Guidance Security Controls

SURF Framework of Legal Standards for (Cloud) Services, Appendix C

Utrecht, October 2016
Version number: 2.0

Credits

Guidance Security Controls
SURF Framework of Legal Standards for (Cloud) Services – Annex C

SURF
P.O. Box 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

SURF is the collaborative ICT organisation for higher education and research in the Netherlands.
This publication is available in digital format on the SURF website: www.surf.nl/publicaties

Introduction

SURF published the *SURF Framework of Legal Standards for (Cloud) Services* on 13 November 2013. It was updated in February 2016 for amendments after it had been in use for two years in order to meet new laws and regulations. The Processor Agreement – Annex A to the SURF Framework of Legal Standards for (Cloud) Services – obliges suppliers to take appropriate measures for the physical and logical security of the provided service.
The set of measures in this document is intended as a guide to make the concept of "appropriate security measures" more concrete. It is not a requirement; the same or a better effect may be achieved with other measures.

The suggested measures are classified into the following categories:

1. Policy and organisation
2. Access security
3. Anti-malware and technical vulnerabilities management
4. Data confidentiality, integrity and privacy
5. Monitoring and logging

Dutch Data Protection Act

The Dutch Data Protection Act (Wet Bescherming Persoonsgegevens or WBP) states that *appropriate organisational and technical security measures must be taken when processing personal data*[1]*. The measures are based on a risk analysis and cover risks to achieve reliability. As the required reliability and security level increase, the person responsible shall take a wider range of stricter security measures to cover the risks involved and effectively guarantee the required level of security*[2]. These measures also need to be taken if data processing is outsourced. This guide provides a number of measures to be met by the security of personal data processing depending on the risk class.

The measures are built around Article 3.2 of the Data Protection Authority's *Personal Data Security* guideline dated February 2013[3] (previously the Personal Data Protection Board). The guideline is also based on a risk analysis to make well-informed choices in terms of the security measures to be taken. A risk analysis and regular evaluations are recommended.

Article 3.2 of the Data Protection Authority's *Personal Data Security* guideline often refers to ISO 27002:2007, the code of practice for information security controls. However, not all measure categories are referred to. The tables on the following pages therefore only show a selection of measures – the measures regarding staff reliability are not included, for example – even though measures are also required in this respect depending on the risk category. The tables refer suppliers to the relevant articles in the standards for further information.

Change management measures have been added to the existing provisions of Article 3.2 of the above guideline. Change management is so essential to the availability, integrity and confidentiality of data processing that it was added to the set.

Availability of information systems is outside the scope of this guide's set of measures. The Framework of Legal Standards assumes that availability criteria are agreed in the Agreement or in a Service Level Agreement.

[1] Article 13 of the Data Protection Act (see http://wetten.overheid.nl/BWBR0011468/2016-01-01)

[2] The Personal Data Protection Authority's *Personal Data Security* Guideline, Art. 2.4

[3] https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf (consulted on 19 April 2016)

Specific measures for application controls are not included, because the required application controls very much depend on the service's type of application. It is recommended to include the required application controls in a set that describes the functional requirements. The OWASP[4] Top Ten is a powerful tool in the development and testing of web applications. The OWASP Top Ten *Most Critical Web Application Security Risks* provide the ten most common security problems in web applications. The OWASP Top 10 *Proactive Controls 2016* offer web application developers a list of techniques that should be applied in every application development project.

Appropriate security measures

The measures table shows the measures that are appropriate for processing a Low risk class (public level) and Normal risk class as defined in the Framework of Legal Standards. Measures applicable to the High risk class only are shown in red and are indicated as "HIGH" in the first column. In combination with the basic measures, these measures are considered appropriate for processing sensitive personal data (such as data on race, health and criminal records) and data that must be marked as very high risk for other reasons – the scale of the data processing, for example.

Relevant standards/documents

A number of standards and documents other than the Personal Data Protection Authority's *Personal Data Security guideline* were also consulted for this guide:

- NEN-ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements
- NEN-ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls
- NEN-ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management
- NEN-ISO/IEC 27017:2015 – Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- NEN-ISO/IEC 27018:2014 – Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- NEN-ISO/IEC 27033-1:2015 – Information technology – Security techniques – Network security – Part 1: Overview and concepts
- NEN-ISO/IEC 27035:2011 – Information technology – Security techniques – Information security incident management
- NIST SP800-12 (1995) – Introduction to Computer Security — The NIST Handbook
- NIST SP800-30r1 (2012) – Guide for Conducting Risk Assessments
- NIST SP800-61r2 (2012) – Computer Security Incident Handling Guide
- Personal Data Authority – Policy rules for the implementation of Article 34a of the Dutch Data Protection Act[5]

[4] The Open Web Application Security Project (OWASP) is an open-source computer security project. Individuals, schools and companies use this platform to share information and techniques. See: https://www.owasp.org

[5] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf (consulted on 19 April 2016)

- ENISA – Algorithms, key size and parameters report – 2014[6]
- Common Criteria – Certified Products[7]
- PCI Data Security Standard – v3.2[8]
- CIS Critical Security Controls for Effective Cyber Defense[9]

[6] https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014 (consulted on 20 April 2016)

[7] https://www.commoncriteriaportal.org/products/ (consulted on 20 April 2016)

[8] https://www.pcisecuritystandards.org/ (consulted on 20 April 2016)

[9] https://www.cisecurity.org/critical-controls.cfm (consulted on 20 April 2016)

Table with security measures

1 Policy and organisation

A security policy that is supported and established by the management is the foundation for all information security. The policy is based on an analysis of the risks. Permanent, temporary and external staff must be aware of the policy and know their responsibilities. A process has been established for the management of incidents, including data breaches, changes and availability.

#	Measure	Reference
	Current information security policy and information security organisation	
1.1	The supplier's management has established an information security policy, which it clearly communicates both internally and to all relevant external parties on a regular basis (annually).	ISO 27002:2013 Art. 5.1.1
1.2	The information security policy is assessed at least once a year or when a major change has occurred.	ISO 27002:2013 Art. 5.1.2
1.3	The supplier has defined and established the information security responsibilities, and has implemented them in job descriptions.	ISO 27002:2013 Art. 6.1.1
	Risk analysis	
1.4	The supplier performs a risk analysis at least every three years to document the threats and vulnerabilities, their consequences for the organisation and the likelihood of those consequences. Adequate security measures are established and introduced based on the risk analysis.	ISO 27001:2013 Art. 8.2 ISO 27005:2011 Art. 12.1
1.4 HIGH	The supplier performs a risk analysis at least **every year** to document the threats and vulnerabilities, their consequences for the organisation and the likelihood of those consequences. Adequate security measures are established and introduced based on the risk analysis.	ISO 27001:2013 Art. 8.2 ISO 27005:2011 Art. 12.1
1.5	The supplier describes how the identified risks are treated and supports the reasons for accepting any residual risks.	ISO 27001:2013 Art. 8.3 ISO 27005:2011 Arts. 9 and 10
	Awareness and training	
1.6	All the supplier's employees – as well as external staff and external users, if applicable – shall receive training right after they join and regular further training on the information security policy and the information security procedures later on.	ISO 27002:2013 Art. 7.2.2
1.6 HIGH	All the supplier's employees – as well as external staff and external users, if applicable – shall receive training right after they join and further training on the information security policy and the information security procedures **at least once a year** later on.	ISO 27002:2013 Art. 7.2.2
	Incident management and data breaches	
1.7	The supplier uses processes for the implementation of its incident management. It categorises its activities in this respect: classification, prioritising, diagnosis, communication and documentation.	ISO 27002:2013 Art. 16.1.1 ISO 27035:2011 NIST SP800-61r2

1.8	The supplier uses job descriptions, which include incident management tasks.	ISO 27002:2013 Art. 16.1.1 ISO 27035:2011 NIST SP800-61r2
1.9	The supplier has a set method and fixed format for incident reporting.	ISO 27002:2013 Art. 16.1.2 ISO 27035:2011 NIST SP800-61r2
1.10	The supplier uses an incident classification framework, which may or may not be automated, based on urgency and impact.	ISO 27002:2013 Art. 16.1.4 ISO 27035:2011 NIST SP800-61r2
1.11	The supplier has set up a procedure to inform the client of any potential data breaches it detects (including those with external processors or subcontractors) adequately and on time. In the event of an incident, the supplier shall document all the steps it has taken to meet its duty to report data breaches.	Dutch Data Protection Act, Article 14 Policy rules regarding the obligation to report data breaches, H2.1 – 2.4 (AP)
	Change management	
1.12	The supplier has set up a process for change management, based on ITIL3 or ISO 20000-1 for example.	ISO 27002:2013 Art. 12.1.2
1.13	The supplier tests any changes in a test or acceptance environment before deploying them into production and documents the test results.	ISO 27002:2013 Arts. 12.1.4, 14.2.6 and 14.2.9 PCI DSS v3.2 Art. 6.4.5.3
1.14	The supplier makes changes within the agreed service windows and discusses any changes that have a major impact with the client before implementing them.	PCI DSS v3.2 Arts. 6.4.5, 6.4.5.1 and 6.4.5.2
1.14 HIGH	The supplier makes changes within the agreed service windows and presents any changes that have a major impact to the *Change Advisory Board* before implementing them.	PCI DSS v3.2 Arts. 6.4.5, 6.4.5.1 and 6.4.5.2
1.15	The supplier documents the situation after any changes to the configuration database.	ISO 27002:2013 Art. 12.4.1
	Continuity management	
1.16	The supplier has taken preventive and corrective measures to implement the availability requirements.	ISO 27002:2013 Arts. 17.1 and 17.2
1.17	The supplier is aware of the single points of failure in the infrastructure and has taken measures to ensure any failures can be resolved within the agreed time frame.	ISO 27002:2013 Arts. 17.1 and 17.2
1.18	The supplier continuously monitors the availability and capacity of applications and systems.	ISO 27002:2013 Arts. 12.1.2 and 12.1.3
1.18 HIGH	The supplier continuously monitors the availability and capacity of applications and systems. Any threshold values that are exceeded are detected and reported to the client on time.	ISO 27002:2013 Arts. 12.1.2 and 12.1.3
1.19	The supplier makes back-ups according to the availability requirements.	ISO 27002:2013 Art. 12.3
1.20	The supplier stores back-ups securely off-site. There must be a distance of at least five kilometres between the primary storage and back-up location.	ISO 27002:2013 Art. 12.3

1.21 HIGH	The supplier also has continuity plans available for the provided services. It updates and tests these continuity plans regularly. If there is a chance that the tests will affect the provided services, the client shall be informed when the tests are planned. If any deficiencies are found, an improvement plan or new plan with clearly described actions must be prepared.	
	Confidentiality	
1.22	The supplier shall conclude confidentiality agreements with employees and third parties.	
1.23	The supplier's employees – as well as external staff and external users, if applicable – involved in risk class 2 data processing must present a Dutch Certificate of Conduct showing their criminal records.	
1.23 HIGH	The supplier's employees – as well as external staff and external users, if applicable – involved in risk class 3 data processing must present a Dutch Certificate of Conduct showing their criminal records.	

2 Access security

Access control is essential to determine and know who has access to (sensitive) data. Every user is assigned a unique login ID and given access to the data, possibly based on roles. Access control also includes physical access control and access to mobile devices.

#	Measure	Reference
	Physical access security and equipment security	
2.1	IT facilities and equipment are physically protected against unauthorised access, damage and malfunctions. The measures taken are in accordance with the identified risks.	ISO 27002:2013 Arts. 11.1 and 11.2
	Logical access security	
2.2	The supplier has established and documented an access security policy, which requires at least that: • the users and administrators have a unique login ID and password combination; • shared login ID and password combinations are not permitted; • user and administrator access is limited to the network and the network services they have been specifically authorised for.	ISO 27002:2013 Arts. 9.1 and 9.2.4
2.3	The supplier has a policy for mobile devices, which requires at least that: • the device has a key lock or similar feature, with password access for example; • private and business use are kept separate and business data on the device is encrypted.	ISO 27002:2013 Arts. 6.2.1 and 11.2.8
2.4	The supplier establishes a formal process to manage the access rights of users and administrators. The access administration process includes at least: • the registration of users and their assigned rights; • the allocation of no more rights than those necessary to perform the tasks; and • the modification or withdrawal of those rights when the contract or employment changes or ends.	ISO 27002:2013 Arts. 9.2.1, 9.2.2, 9.2.3, 9.4.1 and 9.2.6

2.5	Users and administrators are informed of the access security policy and sign a statement confirming that they shall not disclose any personal confidential authentication information and they shall take action immediately in the event of a breach in order to limit the consequences.	ISO 27002:2013 Art. 9.3.1
2.6	The supplier checks whether the assigned rights are correct every month.	ISO 27002:2013 Art. 9.2.5
2.7	The supplier sets up secure login procedures for systems and applications based on the access security policy. The login procedures shall include at least a strong password. The risk analysis shows whether strong authentication (multi-factor authentication) is required for specific systems or applications.	ISO 27002:2013 Arts. 9.4.2 and 9.4.3

3 Management of technical vulnerabilities and anti-malware

Malware can penetrate networks and systems and exploit vulnerabilities in various ways. This threat can be reduced with antivirus software and regular vulnerability testing of systems and applications.

#	Measure	Reference
	Vulnerabilities management	
3.1	The supplier sets up a process to prevent the exploitation of technical vulnerabilities. The process requires at least that: • systems and software are updated regularly (patching); • information on new vulnerabilities is gathered on time (intelligence); • a vulnerability assessment of the network and systems is performed; • the vulnerabilities of web applications are tested on a regular basis (web application scanning); • antivirus software is used and updated daily; • the installation of (unauthorised) software is restricted.	ISO 27002:2013 Arts. 12.2, 12.6.1, 12.6.2 and 14.2 ISO 27033-1:2015 Art. 8.3
3.1 HIGH	The supplier sets up a process to prevent the exploitation of technical vulnerabilities. The process requires at least that: • systems and software are updated regularly (patching); • information on new vulnerabilities is gathered on time (intelligence); • software packages and infrastructure software are *automatically* checked for known weaknesses; • web applications are tested continuously in terms of vulnerabilities (web application scanning) and *a penetration test is performed at least once a year*;	ISO 27002:2013 Arts. 12.2, 12.6.1, 12.6.2 and 14.2 ISO 27033-1:2015 Art. 8.3

#	Measure	Reference
	• *anti-malware (including antivirus) software from various suppliers with different engines* is used and updated daily; • the installation of (unauthorised) software is restricted.	
	Intrusion detection	
3.2	The supplier inspects data traffic from external or untrusted networks in real time.	ISO 27033-1:2015 Arts. 8.5 and 8.6
3.3 HIGH	The supplier has an intrusion detection/prevention system that recognises network-based attacks based on signatures, protocol validation and anomaly detection.	
3.4 HIGH	The supplier removes and/or disables all services that are not essential for the work. If the system software does not allow this, the supplier blocks the services with documented filters on the nearest network component that can provide this filter.	

4 Data confidentiality, integrity and privacy

The data must be well-protected in case an attacker manages to circumvent the access control. This applies to both data at rest and data in transit. Additional measures are required to protect privacy-sensitive data.

#	Measure	Reference
	Protection of personal data	
4.1	The supplier must have a privacy policy or privacy regulations that are less than three years old.	ISO 27002:2013 Art. 18.1
4.2	The supplier has appointed and instated a privacy officer.	Dutch Data Protection Act, Article 62
	Encryption	
4.3	The supplier shall always encrypt confidential data at rest in the following situations: • on removable media (such as externally stored back-up tapes, DVDs, memory cards and USB flash drives); • in the storage memory of mobile devices (such as the internal and external memory of laptops, smartphones and tablets).	ISO 27002:2013 Arts. 10.1, 13.2 and 14.1.2 The Personal Data Protection Authority's *Personal Data Security* guideline, page 25
4.3 HIGH	The supplier shall *always* encrypt confidential data at rest.	
4.4	End-to-end encryption is always necessary when transporting data that is classed as sensitive or critical (during a back-up, for example). The supplier shall always encrypt confidential data in transit in the following situations: • private network management sessions (with encryption provisions in the management tools or protocols used); • wireless data communication; • the storing or sending of passwords.	
4.4 HIGH	End-to-end encryption is always necessary when transporting data. The supplier shall *always* encrypt confidential data in transit.	
4.5	The supplier uses connection encryption and hashing algorithms that meet the current requirements.	Policy rules regarding the obligation to

		report data breaches, H7.2.3 ENISA algorithms, key size and parameters report 2014
4.6	The supplier uses hardware solutions (such as smart cards and Hardware Security Module products) that have been certified according to the relevant standards.	Common criteria
4.7	The supplier erases data and removable media from old equipment securely before discarding it.	ISO 27002:2013 Art. 11.2.7 NIST Art. 14.5.7
4.8 HIGH	Authentication of users based on cryptographic techniques, hardware tokens or challenge/response protocols (strong authentication) is mandatory in the following situations: • when Single Sign-On is applied; • for any type of access from an untrusted network; • when managing critical security features (such as firewalls, routers and intrusion detection and prevention systems).	
4.9 HIGH	The supplier aligns the validity of cryptographic keys and certificates with the application's critical content at least once a year.	

5 Monitoring and logging

Logging and tracking user activity is essential to prevent, detect or minimise the impact of a breach.

#	Measure	Reference
5.1	The supplier documents the (personal) data activities of users in logs, and registers all approved and rejected attempts to access information sources.	ISO 27002:2013 Art. 12.4.1
5.2	The supplier protects the log facilities and log file information against forgery and unauthorised access.	ISO 27002:2013 Art. 12.4.2 Dutch Data Protection Act, Article 10.2
5.3	The supplier records the activities of system administrators and operators and assesses them regularly.	ISO 27002:2013 Art. 12.4.3
5.4	The supplier uses a single time source as a reference to synchronise all relevant information processing systems in order to guarantee the accuracy of the log files.	ISO 27002:2013 Art. 12.4.4
5.5	The supplier sends the client monthly reports that include at least the following: • the number of successful and failed login attempts; • date and time of unsuccessful login attempts; • requested and authorised access to shared files/information outside normal times of operation; • administrators' activities; • significant user actions (such as changes to permissions, configuration parameters and master data, depending on the application); • detected malware (worms, viruses, spyware, etc.) and disruption of services.	
5.6	The supplier stores all information in the log files for at least three months, but for no more than 12 months, unless legally required to do otherwise or unless the log files are needed in an investigation of a (suspected) security incident. The client may access this information during this period.	Dutch Data Protection Act, Articles 10.1 and 10.2