

Request for quotations, INFORMATION SECURITY POLICY

1 ABOUT THE SWEDISH COMMITTEE FOR AFGHANISTAN

The Swedish Committee for Afghanistan (SCA) is an aid organisation that has worked in Afghanistan since 1982. We carry out development projects in the area of education, healthcare, rural development, and rehabilitation of persons with disabilities. SCA has about 5500 employees, 99% of whom are Afghans. Our operations are especially directed to the most vulnerable groups in the society and are always carried out in close cooperation with the local society.

We mainly work in the poor rural areas of Afghanistan with a special focus on women, children, and persons with disabilities. The work with human rights and gender issues is central to SCA and permeates the entire organisation. In Sweden, SCA has about 12,000 members and monthly sponsors as well as an office in Stockholm with about 24 employees.

SCA is a political and religiously independent aid organisation that is funded by thousands of individuals, SIDA, EC, and the World Bank. The member-based organisation was established in 1980.

2 BACKGROUND

SCA is in need of an information security policy to protect its data and other IT assets, and networks from unauthorised users.

2.1 SCA's ICT infrastructure

SCA is operating in two countries, Afghanistan, and Sweden. Users in both locations are using a joint Office 365 services that includes Exchange, the Office package, SharePoint, OneDrive, Microsoft Teams, Planner, etc.

In Afghanistan, the Kabul Management Office (KMO) has a corporate network connected with the five Regional Management Officers (RMOs). There are 14 servers available at KMO providing various services such as file storage and printing, Active Directory (AD), Additional Activate Directory, DHCP, WDS, WINS, backup executive server for user data and critical system server states, firewalls that filter all incoming and outgoing data traffic and provide KMO with connectivity to the RMOs. Each RMO has its own Kaspersky endpoint security central server configured with different policies that protect individual workstations. They also house read-only domain controllers (RODC) that allow the RMOs to locally authenticate their domain accounts.

In Sweden, the Stockholm Management Office (SMO) has outsourced its data centre to a local service provider that hosts servers such as active directory and application server for the applications Visma & iSCALA. The local service provider provides support services for wired and wireless networks (LAN & WLAN) and firewall on local premises in SMO. The Office 365 services are managed locally by the ICT Coordinator.

2.2 List of key applications:

Sweden

- Office 365
- iScala (bookkeeping and budget)
- KomMed Cloud (CRM system for members and donors)
- Visma Lön (salaries)
- Centsoft (invoicing)
- QBank (image bank)
- 23 minor applications of various sorts

Afghanistan

- iScala (bookkeeping and budget)
- Personec (HR administration)
- QBank (image bank)

Procuring organisation is the **Swedish Committee for Afghanistan** (SCA, Swedish organisation number 802010-4850).

This procurement will be done by a price comparison process with this Request for Quotations (RfQ) having been communicated by direct request to at least 3 potential suppliers. The RfQ has also been announced on SCA's official website (swedishcommittee.org/about/bidannouncements).

2.3 Method of evaluation

Evaluations of quotations will be done in three stages:

1. Evaluation of administrative requirements
2. Evaluation of technical requirements
3. Financial evaluation

The methods for evaluation of each stage are described in more detailed below under their respective headings.

3 DESCRIPTION OF THE ASSIGNMENT

The supplier should develop an information security policy based on ISO/IEC 27001. The policy should take into consideration SCA's handling of personal data in adherence with the EU General Data Protection Regulation (GDPR).

The policy should generally apply to SCA's operations in both Afghanistan and Sweden. Where necessary, aspects specific to either country should be specified, for example in relation to physical infrastructure, internet availability, legislation, etc.

3.1 Policy contents

3.1.1 Confidentiality

The supplier should review SCA's current ICT infrastructure, IT platforms and data and classify them in terms of confidentiality, i.e. highly confidential, restricted, and public.

The policy should also classify the following:

- Who should have access to each level of classified data?
- Access rights on ICT infrastructure and IT platforms.

3.1.2 Availability

The policy should include a set of rules that ensures users have access to the systems and the resources they need at any time.

3.1.3 Integrity

The policy should set a clear rule that the data is protected from unauthorised changes to ensure that it is reliable and correct.

3.1.4 Security operations

The policy should clearly describe the procedures and guidelines to support the core IT services of SCA. This should cover the following:

- Physical and logical security of ICT assets
- Procedure for data transfer internally and externally (encryption, data transfer protocol, etc.)
- Password policy
- Intrusion and detection procedures
- Virus protection procedure
- Procedure for Firewall maintenance and updating
- Logs and auditing procedures

3.1.5 Third party service providers

The policy should cover the engagement of SCA's external service providers to ensure the confidentiality, integrity, and availability of the provided services. The policy can be varied between Afghanistan and Sweden where applicable.

3.2 Method

The supplier is not expected to make physical visits to SCA's offices but will have access to all relevant documentation in digital form. The SCA contact for the assignment will be stationed in SCA's Stockholm office.

The supplier is expected to write the policy in English and submit it to the contact person at SMO. After the policy has been submitted, the supplier should provide a presentation that explains the policy to the key staff of SCA a total of 10 users.

3.3 Timeline

We expect the policy to be finalised and approved by 18 December 2020.

The assignment should be finalised with a presentation of the policy for key SCA staff (about 10 individuals) no later than 28 January 2021.

4 ADMINISTRATIVE REQUIREMENTS

All requirements under this heading are mandatory. Only quotations that live up to all these requirements are eligible to proceed to the next stage of evaluation.

4.1 Submitting a quotation

Your quotations shall be sent to SCA by e-mail to peter.isotalo@sak.se. Quotations must be sent as attachments in PDF format no later than 25 September 2020 at 15.00 o'clock (Central European Time). Write "SMO 2020-39, Information Security Policy" as the subject.

4.2 Proof of tax registration

SCA will only accept quotations from suppliers that are tax registered. In the quotation, this must be documented by including either a Swedish VAT registration number (*momsregistreringsnummer*), or equivalent proof of registration in other countries.

4.3 Conditions for payment

Payment will be made 30 days after receiving an invoice. SCA will only accept digital invoices. Invoices can be made as *e-faktura*, or as PDF files sent by e-mail. All payments must be in Swedish kronor (SEK).

Invoices from the Supplier shall include a clear description of the goods or services to be reimbursed. Invoices shall also include the full name of the Supplier, invoicing address, name of SCA's contact with the Supplier, SCA's contract number, and any budget codes specified by SCA to the Supplier. The currency must be specified on all invoices. For payment within Sweden, Postgiro or Bankgiro number must be provided. For payment outside of Sweden, account numbers and any other information necessary to execute payment must be provided.

4.4 Immaterial rights

SCA shall have full ownership of the results of the Assignment, including the right to use the results in its own name. The Supplier shall not use the results of the Assignment without prior written approval by authorised signatory of SCA.

4.5 Confidentiality

Suppliers may not divulge to a third party any confidential information that has been shared with suppliers by SCA, or any information that has been obtained while completing assignments.

Suppliers must guarantee that confidential information that has been obtained throughout the assignment shall not be shared with third parties, either during the duration of this contract, nor after its termination or expiring.

4.6 Personal data processing agreement

If it is deemed relevant for the service being procured by parties submitting quotations, a standard suggestion for a personal data processing agreement may be provided as part of the quotation.

4.7 Price quotation

The price for the total cost of the assignment must be clearly specified, as well as a break-down of individual costs. The quoted price must include all expenses that a supplier deems necessary to fulfill the assignment.

All prices must be quoted in SEK.

5 TECHNICAL REQUIREMENTS

Under this heading, the requirements specified for the services by SCA will be specified. All requirements specified under this heading are mandatory. Only quotations that fulfill the minimum requirements are qualified for final evaluation.

5.1 Certification

The supplier must provide documentation that they are certified to perform information security analyses according to ISO/IEC 27001.

5.2 Qualifications and experience

The staff that will work on the assignment should have the following qualifications:

- Extensive experience of working with NGOs (non-governmental organisations) or similar organisations.
- Previous experience where the consultant has carried out at least three similar assignments.

Documentation of the supplier's staff qualifications must be included in the quotation.

5.3 Planning

The quotation must include a workplan for the completion of the assignment in line with the description of the assignment above.

6 FINANCIAL EVALUATION

After evaluation of the technical requirement there is the final financial evaluation. Quotations that have fulfilled all the technical requirements are qualified for financial evaluation. The quotation with the lowest overall cost for the requested services will be offered a contract by SCA.