centro criptológico nacional

ICT Security Guide
CCN-STIC 823

ANNEX I - Clauses and Service Level Agreements

JANUARY 2022

MINISTERIO DE DEFENSA

1. ANNEX I Clauses and Service Level Agreements

1.1 Conformity with the National Security Scheme (in Spanish, ENS)

Note: In case of procurement of cloud services through an intermediary entity acting as a service provider (TENDERING or AWARDING ENTITY), but which does not own the systems that will provide the cloud services, it will be necessary to also require ENS compliance to the end systems providing the cloud services, owned by the end cloud service provider.

Considering the provisions of Article 29 of Royal Decree 3/2010, of 8 January, which regulates the National Security Scheme in the field of Electronic Administration, and the Resolution of 13 October 2016, of the Secretary of State for Public Administrations, which approves the Technical Instruction on Security in accordance with the National Security Scheme, which describes the obligation to require private sector operators providing services or solutions to public entities, In accordance with the National Security Scheme, the CONTRACTING ENTITY deems necessary that the suppliers participating in the tender in question shall exhibit the corresponding Statement of Conformity with the National Security Scheme (when the system category is BASIC), or the Certification of Conformity with the National Security Scheme (when the category is MEDIUM or HIGH).

Therefore, based on the above, and on the analysis of risks to which the services subject to the tender are exposed, the CONTRACTING ENTITY, establishes as necessary that the TENDERING ENTITY shall have the corresponding Statement or Certification of Compliance with the National Security Scheme, according to the relevant category of security, of the systems involved in the provision of the services indicated, and it should maintain the compliance in force during the term of the contract. In the event that the successful tenderer is unable to maintain compliance with the NSS - due to loss, withdrawal or suspension of the Compliance Certification or impossibility of maintaining the Compliance Declaration - it must communicate this circumstance immediately and without undue delay to the CONTRACTING ENTITY, which will consider the impact of this circumstance on the provision of the services covered by the contract.

When the contract covers, totally or partially, the use of on-premise systems (e.g. software), in accordance with the provisions of *the CCN-STIC Guide 858 Implementation of SaaS systems in local mode (on-premise*), the TENDERING ENTITY must provide the following documents: Installation Guide (addressed to administrators), the Secure Use Guide (addressed to users) and the Supplier-Customer Relationship Guide.

The AWARDEE assumes its obligation to comply fully with the National Security Scheme, and with the need for the information systems of those suppliers that are essential for the provision of the service covered by the contract to comply with Royal Decree 3/2010 of 8 January.

1.2 Confidentiality clauses

1.2.1 Recruitment confidentiality

Without prejudice to the provisions of Law 19/2013, of 9 December, on transparency, access to public information and good governance, and the provisions contained in Law 9/2017, of 8 November, on Public Sector Contracts, relating to the obligation to publicise the award and to the information to be given to candidates and tenderers, the contracting authorities shall not disclose the information provided by the TENDERING ENTITIES that has been designated as confidential by the latter when they submited their tender.

Confidentiality may concern, inter alia, technical or commercial secrets, confidential aspects of tenders and any other information the content of which could be used to distort competition, whether in the tendering procedure in question or in subsequent tendering procedures.

The obligation of confidentiality may not prevent the public disclosure of non-confidential parts of the contract, such as the settlement, the final deadlines for performance of the services, the identity of the successful tenderer or the essential parts of the tender, as well as subsequent modifications.

Likewise, all the documentation or information provided by the CONTRACTING ENTITY to the tenderers so that they have the information required to submit their corresponding offer is confidential and must be treated as such.

Once the contract is awarded, if the CONTRACTING ENTITY provides the AWARDEE ENTITY with additional information necessary for the provision of the services, such information shall be treated as confidential and shall be treated as such by the AWARDEE ENTITY and by any person involved in or related to the performance of the contract.

When the information submitted includes personal data, it will be necessary to consider the provisions in relation to Data Protection established in the regulations in force.

All persons involved in any stage of the tender process shall be subject to the duty of confidentiality referred to in Article 5.1.f) of the General Data Protection Regulation (EU) 2016/679 (GDPR).

All information processed, generated or relating to the execution of the contract must be processed in accordance with the provisions of the corresponding Tender Document and described in the section that regulates the processing of personal data on behalf of third parties. Otherwise, if no personal data processing is declared or it does not exist, the AWARDEE ENTITY entity shall return all the information to the CONTRACTING ENTITY or its designee at the end of the contract.

1.2.2 Confidentiality in the execution of the contract

The objective and temporary extension of the duty of confidentiality imposed on the AWARDEE ENTITY is determined in accordance with the provisions of Article 35.1.m) of Law 9/2017, of 8 November, on Public Sector Contracts. Therefore, the AWARDEE shall

be obliged to maintain full confidentiality and secrecy with respect to the information handled during the execution of the contract for 5 years from the date of knowledge of the information concerned, unless a different period is determined in the corresponding Tender Documents or in the subsequent contract.

For all purposes, "all information and documentation relating to the CONTRACTING ENTITY, as well as good internal uses, practices and procedures", which may come to the attention of the AWARDEE ENTITY in the performance of the contract, shall be considered confidential. The CONTRACTING ENTITY does not grant any rights to the AWARDEE ENTITY for access to its information system. In the same vein, confidentiality is granted to any information to which it has access during the execution of the contract, which has been given this status in the specifications or in the contract, or which by its very nature must be treated as such, including, expressly, all information associated with security and protection measures, developed configurations, service and application protections, elements and descriptions of infrastructure and architecture, authentication processes and security protocols, communications, incidents, third party reports, capacity controls and evaluations of the availabilities involved, automatic analyses, networks and perimeter protections, elements assigned to continuity, activity logs and associated protections, backup and restoration protocols, maintenance elements and guarantees involved, and any other elements that may be considered a risk for the purposes of the contracted service or the information linked to the same.

The AWARDEE ENTITY undertakes not to disclose, transfer or expose the information owned by the CONTRACTING ENTITY without its prior express written consent. Furthermore, the AWARDEE shall refrain from using the documentation and/or information known or provided during the execution of the contract for purposes other than the execution of the contract.

When the contract does not require access to the CONTRACTING ENTITY's information system but involves access to the facilities, the AWARDEE undertakes to maintain full confidentiality of the information that could be accidentally obtained through access to the facilities, and especially that which could pose a risk to the CONTRACTING ENTITY in case it becomes known and/or could lead to a breach of security.

When the information submitted includes personal data, it will be necessary to consider the provisions in relation to Data Protection, in the regulations in force and stated in the corresponding Tender Document. In the event that the procurement involves access by the AWARDEE ENTITY to personal data for whose processing the CONTRACTING ENTITY is responsible, the AWARDEE ENTITY and all persons involved in any phase of the procurement process shall be subject to the duty of confidentiality referred to in Article 5.1.f) of the General Data Protection Regulation (EU) 2016/679 (GDPR) and stated in this Tender Document. The AWARDEE ENTITY undertakes to enter into confidentiality agreements with the personnel assigned to the performance of the contract, and to maintain constant awareness and training.

1.3 Applicable data protection legislation

If the purpose of the service contained in the contract subject to tender requires the processing of personal data, the provisions of the General Data Protection Regulation (EU) 2016/679 (RGPD), in the Organic Law 3/2018, of 5 December, on Personal Data Protection and guarantee of digital rights (LOPDGDD) shall be met- with special incidence to the provisions of its First Additional Provision - and the remaining applicable regulations, as well as, where applicable, the provisions of Royal Decree-Law 14/2019, of 31 October, which adopts urgent measures for reasons of public security in matters of digital administration, public sector procurement and telecommunications, which shall be applicable to the AWARDEE ENTITY and its possible subcontractors, throughout the duration of the contract, regardless of the location of the systems involved in the provision of the services.

The purpose of the processing of personal data by the CONTRACTING ENTITY shall be to provide the services covered by the contract. The use of personal data for purposes other than those stated above shall constitute a breach by the AWARDEE ENTITY, which may result in the termination of the contract.

1.4 Declaration of location

As established in Law 9/2017, of 8 November, on Public Sector Contracts, considering the nature of the service, the AWARDEE ENTITY shall provide the identification of the location of the information systems linked to the services covered by the contract, including all the locations associated with the storage and provision of the service, contemplating all the activities involved, such as collection, storage, processing and management.

The AWARDEE ENTITY must identify all subcontractors that will participate in the performance of the services covered by the tender, both in the tender submitted and during the term of the contract, and must identify the location and the specific services provided by each of them. Subcontracting shall in all cases be subject to the provisions contained in the data protection regulations, without exception.

For all purposes, the limitations established in the data protection regulations relating to international data transfers shall be considered. Compliance with such provisions is an essential condition, which shall be extended to the subcontracted entities. This obligation is considered essential to the contract and shall be maintained throughout the term of the contract.

Any modification during the course of the contract relating to the requirements set out in this paragraph must be communicated without delay to the CONTRACTING ENTITY.

1.5 International Data Transfer

No transfers shall be made to a third country or international organisation outside the European Union, except in the cases specifically authorised by the General Data Protection Regulation (EU) 2016/679 (GDPR) and Organic Law 3/2018, of 5 December,

on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), the only exception being the transfer to countries, organisations or territories that have been declared to have an adequate level of protection by the data protection supervisory authorities, or when the transfer is necessary in compliance with a legal obligation, international agreement or court order.

The AWARDEE ENTITY shall communicate without undue delay any change in relation to the conditions for the transfer of personal data, especially the loss of the "adequate level of protection" for international transfers, in accordance with the GDPR. This expressly includes cases in which the Commission determines the loss of the adequacy of a country, organisation, entity or company, including those that no longer adhere to any international agreements that allow international data transfers.

1.6 Service associated with electronic identity verification

Considering the provisions of Law 39/2015, of 1 October, on the Legal Regime of the Public Sector, and in the event that the service tendered by the CONTRACTING ENTITY includes a system of identification by means of an agreed password for the purposes described in Article 9.2c) of the aforementioned law, it shall be necessary that the bids submitted by the TENDERING ENTITIES include or facilitate the identification of the location and provision of the service, as well as the technical resources that are going to be assigned for the collection, storage, treatment and management, which may only be located in the territory of the European Union, in accordance with the provisions of Article 122.2c) of Law 9/2017, of 8 November on Public Sector Contracts. Where special categories of data are involved, as provided for in article 9 of the General Data Protection Regulation (EU) 2016/679 (GDPR), the location shall be limited to the national territory.

To all intents and purposes, when the service tendered allows subcontracting, this shall be subject to the same terms as described above. Therefore, it will be necessary to expressly declare the location of the services or resources concerning the subcontracted processes. When there are several subcontractors, it will be necessary to declare this for each of them individually.

When the contract has already been awarded, and there is a modification that affects the location or provision of the service, including changes in subcontracting, the CONTRACTING ENTITY must be notified without delay, clearly identifying the changes made. This entitles the CONTRACTING ENTITY to terminate the contract.

The AWARDEE ENTITY shall in all respects be directly liable for any failure to comply with the subcontracting and for the declared obligations.

1.7 Processing of data of the types described in Article 46 bis of Law 40/2015

Considering the provisions of Article 46 bis of Law 40/2015, of 1 October, on the Legal Regime of the Public Sector and in cases where the service tendered by the CONTRACTING ENTITY affects data relating to the electoral roll, municipal registers of

inhabitants and other population registers, tax data related to own or assigned taxes and data of users of the National Health System, it will be necessary for the TENDERING ENTITIES to include in their offers the location and provision of the service, which may only be provided within the territory of the European Union.

To all intents and purposes, when the service tendered allows subcontracting, this shall be subject to the same terms as described above. Therefore, it will be necessary to expressly declare the location of the services or resources concerning the subcontracted processes. When there are several subcontractors, it will be necessary to declare this for each of them individually.

When the contract has been awarded, and there is a modification that affects the location or provision of the service, including changes in subcontracting, the CONTRACTING ENTITY must be notified without delay, clearly identifying the changes produced, being the CONTRACTING ENTITY entitled to terminate the contract.

The AWARDEE ENTITY shall in all respects be directly liable for any failure to comply with the subcontracting and for the declared obligations.

1.8 Contract termination regulation: Technology transfer

During the execution of the contract, the AWARDEE ENTITY undertakes to provide the persons designated by the CONTRACTING ENTITY with all the information and documentation requested by them in order to have full technical knowledge of the circumstances in which the services are developed, their activities and, in general, all the technical operations, as well as possible problems that may arise and the technologies, methods and tools used to solve them.

After the end of the contract, the CONTRACTING ENTITY shall develop the necessary actions for the transfer of the knowledge and information involved in the service. The process shall include, necessarily and at the request of the CONTRACTING ENTITY, the return of all the information to the CONTRACTING ENTITY itself or to whoever is designated by it, within a maximum period that will be determined in the corresponding Tender Document, by means of the necessary secure means and the information must be in a format that will be determined in the corresponding Tender Document.

For the technology transfer and restitution process, the successful AWARDEE ENTITY shall submit a detailed plan, including the means to be used, the contingency actions designed and the risks that may arise in the process. When necessary, and especially when there is a new awardee entity, the transition period for the organised management of the transfer and restitution process shall be included.

For the purposes of compliance with current data protection regulations, the legal retention periods that may be mandatory for the awardee entity shall be taken into account.

This clause will be mandatory when the service is terminated early, with the outgoing awardee being responsible for an orderly transfer and restitution.

1.9 Management of data backup and restoration

The AWARDEE ENTITY shall have the necessary mechanisms in place to implement a backup and recovery testing policy that includes at least the following requirements:

- Identification of the scope of backups.
- Backup policy.
- Encryption measures for backup information.
- Procedure for requesting backup restorations.
- Carrying out restoration tests.
- Transfer of backups (if applicable).

1.10 Disaster recovery management (continuity plan)

To ensure the continuity of the services covered by the contract, the AWARDEE ENTITY shall have and submit a contingency recovery plan. This plan shall be activated in the event of total or partial unavailability of the main resources, which for any reason causes the unavailability of the services covered by the contract. This plan shall include:

- Identification and description of planned alternative means of service provision, alternative personnel, existence or planning of alternative facilities and means of communication, etc.
- At least one recovery test per year. The final test report must be sent to the person in charge determined by the CONTRACTING ENTITY, as well as a work plan with corrective actions if events or actions to be corrected are detected.
- Updating disaster recovery plan documentation as necessary.

1.11 Standard Service Level Agreement

1.11.1 Scope of services

Without prejudice to the provisions of the corresponding Technical Specifications, the AWARDEE ENTITY shall include in its tender the planned timetable for the provision of the service covered by the contract (e.g. "24 hours a day, 365 days a year", etc.).

In the service level agreement section, the accepted range for each of the indicators described above shall be established, with the exception of the ranges established for maintenance windows.

1.11.2 Communications and incidents

All communications related to the services or to the corresponding Service Level Agreement shall be made by the areas or departments of the CONTRACTING ENTITY declared for that purpose in the corresponding Tender Document.

The tender documents shall also indicate the medium to be used for communications (e.g. e-mail and/or telephone calls, etc.).

It is mandatory that the service provided by the CONTRACTING ENTITY has an operational record of the requests or notifications made by the CONTRACTING ENTITY, using, where appropriate, the tool indicated in the corresponding Tender Documents. For all purposes, this record shall also register incidents and requests, and shall comply with the provisions of the data protection regulations.

1.11.3 Required Service Levels

1.11.3.1 Availability of contracted services

The AWARDEE ENTITY shall provide the following information in its tender:

Indicator 1: ensure availability of contracted services.

Indicator description: percentage of time that services have been active and providing service.

Unit of measurement: percentage.

Metric: I1= Tp-Tc/Tp*100.

- **Tc:** Total time, measured in minutes, that services are out of service during the measured period.
- **Tp:** Total time, measured in minutes, of the measured period.

Minimum frequency of analyses: monthly.

Target value: > 99,5 %.

Penalty: 1.3% of the billing for that period.

1.11.3.2 Availability of contracted services (special conditions)

Indicator 3: guarantee the availability of the contracted services in a certain time slot, e.g. daytime hours 07:00 to 22:00.

Indicator description: percentage of availability of services during daytime hours (07:00 to 22:00 hours) during the measured period.

Unit of measurement: percentage.

Metric: I3= 900-Tc/900*100.

- **Tc:** Total time, measured in minutes, in which services are out of service during the measured period from 07:00 to 22:00 hours.

Minimum frequency of analyses: monthly.

Target value: > 98 %.

Penalty: 1.3% of the billing for that period.

1.11.3.3 Storage availability

Indicator 4: Ensure availability of storage.

Indicator description: percentage of time the storage has been active and providing service.

Unit of measurement: percentage.

Metric: I4= Tp-Tc/Tp*100.

- **Tc:** Total time, measured in minutes, that the storage is out of service during the measured period.
- **Tp:** Total time, measured in minutes, of the measured period.

Minimum frequency of analyses: monthly.

Target value: > 99,5 %.

Penalty: 2.5% of the billing for the period.

1.11.3.4 Troubleshooting, problem solving

Indicator 5: maximise the number of incidents, problems solved.

Indicator description: percentage of incidents, problems accepted and solved.

Unit of measurement: percentage.

Metric: I5= Nr/Nt*100.

- **Tr:** number of incidents, problems solved during the measurement period
- **Tp:** total number of incidents, problems that were open at the beginning of the measurement period plus those that were opened during the measurement period.

Minimum frequency of analyses: monthly.

Target value: > 95 %.

Penalty: 3.2% of the billing for the period.

Incidents and service requests shall maintain a flow with the notifier and shall be closed when they have been communicated to the notifier and no further action is considered.

It will necessarily be included in the register:

- Time at which the incident starts and ends (including the time at which the incident occurs, the time at which it is reported and the time at which the resolution is completed).
- Start reporting time and end reporting time.
- Resolution times.
- Conclusions and improvement.

In this regard, the points required by the applicable regulations for the identification, management and registration of incidents that may affect the

service, which will be agreed with the CONTRACTING ENTITY, will be taken into account.

The AWARDEE ENTITY shall resolve incidents that are properly reported in a given time, as defined in the corresponding tender documents:

- Critical incidence: (For example: 1 working hour or 4 non-working hours).
- Major incident: (For example: 2 working hours or 12 non-working hours).
- Minor incidence: (For example: 3 working hours or 72 non-working hours).

Data will be collected to assess the incident management system, allowing to know the number of security incidents handled (and specifically):

- Time taken to close 50% of incidents.
- Time taken to close 90% of incidents.

Annually, these values shall be collected in a report submitted to the CONTRACTING ENTITY.

1.11.3.5 Resolution of requests for changes and/or updates

Indicator 6: Encourage the correct implementation of changes and/or updates.

Indicator description: percentage of hardware/software installations, changes and upgrades successfully executed and with a maximum resolution time of 2 days.

Unit of measurement: percentage.

Metric: I6= Nr/Nt*100

- **Nr:** number of changes and/or updates correctly executed and with a maximum resolution time of 2 days during the measurement period.
- **Tp:** of changes and/or updates during the measurement period.

Minimum frequency of analyses: monthly.

Target value: > 99 %.

Penalty: 4.5% of the billing for the period.

The necessary tests will be scheduled and, where appropriate, after agreement with the CONTRACTING ENTITY, generating the least possible impact on the operation of the service. All technical stops of the service shall be at times previously agreed with the CONTRACTING ENTITY.

1.11.3.6 Availability of backups

Indicator 7: Ensure availability of backups.

Indicator description: percentage of planned backups that have been successfully executed.

Unit of measurement: percentage.

Metric: I7= Np-Nf/Np*100.

- **Nf:** number of backups planned and not successfully completed during the measured period.
- **Np:** number of planned backups during the measured period.

Minimum frequency of analyses: monthly.

Target value: > 99,9 %.

Penalty: 2.5% of the billing for the period.

1.11.3.7 Reliability of data recovery

Indicator 8: ensure the reliability of data recovery.

Indicator description: percentage of data recovery from successfully executed backups.

Unit of measurement: percentage.

Metric: I8= Nr/Nt*100.

- **Nr:** Number of backup restores successfully completed during the measured period.
- **Np:** number of restores from backups requested during the measured period.

Minimum frequency of analyses: monthly.

Target value: > 99 %.

Penalty: 2.5% of the billing for the period.

1.11.3.8 Activation of the backup service

Indicator 9: ensure a maximum activation time of the back-up service for the indicated services.

Indicator description: time consumed in starting up the backup service.

Unit of measurement: time measured in hours.

Metric: I9= Ta.

- **Ta:** time measured in hours, spent in preparing the backup service to provide a correct service, during the measured period.

Minimum frequency of analyses: monthly.

Target value: < 24.

Penalty: 2.4% of the billing for that period.

1.11.3.9 Availability of contracted capacity

Indicator I10: manage contracted capacity.

Indicator description: to ensure that the contracted capacity thresholds are not exceeded, establishing a threshold at which it will be necessary for the AWARDEE

ENTITY to notify the CONTRACTING ENTITY in order to authorise the increase in resources.

Unit of measurement: time measured in days.

Metric: I10= Ta.

- **Ta:** time measured in days to report that the 85% threshold in usage of contracted resources has been exceeded, during the measured period.

Minimum frequency of analyses: monthly.

Target value: <= 30.

Penalty: 2.5% of the billing for that period.