ISO/IEC 19086-4:2019 (E)

Cloud computing — Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Symbols and abbreviated terms

5 Relationship with other parts of the cloud computing SLA framework

5.1 General
5.2 Conformance

6 Overview

6.1 General
6.2 Structure of this document

7 Information security components

7.1 Information security policy component
7.1.1 Description
7.1.2 Cloud service qualitative objectives
7.1.3 Guidance
7.2 Organization of information security component
7.2.1 Description
7.2.2 Cloud service qualitative objectives
7.2.3 Guidance
7.3 Asset management component
7.3.1 Description
7.3.2 Cloud service level objectives
7.3.3 Cloud service qualitative objectives
7.3.4 Guidance
7.4 Access control component
7.4.1 Description
7.4.2 Cloud service level objectives
7.4.2.1 Maximum time required to revoke user access
7.4.2.2 Time required to revoke user access at a specified commitment level
7.4.3 Cloud service qualitative objectives
7.4.3.1 User registration and de-registration
7.4.3.2 Review access patterns
7.4.3.3 Authentication mechanism
7.4.3.4 Third-party authentication support
7.4.3.5 Strong authentication support
7.4.3.6 Anonymous and pseudonymous authentication support
7.4.4 Guidance
7.5 Cryptography component
7.5.1 Description
7.5.2 Cloud service qualitative objectives
7.5.2.1 Cryptographic controls for data in motion
7.5.2.2 Cryptographic controls for data at rest
7.5.2.3 Cryptographic controls for data during execution

7.5.2.4 Key management policy
7.5.3 Guidance
7.6 Physical and environmental security component
7.6.1 Description
7.6.2 Cloud service qualitative objectives
7.6.2.1 Data centre monitoring
7.6.2.2 Secure disposal and re-use of equipment
7.6.2.3 Facilities authorization
7.6.3 Guidance
7.7 Operations security component
7.7.1 Description
7.7.2 Cloud service level objectives
7.7.2.1 Vulnerability reporting interval
7.7.2.2 Period of time of logs availability
7.7.3 Cloud service qualitative objectives
7.7.3.1 Malware protection
7.7.3.2 Logging and monitoring
7.7.3.3 Vulnerability management
7.7.3.4 Vulnerability notification method
7.7.3.5 Vulnerability impact statement
7.7.4 Guidance
7.8 Communications security component
7.8.1 Description
7.8.2 Cloud service qualitative objectives
7.8.3 Guidance
7.9 Systems acquisition, development and maintenance component
7.9.1 Description
7.9.2 Cloud service qualitative objectives
7.9.2.1 System acquisition procedures
7.9.2.2 Secure development procedures
7.9.2.3 Maintenance procedures
7.9.3 Guidance
7.10 Supplier relationships component
7.10.1 Description
7.10.2 Cloud service qualitative objectives
7.10.3 Guidance
7.11 Information security incident management component
7.11.1 Description
7.11.2 Cloud service level objectives
7.11.3 Cloud service qualitative objectives
7.11.4 Guidance
7.12 Business continuity management component
7.12.1 Description
7.12.2 Cloud service qualitative objectives
7.12.3 Guidance
7.13 Compliance component
7.13.1 Description
7.13.2 Cloud service qualitative objectives
7.13.3 Guidance

8 Protection of personally identifiable information component

8.1 Consent and choice component
8.1.1 Description
8.1.2 Cloud service qualitative objectives
8.1.3 Guidance
8.2 Purpose legitimacy and specification component
8.2.1 Description
8.2.2 Cloud service qualitative objectives
8.2.2.1 Purpose legitimacy
8.2.2.2 Third-party access list
8.2.3 Guidance
8.3 Data minimization component
8.3.1 Description
8.3.2 Cloud service level objectives

8.3.3 Cloud service qualitative objectives
8.3.3.1 Minimize stakeholder access
8.3.3.2 Data minimization cryptographic controls
8.3.4 Guidance
8.4 Use, retention and disclosure limitation component
8.4.1 Description
8.4.2 Cloud service qualitative objectives
8.4.3 Guidance
8.5 Accuracy and quality component
8.5.1 Description
8.5.2 Cloud service qualitative objectives
8.5.3 Guidance
8.6 Openness, transparency and notice component
8.6.1 Description
8.6.2 Cloud service qualitative objectives
8.6.2.1 PII subcontractor list
8.6.2.2 Requirement for specific consent
8.6.3 Guidance
8.7 Individual participation and access component
8.7.1 Description
8.7.2 Cloud service qualitative objectives
8.7.2.1 PII subject participation and access
8.7.2.2 PII principal access capabilities
8.7.3 Guidance
8.8 Accountability component
8.8.1 Description
8.8.2 Cloud service level objectives
8.8.3 Cloud service qualitative objectives
8.8.3.1 Notification of data breach
8.8.3.2 PII disposal policy
8.8.4 Guidance
8.9 Protection of PII compliance component
8.9.1 Description
8.9.2 Cloud service qualitative objectives
8.9.3 Guidance

Page count: 20