
Project title:

Partnerships for Sustainable Trade (PST)

Annex on Information Security

The Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH operates an Information Security Management System (ISMS) and is planning certification to ISO/IEC 27001 which will be maintained. Certification always documents implementation of the current version of this standard.

The following information security regulations apply to service delivery:

1 Handling confidential data

Any and all data relating to the contract as well as any other information, such as submitted documents and exchanged information, of which the contractor and its employees become aware in the course of performing the contract, shall be treated as confidential during and beyond the term of the contract. Furthermore, the need-to-know principle applies, i.e. such documents and information may be disclosed and made accessible only to persons to whom this information is absolutely essential for fulfilling their duties. This provision applies even if such documentation and information has not been explicitly designated as secret or confidential. Contractors shall not allow third parties to access documentation or work results of any kind, in particular reports, without the prior consent of GIZ in text form. Third parties under this provision also include the ultimate commissioning party/client. The contractor is also not permitted to use this data and information for its own purposes.

2 Regulations governing subcontractors

The contractor may only award contracts to completely reliable, qualified and competent tenderers under cost-efficient conditions and on the basis of competition. When conducting procurement, the contractor shall ensure transparency, equality of treatment, the eligibility of tenderers and sustainability. As far as possible, at least three tenders should be obtained.

Procurements above the most recently defined EU threshold for contracts for goods and services are subject to the latest versions of both the Act Against Restraints on Competition (GWB) and the Regulation on the Award of Public Contracts (VgV), if the contractor procures the goods or services in the European Economic Area. For procurements outside the European Economic Area, these rules shall be applied by analogy.

The contractor's obligations to provide work and services shall remain unaffected in the event that the contractor commissions third parties to provide subcontracted work and services. Any subcontracting of work and services by the contractor to third parties shall require GIZ's prior approval in text form, unless the contract stipulates that such work or services be procured by the contractor. The contractor shall undertake to ensure that the subcontractors it uses comply with the provisions of these Terms and Conditions.

3 Reporting security incidents

The contractor shall inform GIZ (informationsecuritymanagement@giz.de) without delay and in an appropriate form about information security incidents which (also) affect GIZ information.

An information security incident is an event that may have – or already has – negatively impacted information security, for example through unauthorised viewing/disclosure of information (loss of confidentiality), modification of information (loss of integrity) or deletion of information/disruption of access to information (loss of availability).

4 Retaining GIZ-related records, contract termination

The contractor shall retain contract-related records and work results, including financial records, for ten years after acceptance of the final report or, as the case may be, of the work. They shall be returned at GIZ's request.

Upon termination of the contract, the contractor shall return any other records, aids, materials and objects, which were passed to the contractor by GIZ on a non-permanent basis as intended, without delay and without being prompted to do so. This provision shall also apply to any copies of such items.

In the above-mentioned cases, the return shall follow a procedure defined by GIZ. GIZ is also entitled to request secure (i.e. not re-constructible) erasure or destruction, either in whole or in part. Evidence of the erasure and the erasing procedure used shall be provided to GIZ upon request, e.g. in a written declaration. There shall be no additional remuneration.

Statutory retention obligations and periods shall remain unaffected by this provision.

5 Qualifications and requirements for the assigned experts

The contractor shall be obliged to assign only such experts as are trustworthy and capable of performing the tasks allocated to them, who have the necessary professional and local knowledge, and are adequately informed of and prepared for the security situation in the country of assignment. The contractor shall ensure that the experts assigned are appropriately informed of the contractual regulations governing information security. If participation by the contractor and/or its experts in special preparatory courses is agreed, the preparation period shall not form part of the period of assignment.

6 Access to information

The contractor may access only the information specified in the context of service delivery by analogue or technical means.

Access to areas and information not thus specified is prohibited.

If necessary, GIZ shall specify how the contractor is to handle metadata (bearing in mind the need-to-know principle relating to confidentiality).

7 Use of devices

When devices are used in the course of performing the contract, the contractor shall ensure that the place of use is properly secured and that unauthorised third parties cannot use them. Measures shall also be taken to ensure that unauthorised third parties cannot see any GIZ-related information (e.g. by applying privacy filters).