

Appendix D - Baseline Information Security

Security Requirements	Contract text	Validation
1	For the Performance agreed, Counterparty is certified in conformity with the most recent version of the NEN-ISO/IEC 27001 standard or similar, and will remain for at least the term of the Agreement.	No rationale needed
2	Counterparty must, wherever Client does not refer to specific security guidelines in terms of measures to be taken, observe the guidelines from the most recent version of the NEN-ISO/IEC 27002 standard.	No rationale needed
3	Counterparty must demonstrably lay down the responsibilities, tasks and authorities for at least all processes stated in the Agreement, in appropriate sections in the (project)organisation.	No rationale needed
4	Counterparty must have a policy for separation of functions (if reasonably feasible) when applying executive, auditing and management tasks involved with the Performance, and must demonstrably have, operationally safeguarded this in processes.	No rationale needed
5	Counterparty must have an operationally safeguarded project management process for the Performance in which information security has been demonstrably integrated.	No rationale needed
6	Counterparty must demonstrably have an operationally safeguarded process for the encryption of data on mobile equipment, involved with the Performance, where account is taken of the classification of these data {4} and actuality of the safety of the encryption methods used {3}.	No rationale needed
7	Remote access to equipment and software of Client, by the Counterparty, in the Client's network, is permitted only via a specially designed Access for Third Parties service {5} of Client.	No rationale needed
8	Counterparty must demonstrably have an operationally safeguarded process for the screening of the Staff who perform work activities: 1. in the area of development or review of design drawings and/or - documents; 2. development, testing, managing, installing, configuring and/or operating software or equipment; 3. in operational or technical spaces; 4. on cables and pipes; 5. on security and safety documentation and instructions, involved with the Performance, by means of at least a relevant Certificate of Good Conduct (COGC), where, in terms of the contract period, a screening should never be older than 5 years. Pending the application of a screening, an own statement of relevant person will suffice, during a period of six weeks at most, calculated from the start date of this person on the Performance, which cannot be extended.	No rationale needed
9	Counterparty must demonstrably have operationally safeguarded that Staff have received an education and training in the area of safety awareness, matching the nature of the work to be performed, whereas also annual retraining is being received, during which at least also personal responsibility and specific security frameworks of Client are discussed.	No rationale needed
10	Counterparty must demonstrably have operationally safeguarded that Staff responsible for the testing of information systems involved with the Performance, have up-to-date and specialist knowledge and training, with regard to the testing of its security.	No rationale needed

11	Counterparty must demonstrably have an operationally safeguarded process for the defining of tasks and responsibilities with regard to information security for the Performance and must communicate to the Staff that: 1. these remain in force until after the termination or modification of the employment; 2. these must be executed.	No rationale needed
12	Counterparty must demonstrably have operationally safeguarded that of all information systems involved with the Performance, an inventory was drawn up in a Configuration Management Database (CMDB), such that it can be used effectively, for an effective Configuration Management (CM) ITIL process, and that this CMDB is kept up-to-date.	No rationale needed
13	Upon request of the Client, Counterparty must transfer the data stated in the Configuration Management Database (CMDB), regarding information systems that were unlocked via the Client's infrastructure.	No rationale needed
14	Counterparty must demonstrably have operationally safeguarded that all information involved with the Performance is classified in accordance with the classification scheme {4} of Client and that the accompanying security measures are being observed.	No rationale needed
15	Counterparty must have operationally safeguarded processes for the safe removal of media, transport of media and the management of removable media, involved with the Performance, in accordance with the classification scheme {4} of Client.	No rationale needed
16	Counterparty must ensure an operationally safeguarded procedure for the provision of physical or logical access to information processing facilities, including the issuing and retrieving of accounts and authorisations, and an up-to-date registration thereof.	No rationale needed
17	If Client or third party is responsible for the provision of the physical or logical access to information processing facilities, then Counterparty shall observe the access procedure used by Client or third party.	No rationale needed
18	At least annually, Counterparty must assess and update both the physical and logical access rights to information processing facilities of the Staff, via an operationally safeguarded and formal process.	No rationale needed
19	Counterparty must require the Staff to observe the Policy for use of passwords {1} of Client when making use of authentication data related to the Performance.	No rationale needed
20	Counterparty must demonstrably have an operationally safeguarded process for the monitoring of the use of system tools that are able to circumvent control measures for information systems involved with the Performance.	No rationale needed
21	Counterparty must demonstrably have operationally safeguarded that only specifically authorised Staff has access to the Source code of information systems involved with the Performance.	No rationale needed
22	If Counterparty is contractually or legally obliged to make use of cryptography to protect information involved with the Performance, for the use of these cryptographical control measures, Counterparty must have policies and operationally safeguarded processes, including the use, the protection and the lifespan of the accompanying cryptographical keys, during their entire lifecycle.	No rationale needed

23	Counterparty must demonstrably dispose of an operationally safeguarded process for the destruction of data on media in the event of disposal or replacement of (parts of) information systems that these media contain, and are involved with the Performance.	No rationale needed
24	Counterparty must demonstrably have operationally safeguarded operation procedures and make these available to the Staff and, where applicable, to employees of Client, who need them for the Performance.	No rationale needed
25	Counterparty must demonstrably have operationally safeguarded processes for protection against malware on information systems involved with the Performance, whereby at least attention is paid to prevention, detection, communication and recovery.	No rationale needed
26	Counterparty must demonstrably have an operationally safeguarded process for making back-ups of all information and software used for the Performance, on a daily basis at least.	No rationale needed
27	Counterparty must test the recovery process that is part of the back-up process of all information and software used for the Performance, at least annually, and notify Client of the outcome thereof.	No rationale needed
28	Counterparty must demonstrably have an operationally safeguarded process for the sufficing periodic assessment of log files of information systems involved with the Performance, whereby the interval between two assessments should never exceed a period of one month.	No rationale needed
29	Counterparty must demonstrably have an operationally safeguarded process for the monthly assessment of activities of system managers and operators on information systems involved with the Performance, which have been documented in log files.	No rationale needed
30	Counterparty must keep log files of information systems, involved with the Performance, available for at least three months (and at least 3 years in case of a suspected incident), unless a different retention period was agreed with Client, and disclose these log files to Client upon Client's request.	No rationale needed
31	In order to protect the information in information systems, Counterparty must, demonstrably have operationally safeguarded processes for management and control of networks involved with the Performance, where attention is being paid to at least the aspects below: - Management or network security - Technical vulnerability management - Identification and authentication - Network audit logging and monitoring - Intrusion detection and prevention - Protection against malicious code - Cryptographic based services - Business continuity management	No rationale needed
32	Counterparty must have incorporated security mechanisms, service provision levels and management requirements for all services involved with the Performance, in a Service Level Agreement (SLA) with Client, paying attention to at least the safety aspects availability, reporting of incidents, implementing changes and escalation.	No rationale needed
33	Counterparty must demonstrably have operationally safeguarded policies, procedures and control measures to protect the transport of information involved with the Performance, that is done via all sorts of communication facilities.	No rationale needed

34	During the entire lifecycle, Counterparty must make security an integral part of the process for development and maintenance of information systems. In the event of software, at least the measures mentioned in the CIP document Grip on SSD - Security Demands for (web)applications {10} must be implemented for this purpose.	No rationale needed
35	Counterparty must demonstrably have information security operationally safeguarded in the processes which are part of the development lifecycle of information systems involved with the Performance, whereby at least the process requirements from the Directive Security during development {15} are being implemented.	No rationale needed
36	Counterparty guarantees the functioning of information systems (at least until their End of Life (EOL), as indicated by Supplier), which are part of the Performance, on/with products or software that are not EOL and with an up-to-date patch level, or offers a free-of-charge upgrade to make this possible after all.	No rationale needed
37	Regarding information systems involved with the Performance, Counterparty must make adjustments free of charge, or make patches available (at least to the End of Life (EOL) of this information system, as indicated by Supplier), within 60 days after learning about vulnerabilities in the event of software and within 6 months in case of equipment, with the aim to resolve these vulnerabilities.	No rationale needed
38	Client is entitled to perform audit(s) during which the requirements from the contract between Client and Counterparty are assessed on setup, existence and/or functioning. Counterparty must fully and voluntarily cooperate with this audit.	No rationale needed
39	Counterparty must have an operationally safeguarded process for the registration, reporting and processing of information security incidents, which is in line with the incident management process of Client, whereby at least the requirements from the Directive for information security incidents {16} are being implemented. At least on a monthly basis, reports must be reported to Client, regarding these information security incidents.	No rationale needed
40	Counterparty must demonstrably have a continuity plan for maintaining the Performance in the event of unfavourable situations, during which also the continuity of the information security is guaranteed.	No rationale needed
41	Counterparty must demonstrably verify and adjust the continuity plan for the Performance at least annually, to guarantee that it remains solid and effective.	No rationale needed
42	Counterparty must demonstrably have operationally safeguarded procedures for protection against loss, destruction, falsification, unauthorised access and unauthorised release of registrations on information systems involved with the Performance, in accordance with legal, regulatory, contractual and company requirements.	No rationale needed
43	Data or software of Client, or metadata generated by him, which is available on information systems of Counterparty, is and will always remain the property of Client. If data was provided to Counterparty by Client, Staff can use this only for the purpose it was issued for.	No rationale needed
44	Counterparty must demonstrably have operationally safeguarded processes for the destruction of data or software of Client on equipment and all back-up media of Counterparty, after termination of the contract between both parties.	No rationale needed

45	If Client's data is available on information systems of Counterparty, in the event of termination of the contract between these parties, the Counterparty must provide assistance in the transfer of this information to the new supplier or back to the Client.	No rationale needed
46	If Client's data or software is available on information systems of Counterparty, the Counterparty must indicate the whereabouts of these information systems. If these are to be found outside the EU, this can only be in countries where a suitable level of data protection is provided; the specific countries have been determined by the European Committee.	No rationale needed
47	Counterparty must perform an audit at least annually, regarding the setup, existence and functioning of the measures in the area of the information security stated in the contract with Client, and inform this Client about the findings and intended improvement measures.	No rationale needed
48	Counterparty must demonstrably have operationally safeguarded processes for the periodic assessment of the compliance with policy regulations, standards and other requirements regarding security, in terms of Staff involved with the Performance.	No rationale needed
49	Counterparty must demonstrably have operationally safeguarded processes for the periodic assessment of compliance with technical policy rules, standards and other requirements regarding security of information systems involved with the Performance.	No rationale needed
50	Counterparty must keep to the agreements and procedures in the area of information security in the agreed Dossier Agreements and Procedures (DAP) in which also the objective, method and frequency of contact about the information security is described at a strategic, tactical and operational level.	No rationale needed