100
17.34	Key management.....	101
17.45	Electronic messaging security.....	102
18	Physical and environmental.....	103
18.1	Physical and environmental security controls.....	103
18.2	Asset management .....	103
18.23	Off-site movement .....	104
18.34	Physical access .....	105
18.45	Visitors .....	106
18.56	Environmental threats and equipment power failures .....	107
18.67	Physical security review.....	109

19	Operations .....	109
19.1	Operations security controls.....	109
19.2	Operations management policies and procedures.....	110
19.23	Documentation of service operations and external dependencies .....	110
19.34	Capacity management .....	111
19.45	Service levels .....	112
19.56	Reliability and resiliency .....	113
19.67	Recoverability .....	114
20	Change management .....	115
20.1	Change management controls .....	115
20.2	Change management process.....	115
20.23	Backup procedures .....	116
20.34	Back-out or rollback procedures.....	117
20.45	Separation of environment.....	118
20.56	Patch management procedures.....	118
21	Business continuity planning (BCP) and disaster recovery (DR).....	119
21.1	BCP and DR controls.....	119
21.2	BCP framework.....	119
21.23	BCP and DR plans.....	120
21.34	BCP and DR testing.....	122
22	Cloud services administration.....	123
22.1	Cloud services administration controls .....	123
22.2	Privilege account creation.....	123
22.23	Generation of administrator passwords .....	124
22.34	Administrator access review and revocation.....	125
22.45	Account lockout .....	126
22.56	Password change .....	127
22.67	Password reset and first logon.....	128
22.78	Administrator access security .....	129
22.89	Administrator access logs .....	130
<del>22.9</del>	Session management .....	131
22.10		
<del>22.10</del>	Segregation of duties.....	132
22.11		
<del>22.11</del>	Secure transmission of access credentials.....	133
22.12		
<del>22.12</del>	Third party administrative access.....	134
22.13		
<del>22.13</del>	Service and application accounts.....	135
22.14		

23	Cloud user access.....	137
23.1	Cloud user access controls.....	137
23.2	User access registration .....	137
23.23	User access security.....	138
23.34	User access password.....	139
23.45	User account lockout .....	140
23.56	User password reset and first logon change .....	141
23.67	Password protection .....	142
23.78	User session management.....	142
23.89	Change of cloud user's administrator details notification.....	144
<del>23.9</del>	<del>Self-service portal creation and management of user accounts.....</del>	<del>144</del>
23.10		
<del>23.10</del>	<del>Communication with cloud users.....</del>	<del>145</del>
23.11		
24	Tenancy and customer isolation .....	146
24.1	Tenancy and customer isolation controls .....	146
24.2	Multi tenancy .....	146
24.23	Supporting infrastructure segmentation.....	147
24.34	Network protection.....	149
24.45	Virtualisation .....	151
24.56	Storage area networks (SAN) .....	153
24.67	Data segregation .....	154
<del>Annex A (normative)</del>	<del>Cloud service provider disclosure .....</del>	<del>131</del>
<del>Annex B (informative)</del>	<del>Implementation guidelines for cloud users .....</del>	<del>142</del>
<del>Annex C (informative)</del>	<del>Implementation guidelines for cloud service providers .....</del>	<del>150</del>
Annex A	.....	156
Annex B	.....	171
Bibliography	.....	180

## Foreword

This Singapore Standard was prepared by the Multi-Tiered Cloud Security Working Group ~~of set up~~ by the Cloud Computing Standards ~~Coordinating Task Force under the direction of the Information Technology Standards~~ Technical Committee ~~(under the purview of ITSC).~~

Cloud computing shifts away from conventional hosting and delivery of services, to utility-based consumption in both the enterprise and personal space, enabling 'everything-as-a-service'. In the midst of a cloud environment, the traditional IT security models are no longer adequate. An example would be perimeter security which has been appropriate for conventional on-premise IT systems but is often inadequate for the cloud. The cloud environment shifts the ownership of security to a shared responsibility model. An example would be physical security controls of data centres, which would traditionally be operated and managed by an organisation, whereas for a cloud ~~User~~service customer (CSC), these controls now become the responsibility of the Cloud Service Provider (CSP).

This Singapore Standard aims to foster and encourage the adoption of sound risk management and security practices for cloud computing, by providing relevant cloud computing security practices and controls for cloud ~~users~~service customers, auditors and certifiers to understand cloud security requirements, and for public Cloud Service Providers to strengthen and demonstrate the cloud security controls in place, in their cloud environments.

~~Acknowledgement is~~In preparing this standard, reference was made ~~for~~to the ~~use of information from~~following publications:

- Special Publication 800-145, The National Institute of Standards and Technology (NIST) Definition of Cloud Computing – Recommendation of the National Institute of Standards and Technology, September 2011 on which Clause 4 is based;
- Special Publication 800-100, Information Security Handbook: A Guide for Managers, October 2006 on which Clause 3.12 is based;
- Special Publication 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organisations, Building Effective Security Assessment Plans, June 2010 on which Clauses 3.14, 3.16 and 3.19 are based;
- Special Publication 800-60 Volume I Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008 on which Tables 4 and 5 are based;
- ~~TR31:2012 Technical Reference for Security and Service Level Guidelines for the Usage of Public Cloud Computing Services.~~
- SS ISO/IEC 21878:2019 Information technology – Security techniques – Security guidelines for design and implementation of virtualised servers.

Attention is drawn to the possibility that some of the elements of this Singapore Standard may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

**NOTES**

1. ~~Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions. Where SSs are deemed to be stable, i.e. no foreseeable changes in them, they will be classified as "Mature Standards". Mature Standards will not be subject to further review, unless there are requests to review such standards.~~
2. ~~An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore and the Singapore Standards Council shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR. Although care has been taken to draft this standard, users are also advised to ensure that they apply the information after due diligence.~~
3. ~~Compliance with a SS or TR does not exempt users from any legal obligations.~~

**NOTES**

1. Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions. Where SSs are deemed to be stable, i.e. no foreseeable changes in them, they will be classified as "Mature Standards". Mature Standards will not be subject to further review, unless there are requests to review such standards.
2. An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore and the Singapore Standards Council shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR. Although care has been taken to draft this standard, users are also advised to ensure that they apply the information after due diligence.
3. Compliance with a SS or TR does not exempt users from any legal obligations.