ISO/IEC 27018 Introduction
ISO/IEC 27017 Update

Dale Johnstone

26 January 2015

INTERNATIONAL STANDARD

ISO/IEC 27018

First edition
2014-08-01

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

Reference number
ISO/IEC 27018:2014(E)

ISO/IEC DIS 27017

Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Edition: 1 (Monolingual)	**ICS:** 35.040
Status: Under development	**Stage:** 40.00 (2014-11-18)
TC/SC: ISO/IEC JTC 1/SC 27	**Number of Pages:**
Target publication date: 2015-10-31	

ISO/IEC 27018 – Introduction

- Published 1st August 2014
- Applicable to public cloud computing organizations acting as **PII processors**
- Provides Guidelines (should) based on ISO/IEC 27002
- Establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII)
- Used in accordance with the privacy principles in ISO/IEC 29100
- Considers regulatory requirements for the protection of PII which might be applicable within the context of the information security risk environment
- May also be relevant to organizations acting as **PII controllers**
- Not intended to cover additional obligations that **PII controllers** may be subject to (i.e. additional PII protection legislation, regulations and obligations)

ISO/IEC 27018 – Overview

Provides a **Code of Practice** to:

- Process personal information (PI) in accordance with the customer's instructions
- Process PI for marketing or advertising purposes with the customer's express consent – such consent cannot be made a condition for receiving service
- Assist to comply when individuals assert their access rights
- Disclose information to law enforcement authorities only when legally bound to do so
- Disclose names of any sub-processors and the possible locations where personal information may be processed prior to entering into a cloud services contract
- Assist cloud customers comply with notification obligations in event of a data breach
- Implement a policy for the return, transfer or disposal of personal data, i.e. when service comes to an end
- Subject their services to independent information security reviews at scheduled intervals (or when significant processing changes occur)
- Enter into confidentiality agreements with staff who have access to personal data and provide appropriate staff training

http://www.natlawreview.com/article/iso-s-new-cloud-privacy-standard-international-standards-organization

ISO/IEC 27018 – 27002 Alignment

5 Information security policies

5.1 Management direction for information security

The objective specified in clause 5.1 of ISO/IEC 27002 applies.

5.1.1 Policies for information security

Control 5.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Public cloud PII protection implementation guidance

The information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers).

Contractual agreements should clearly allocate responsibilities between the public cloud PII processor, its sub-contractors and the cloud service customer, taking into account the type of cloud service in question (e.g., a service of an IaaS, PaaS or SaaS category of the cloud computing reference architecture). For example, the allocation of responsibility for application layer controls may differ depending on whether the public cloud PII processor is providing a SaaS service or rather is providing a PaaS or IaaS service upon which the cloud service customer can build or layer its own applications.

Other information for public cloud PII protection

In some jurisdictions the public cloud PII processor is directly subject to PII protection legislation. Elsewhere, PII protection legislation applies to the PII controller only.

A mechanism to ensure the public cloud PII processor is obliged to support and manage compliance is provided by the contract between the cloud service customer and the public cloud PII processor. The contract could call for independently audited compliance, acceptable to the cloud service customer, e.g., via the implementation of the relevant controls in this International Standard and in ISO/IEC 27002.

ISO/IEC 27018 – 27002 Alignment

Annex A
(normative)

Public cloud PII processor extended control set for PII protection

This annex specifies new controls and associated implementation guidance which, in combination with the augmented controls and guidance in ISO/IEC 27002 (see clauses 5 to 18), make up an extended control set to meet the requirements for PII protection which apply to public cloud service providers acting as PII processors.

These additional controls are classified according to the eleven privacy principles of ISO/IEC 29100. In many cases the controls could be classified under more than one of the privacy principles. In such cases they are classified under the most relevant principle.

A.1 Consent and choice

A.1.1 Obligation to co-operate regarding PII principals' rights

Control

The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.

ISO/IEC 27018 – 27002 Alignment

Clause	Title	Objective Applies	Contents Apply	Implement Guidance	Other Information	Sector-Specific Guidance
5	Information security policies					
5.1	Management direction for information security	YES				
5.1.1	Policies for information security			YES	YES	YES
5.1.2	Review of the policies for information security			YES		
6	Organization of information security					
6.1	Internal organization	YES				
6.1.1	Information security roles and responsibilities			YES	YES	YES
6.1.2	Segregation of duties			YES	YES	
6.1.3	Contact with authorities			YES	YES	
6.1.4	Contact with special interest groups			YES	YES	
6.1.5	Information security in project management			YES		
6.2	Mobile devices and teleworking	YES	YES			
7	Human resource security					
7.1	Prior to employment	YES	YES			
7.2	During employment	YES				
7.2.1	Management responsibilities			YES	YES	
7.2.2	Information security awareness, education and training			YES	YES	YES
7.2.3	Disciplinary process			YES	YES	
7.3	Termination and change of employment	YES	YES			
8	Asset management	YES	YES			
9	Access control					
9.1	Business requirements of access control	YES	YES			
9.2	User access management	YES				YES
9.2.1	User registration and de-registration			YES	YES	YES
9.2.2	User access provisioning			YES	YES	
9.2.3	Management of privileged access rights			YES	YES	
9.2.4	Management of secret authentication information of users			YES	YES	
9.2.5	Review of user access rights			YES	YES	
9.2.6	Removal or adjustment of access rights			YES	YES	
9.3	User responsibilities	YES				
9.3.1	Use of secret authentication information			YES		
9.4	System and application access control	YES				
9.4.1	Information access restriction			YES		
9.4.2	Secure log-on procedures			YES	YES	YES
9.4.3	Password management system			YES	YES	
9.4.4	Use of privileged utility programs			YES	YES	
9.4.5	Access control to program source code			YES	YES	

ISO/IEC 27018 – 27002 Alignment

Clause	Title	Objective Applies	Contents Apply	Implement Guidance	Other Information	Sector-Specific Guidance
10	Cryptography					
10.1	Cryptographic controls	YES				
10.1.1	Policy on the use of cryptographic controls			YES	YES	YES
10.1.2	Key management			YES	YES	
11	Physical and environmental security					
11.1	Secure areas	YES	YES			
11.2	Equipment	YES				
11.2.1	Equipment siting and protection			YES		
11.2.2	Supporting utilities			YES	YES	
11.2.3	Cabling security			YES		
11.2.4	Equipment maintenance			YES		
11.2.5	Removal of assets			YES	YES	
11.2.6	Security of equipment and assets off-premises			YES	YES	
11.2.7	Secure disposal or re-use of equipment			YES	YES	YES
11.2.8	Unattended user equipment			YES		
11.2.9	Clear desk and clear screen policy			YES	YES	
12	Operations security					
12.1	Operational procedures and responsibilities	YES				
12.1.1	Documented operating procedures			YES		
12.1.2	Change management			YES	YES	
12.1.3	Capacity management			YES	YES	
12.1.4	Separation of development, testing and operational environments			YES	YES	YES
12.2	Protection from malware	YES	YES			
12.3	Backup	YES				
12.3.1	Information backup			YES		YES
12.4	Logging and monitoring	YES				
12.4.1	Event logging			YES	YES	YES
12.4.2	Protection of log information			YES	YES	YES
12.4.3	Administrator and operator logs			YES	YES	
12.4.4	Clock synchronization			YES	YES	
12.5	Control of operational software	YES	YES			
12.6	Technical vulnerability management	YES	YES			
12.7	Information systems audit considerations	YES	YES			
13	Communications security					
13.1	Network security management	YES	YES			
13.2	Information transfer	YES				
13.2.1	Information transfer policies and procedures			YES	YES	YES
13.2.2	Agreements on information transfer			YES	YES	
13.2.3	Electronic messaging			YES	YES	
13.2.4	Confidentiality or non-disclosure agreements			YES	YES	

ISO/IEC 27018 – 27002 Alignment

Clause	Title	Objective Applies	Contents Apply	Implement Guidance	Other Information	Sector-Specific Guidance
14	System acquisition, development and maintenance	YES	YES			
15	Supplier relationships	YES	YES			
16	Information security incident management					
16.1	Management of information security incidents and improvements	YES				YES
16.1.1	Responsibilities and procedures			YES	YES	YES
16.1.2	Reporting information security events			YES	YES	
16.1.3	Reporting information security weaknesses			YES	YES	
16.1.4	Assessment of and decision on information security events			YES		
16.1.5	Response to information security incidents			YES	YES	
16.1.6	Learning from information security incidents			YES	YES	
16.1.7	Collection of evidence			YES	YES	
17	Information security aspects of business continuity management	YES	YES			
18	Compliance					
18.1	Compliance with legal and contractual requirements	YES	YES			
18.2	Information security reviews	YES				
18.2.1	Independent review of information security			YES	YES	YES
18.2.2	Compliance with security policies and standards			YES	YES	
18.2.3	Technical compliance review			YES	YES	
	ANNEX A					

ISO/IEC 27018 – Extended Controls

ISO/IEC 27018 – **Public cloud PII processor** should:

- (x 19)
- provide the **cloud service customer** with the means to enable them to fulfil their obligation to facilitate the exercise of **PII principal**s' rights to access, correct and/or erase PII pertaining to them
- provide the **cloud service customer** with all relevant information, in a timely fashion
- adhere to the relevant privacy principles set forth in ISO/IEC 29100, where circumstances are determined by the **public cloud PII processor** that the processing method involves the collection and use of PII
- etc…

ISO/IEC 27018 – **Cloud service customer** should:

- (x 4)
- ensure the **public cloud PII processor**'s compliance with purpose specification and limitation principles
- ensure that no PII is processed by the **public cloud PII processor** or any of its sub-contractors for further purposes independent of the instructions of the **cloud service customer**
- ensure that the measures implemented by the **public cloud PII processor** meet its obligations

ISO/IEC 27018 –
PII should:

- (x 12)
- not be processed for any purpose independent of the instructions of the **cloud service customer**, where processed under a contract
- ensure express consent is not be a condition of receiving the service, where processed under a contract
- be recorded, including what PII has been disclosed, to whom and at what time, where disclosed to third parties

ISO/IEC 27018 – Contract should:

- (x 15)
- specify that sub-contractors only be commissioned on the basis of a consent that can generally be given by the **cloud service customer** at the beginning of the service
- specify how the **public cloud PII processor** will provide the information necessary for the **cloud service customer** to fulfil his obligation to notify relevant authorities
- define the maximum delay in notification of a data breach involving PII

ISO/IEC 27018 – Information should:

- (x 4)
- cover the fact that sub-contracting is used and the names of relevant subcontractors, but not any business-specific details, where disclosed
- include the countries in which sub-contractors process data and the means by which sub-contractors are obliged to meet or exceed the obligations of the **public cloud PII processor**, where disclosed
- under a non-disclosure agreement and/or on the request of the **cloud service customer**, where public disclosure of sub-contractor information is assessed to increase security risk beyond acceptable limits, where disclosed

ISO/IEC 27018 –
Other should:

- Policy (x2)
- Procedure (x2)
- Information (x4)
- Temporary files and documents (x1)
- Portable physical media and device (x1)
- Hardcopy material (x1)
- User Profiles (x4)
- Disclosures (x1)
- If > 1 individual has access to stored PII (x1)

INTERNATIONAL STANDARD

ISO/IEC 27018

First edition
2014-08-01

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

Reference number
ISO/IEC 27018:2014(E)

ISO/IEC DIS 27017

Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services

General information | Revisions | Corrigenda / Amendments

Edition: 1 (Monolingual)	**ICS:** 35.040
Status: Under development	**Stage:** 40.00 (2014-11-18)
TC/SC: ISO/IEC JTC 1/SC 27	**Number of Pages:**
Target publication date: 2015-10-31	

ISO/IEC 27017 – Update

- **Guidelines** for information security controls applicable to the **provision and use of cloud services**
- Additional **implementation guidance** for relevant controls specified in ISO/IEC 27002
- Additional c**ontrols with implementation guidance** that specifically relate to cloud services
- Provides controls and implementation guidance for both **cloud service providers** and **cloud service customers**
- Structured similar to ISO/IEC 27002
- Includes clauses 5 to 18 of ISO/IEC 27002 by stating the applicability of its texts at each clause and paragraph
- When objective with controls, or a is control needed in addition to ISO/IEC 27002, they are given in Annex A: Cloud Service Extended Control Set (normative)

ISO/IEC 27017 – 27002 Alignment

5.1 Management direction for information security

The objective specified in clause 5.1 of ISO/IEC 27002 applies.

5.1.1 Policies for information security

Control 5.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
An information security policy for cloud computing should be defined as a topic-specific policy of the cloud service customer. The cloud service customer's information security policy for cloud computing should be consistent with the organization's acceptable levels of information security risks for their information and other assets. When defining the information security policy for cloud computing, the cloud service customer should take the following into account: — information stored in the cloud computing environment may be subject to access and management by the cloud service provider; — assets may be maintained in the cloud computing environment, e.g. application programs; — processes may run on a multi-tenant, virtualized cloud service; — the cloud service customer's users of the cloud service;	The cloud service provider should augment its information security policy to address the provision and use of its cloud services taking the following into account: — the baseline information security requirements applicable to the design and implementation of the cloud service; — risks from authorised insiders; — multi-tenancy and customer isolation (including virtualisation); — access by cloud service provider administrators; — appropriate access control procedures, e.g. strong authentication for administrative access to hosted cloud services; — communications to customers during change management; — virtualisation security — access to and protection of cloud service

ISO/IEC 27017 – 27002 Alignment

— the cloud service customer's administrators with privileged access; — the geographical locations of the cloud service provider's organisation and the countries where the cloud service provider may store the cloud service customer data (even temporarily).	customer data; — lifecycle management of cloud service customer accounts; — communication of breaches and information sharing guidelines for aiding investigation and forensics.

Other information for cloud services

The information security policy for cloud computing of the cloud service customer is one of the topic-specific policies described in ISO/IEC 27002, 5.1.1. The information security policy of an organization deals with its information and business processes generally. In the case where the organization uses cloud services, it can have a policy for cloud computing as a cloud service customer. The information of the organization is stored and maintained in the cloud computing environment, and the business processes are also operated in the cloud computing environment. General information security requirements stated in the information security policy at the top level are followed by the policy for cloud computing.

In contrast to this, the information security policy for provisioning cloud services deals with the customers' information and business processes, not with the organization's own information and business processes. Information security requirements for provisioning the cloud service should meet those of the prospective customers, and therefore they are not necessarily consistent with information security requirements related to the information and business processes of the cloud service provider. Scope of the policy is often suitably defined in terms of service provisioning, but not solely by organizational structure or physical locations.

Virtualization security in cloud computing has several aspects, e.g., lifecycle management of VMs, storage and access controls for virtualized images, handling of dormant or offline VMs, snapshots, information security of hypervisors, and information security in the use of self-service portals.

5.1.2 Review of the policies for information security

Control 5.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

ISO/IEC 27017 – Extended Controls

ISO/IEC 27017 – Update

- Draft International Standard (DIS) Stage of the Development Lifecycle (January 2015)
- Next Meeting to Discuss DIS Voting and Comments Scheduled for 1st Week of May 2015
- Expected to be Finalised and Published as an International Standard in October 2015

Questions