Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

RWS INFORMATIE

Information Security: TSR

Information Security: Tender Specification Requirements for IS contracts

Date:	2 September 2019
Status:	Final

Credits

Published by:	Security Centre, Rijkswaterstaat
Information:	Marco Rijkschroeff / Turabi Yildirim / Sahar Habib
Telephone:	
Fax:	
Prepared by:	Security Centre, Rijkswaterstaat
Layout:	
Date:	2 September 2019
Status:	Final
Version number:	1.7

Contents

1 Information security of system requirements in IS procurement contracts 6
1.1 Organising information security 6
1.2 Access security 6
1.3 Physical and environmental security 6
1.4 Security of operations 6
1.5 Communications security 7
1.6 Acquisition, development and maintenance of equipment and software 7
1.7 Compliance 8
Appendix A: Sources in contract texts 9
Appendix B: Numbering of contract requirements 11

1 Information security of system requirements in IS procurement contracts

NOTE: This document is an annex with the system requirements listed in the adopted master document 'Information Security in Standard RWS IS Contract Requirements'.

References to external documents are described as {n} and can be found in Appendix A. References to external documents are described as IBR-n and can be found in the document Information security guidelines for RWS IV contract requirements v1.0. Terms beginning with a capital letter are proper nouns and refer to specific meanings in the ARBIT and ARVODI contract texts. Other terms correspond to the definitions mentioned in the Dutch version of NEN/IEC ISO 27000. For all other terms as used in the original Dutch version of this annex, reference is made to their general meaning as found in the leading Dutch dictionary 'Van Dale Groot woordenboek van de Nederlandse taal'. Background information on the numbering of requirements used can be found in Appendix B.

1.1 Organising information security

6.1.2 Information systems involved in the Performance must be set up with an authorisation model and measures that detect or prevent unauthorised access to business assets.
NOTE: If the Performance consists solely of the procurement of information systems, this text must be interpreted to mean that the information system comes with this functionality as standard.

6.2.1 Mobile devices used by Personnel must store data relating to the Performance in an encrypted manner in accordance with the Client's IBR-1 guideline: *Data Classification Policy* by means of cryptographic applications using only algorithms and settings designated as 'good' from the most current version of the NCSC document: Guidelines for Transport Layer Security (TLS) {1}.

1.2 Access security

9.1.2 Information systems involved in the Performance contain only standard functional accounts necessary for software or accounts provided through the current authorisation process.

9.4.1 Accounts on information systems involved in the Performance only have access rights linked to roles assigned through the current authorisation process.

9.4.2 Information systems involved in the Performance have a secure login procedure in accordance with the Client's IBR-2 guideline: *Logical access security policy*.
NOTE: If the Performance consists solely of the procurement of information systems, this text must be interpreted to mean that the information system comes with this functionality as standard.

9.4.3 Information Systems involved in the Performance have password management features that enforce the use of strong passwords that at least comply with the Client's IBR-3 guideline: *Password Use Policy*.
NOTE: If the Performance consists solely of the procurement of information systems, this text must be interpreted to mean that the information system comes with this functionality as standard.

1.3 Physical and environmental security

11.1.x Information processing facilities involved in the Performance are physically secured at least in accordance with the Client's IBR-6 guideline: *Guidelines for Physical Security*.

11.2.x Information processing facilities involved in the Performance are protected against loss, damage, theft, compromise or interruption, implementing at least the requirements from the Client's IBR-6 guideline: *Guidelines for Physical Security*.

1.4 Security of operations

12.1.4 The Contractor must have development, testing, production and, if ordered, educational environments demonstrably separate (logically or physically) for all information systems involved in the Performance. Separation implies that everything necessary must be arranged to avoid interference between environments and to ensure the reliability of the production systems. The acceptance and training environments must be representative of the production environment, such that the test or exercise results reflect the behaviour of the functionality in the production environment.

12.2.1	Information systems involved in the Performance are equipped with detective and preventive measures against malware.
12.2.SC-13	The Contractor must harden the information systems involved in the Performance by: • Disabling non-essential data network services; • Removing (patching) known vulnerabilities; • Deactivating/blocking all unnecessary ports; • Disabling the default account in accordance with the password policy; • Using vendor security options, if available; • Following the standard hardening profiles for the common platforms, see, for example, CIS's 'Security Benchmarks' for this purpose: http://www.cisecurity.org/.
12.3.1	Information systems involved in the Performance have facilities for making backups of all their existing information and software. If information systems are located on the Client's infrastructure, it must be possible to do this to the Client's central backup facility.
12.4.x	Information systems involved in the Performance record events, meeting at least the requirements listed in the Client's IBR-7 guideline: *Guidelines for Logging*. NOTE: If the Performance consists solely of the procurement of information systems, this text must be interpreted to mean that the information system comes with this functionality as standard.

1.5 Communications security

13.1.3	Groups of information systems and users involved in the Performance can be separated based on their function, role and/or classification into logical or physical network domains in accordance with a zoning model. Information systems placed in the Client's infrastructure must, for this purpose, adhere to the Client's design (in accordance with PSA).
13.1.3 Melvin's proposal in email of 15/8	Groups of information systems and users involved in the Performance can be separated based on their function, role and/or classification into logical or physical network domains in accordance with a zoning model. Information systems placed in the Client's infrastructure must, for this purpose, adhere to the Client's design (in accordance with PSA).
13.2.3	Information systems involved in the Performance that use electronic messages containing data whose confidentiality and/or integrity need to be ensured must use encryption for this purpose. The underlying algorithms and settings used may only be designated as 'good' in the most current version of the NCSC document: Guidelines for Transport Layer Security (TLS) {1}. NOTE: If the Performance consists solely of the procurement of information systems, this text must be interpreted to mean that the information system comes with this functionality as standard.

1.6 Acquisition, development and maintenance of equipment and software

14.1.1	At least the measures mentioned in the CIP document *Grip on SSD - Security requirements for web and other applications* {3} are implemented in the software that forms part of the information systems involved in the Performance. NOTE: If the Performance consists solely of the procurement of information systems, this text must be interpreted to mean that the information system comes with this functionality as standard.
14.1.2	Information systems involved in the Performance that exchange information through public networks must always use encrypted protocols for this purpose. The underlying encryption algorithms and settings used may only be designated as 'good' in the most current version of the NCSC document: Guidelines for Transport Layer Security (TLS) {1}. NOTE: If the Performance consists solely of the procurement of information systems, this text must be interpreted to mean that the information system comes with this functionality as standard.
14.1.3	Information systems involved in the Performance that are part of a chain must, depending on the classification of the exchanged data, always ensure the integrity or confidentiality of this data through encryption. The underlying encryption algorithms and settings used may only be designated as 'good' in the most current version of the NCSC document: Guidelines for Transport Layer Security (TLS) {1}. NOTE: If the Performance consists solely of the procurement of information systems, this text must be interpreted to mean that the information system comes with this functionality as standard.
14.1.SC-03	Information systems involved in the Performance that are accessed remotely and for management purposes must only be approached through encrypted protocols. The underlying encryption algorithms and settings used may only be designated as 'good' in the most current version of the NCSC document: Guidelines for Transport Layer Security (TLS) {1}. NOTE: If the Performance consists solely of the procurement of information systems, this text must be interpreted to mean that the information system comes with this functionality as standard.
14.1.SC-26	At least the measures from the *Guide on Mobile App Development and Management for the Central Government* {4} must be implemented for the development and management of mobile applications.
14.1.SC-04a	Information systems involved in the Performance that will be placed in the Client's infrastructure must be set up in accordance with the Client's standard connection conditions {5}.

NOTE: If the Performance consists solely of the procurement of information systems, this text must be interpreted to mean that the information system comes with this functionality as standard.

14.1.SC-04b Information systems involved in the Performance that will be placed in the Client's infrastructure must use the Client's standard network services {6}.
NOTE: If the Performance consists solely of the procurement of information systems, this text must be interpreted to mean that the information system comes with this functionality as standard.

14.2.8a Information systems involved in the Performance are demonstrably tested for vulnerabilities using common testing methodologies before they are put into production. The test method used for software includes at least the *OWASP Top-10* {7}.

14.2.8b All known vulnerabilities in information systems involved in the Performance are remedied before these information systems are put into production.

14.2.9a Information systems involved in the Performance must have undergone an acceptance test on all system requirements specified in this Agreement before these systems are put into production.

14.2.9b Information systems involved in the Performance must not be put into production until all findings from the acceptance test have been remedied.

1.7 Compliance

18.1.5 Information systems involved in the Performance protect information through cryptographic measures in accordance with relevant agreements, laws and regulations. Only algorithms designated as 'good' in the most current version of the NCSC document: ICT Security Guidelines for Transport Layer Security (TLS) {1} may be applied in this process.
NOTE: If the Performance consists solely of the procurement of information systems, this text must be interpreted to mean that the information system comes with this functionality as standard.

Appendix A: Sources in contract texts

Sources are mentioned in the contract texts, as follows.

Number	Source
{1}	National Cyber Security Centre (NCSC), *ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)* (ICT Security Guidelines for Transport Layer Security (TLS)), URL: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls
{2}	Rijkswaterstaat IRN, *Afspraken en Procedures Netwerkdienstverlening: Netwerktoegang voor Derden* (Network Service Arrangements and Procedures: Third Party Network Access), RWS Intranet URL: http://vpr.intranet.rws.nl/ProjectDirectory/Infosite_Netwerkdienstverlening/Lists/Veel%20gestelde%20vragen/DispForm.aspx?ID=49
{3}	Centre for Information Security and Privacy (CIP), *Grip op SSD - Beveiligingseisen voor (web)applicaties* (Grip on SSD – Security Requirements for web and other applications) URL: https://www.cip-overheid.nl/category/producten/secure-software/
{4}	Central government: *Handreiking Mobiele App Ontwikkeling en Beheer voor de Rijksoverheid* (Guide on Mobile App Development and Management for the Central Government) URL: https://www.noraonline.nl/wiki/Mobility
{5}	Rijkswaterstaat IRN, *RWS IV Aansluitvoorwaarden/RIVA* (RWS IV Connection Conditions/RIVA), URL: Classification RWS Company Confidential: https://werkwijzer.cf-prod.intranet.rws.nl/index.html Classification of RWS Information: https://www.rijkswaterstaat.nl/zakelijk/zakendoen-met-rijkswaterstaat/werkwijzen/werkwijze-in-iv/index.aspx
{6}	Rijkswaterstaat IRN, *Aansluitvoorwaarden NNV Rijkswaterstaat* (Connection Conditions for Rijkswaterstaat's national fibre optic infrastructure). http://vpr.intranet.rws.nl/ProjectDirectory/Infosite_Netwerkdienstverlening/Algemeen_klanten/PDC%20en%20DAP/Forms/AllItems.aspx
{7}	Open Web Application Security Project (OWASP), 'OWASP Top 10' https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
{8}	*BIO Handreiking Veilige afvoer van ICT-middelen* (GISB Guide: The safe removal of ICT assets) https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/04/201902-Handreiking-Veilige-afvoer-van-ICT-middelen-v2.0.pdf
{9}	*BIO Handreiking Mobile Device Management* (GISB Guide: Mobile Device Managementhttps://www.informatiebeveiligingsdienst.nl/product/mobile-device-management/
{10}	*Richtlijnen informatiebeveiliging bij RWS IV-contracteisen v1.0* (Information security guidelines for RWS IV contract requirements v1.0)
{11}	*BIO Handreiking Risicoanalysemethode* (GISB Guide: Risk analysis method) https://www.informatiebeveiligingsdienst.nl/product/handreiking-diepgaande-risicoanalyse-methode-gemeenten/

{12}	*BIO Handreiking Penetratietesten* (GISB Guide: Penetration testing) https://www.informatiebeveiligingsdienst.nl/product/handreiking-penetratietesten-v1-0/
{13}	*Handreiking Risicomanagement ISO-27005* (Guide for Risk Management ISO-27005)
{14}	*BIO Algemene handreiking continuïteitsbeheer* (GISB General Guide to Continuity Management) https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/07/201903-Model-Continu%C3%AFteitsplan_v2.0.docx
{15}	Template for the Information Security Plan IV
IBR-1	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Beleid voor gegevensclassificatie* (Data classification policy)
IBR-2	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Beleid voor logische toegangsbeveiliging* (Logical access security policy)
IBR-3	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Beleid voor wachtwoordgebruik* (Password use policy)
IBR-4	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Richtlijnen voor beveiligen bij ontwikkelen* (Guidelines on security during development)
IBR-5	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Richtlijnen voor informatiebeveiligingsincidenten* (Guidelines for information security incidents)
IBR-6	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Richtlijnen voor fysieke beveiliging* (Guidelines for physical security)
IBR-7	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Richtlijnen voor logging* (Guidelines for logging)
IBR-8	Rijkswaterstaat Security Centre, *Richtlijnen informatiebeveiliging bij RWS IV-contracteisen* (Information security guidelines for RWS IV contract requirements), chapter on *Richtlijnen voor het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT systemen van RWS* (Guidelines for safely connecting management and maintenance equipment to RWS's ICT systems)

If departments other than Rijkswaterstaat use the contract texts, they can choose to adapt these sources to their own organisation-specific sources. The sources actually mentioned in a final contract text must obviously be appended to the contract (this is not necessary if the link is publicly available).

Appendix B: Numbering of contract requirements

The numbering of the contract requirements refers to the corresponding three-point standards in the NEN document *ISO/IEC 27002:2013: IT Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging* (IT Security Techniques – Practical guideline with information security control measures) and is primarily for internal RWS use. Because this proved to be practical, deviations from this numbering have occurred in some cases. The following deviations apply:

1. In some cases, a requirement has been split into two parts; in that case, an ‘a’ and a ‘b’ have been added after the three-point standard to distinguish between them.
2. In some cases, the three-point standards under one two-point standard have merged into one contract requirement. In this case, the third digit in the three-point standard notation is replaced by an ‘x’.
3. Requirements from the CIP document *Cloud computing - Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)* (Cloud computing- An operational product based on the Civil Service Information Security Baseline (CSISB)) for which no corresponding requirement exists within ISO/IEC 27002 have been added to a corresponding two-point standard, with the third ‘digit’ in the three-point notation ‘CC-n’, where ‘n’ corresponds to the number of the standard from the CIP document.
4. Requirements from the RWS Security Centre itself for which no corresponding requirement exists within ISO/IEC 27002 have been added to a corresponding two-point standard, with the third ‘digit’ in the three-point notation ‘SC-n’, where ‘n’ corresponds to the number on the list of SC requirements.

Page 11 of 11