TERMS of REFERENCE
for
Cyber/Digital Security Specialist

Ref. no RS-NCD-96040YF-CS-IC-25-4.30

Background

The Republic of Serbia has received financing from the World Bank in the amount of EUR 70,700,000 equivalent towards the cost of the Serbia Noncommunicable Diseases Prevention and Control Project (SNDPCP), and intends to use part of the proceeds for payments of goods, works, non-consulting and consulting services to be procured under this project.

The PDO of SNDPCP is to contribute to improving health system effectiveness in addressing NCDs in Serbia.

The activities to be financed by SNDPCP are structured into five components:

Component 1: Improving Provider's Competence and Accountability. This component supports improvement in the competence of general practitioners in prevention and management of NCDs, strengthening capacity of PHC facilities to provide patient management by joint teams of GPs and outpatient specialists, establishment of telemedicine services and further digitalization and integration of medical records, establishment of palliative care capacities for patients with NCDs, and implementation of payment models for outpatient, inpatient and palliative care that improve accountability of health care providers for results.

Component 2: Increasing Availability of Services. This component supports upgrading health care infrastructure to improve availability of diagnostic and treatment services, with focus on expanding access to people living in rural areas. The component finances equipment, infrastructure improvements and mobile vehicles. It supports reforms of rationalization of health facilities network proposed by the Masterplan developed under Second Serbia Health Project. It also finances strengthening of health system IT infrastructure, and data analytics for policy making.

Component 3: Strengthening Quality of Public Health and Clinical Services. This component supports development of the national programs for prevention and control of NCDs, implementation of the national Health Care Quality Improvement Plan, good practice guidelines and clinical pathways for NCDs, and improving quality of primary prevention of NCDs through targeted behavior change campaigns.

Component 4: Project Management, Monitoring and Evaluation. This component will support overall project administration, including project management, fiduciary functions, environmental and social compliance, and regular monitoring of and reporting on implementation.

Component 5: Contingency Emergency Response. The objective of this component is to improve the Government's response capacity in the event of an emergency. The component would support a rapid response to a request for urgent assistance in respect of an event that has caused, or is likely to

imminently cause, a major adverse economic and/or social impact in the health sector associated with natural or man-made crises or disasters. In such a case, funds would be reallocated from other components into this one to finance goods and consulting services.

The Project is being prepared under the World Bank's Environment and Social Framework (ESF), which came into effect on October 1, 2018, replacing the Bank's Environmental and Social Safeguard Policies.

Scope of Work

The overall objective of the assignment is to assist the Ministry of Health (MoH) in protecting digital health solutions to be implemented by the identifying threats and vulnerabilities.

The main activities of this assignment include, but are not limited to the following:

- Engaging in the design and implementation of digital health solutions to be implemented by the Project to ensure that they are protected from threats and vulnerabilities. The primary focus is on safeguarding data and ensuring the integrity, confidentiality, and availability of digital resources.
- Assessing potential security risks and vulnerabilities in digital infrastructure and data related to digital health solutions to be implemented by the Project.
- Securing computer networks by configuring firewalls, intrusion detection systems, and monitoring network traffic.
- Evaluating incident response and disaster recovery plans related to digital health solutions to be implemented by the Project.
- Providing cyber security related capacity-building workshops and other activities for the Project team.
- Assessing and monitoring cyber security practices of third-party vendors and service providers. Ensuring that contracts with third parties include cyber security clauses and compliance requirements.
- Implementing data encryption, access controls, and backup solutions to protect sensitive information.
- Conducting security awareness programs to educate Project team and stakeholders about cyber security best practices.
- Identifying and patching vulnerabilities in software and hardware, and keeping systems up to date.
- Keeping up with the latest threats and security trends and applying patches and updates as necessary.
- Analyzing potential risk related to IT activities on the Project.
- Cooperating with Data protection Specialist to ensure comprehensive data protection and security measures.
- Performing any other tasks as directed by the PCU Coordinator and/or officials from the Ministry of Health.

Duration of the assignment

This is a part-time position. The consultant will be engaged until the end of the project (March 31, 2029), after a three-month probation period. It is expected that the Consultant would be engaged for 10 working days a month (on average).

Qualifications and requirements

- Bachelor's or Master's degree in Computer Science, Information Security, or a related field
- Minimum 10 years of work experience in IT sector
- Knowledge of MoH's, HIF's and IPHS's information system is advantage
- Proven experience of five years in the last 10 years implementing cyber security solutions in governmental or healthcare systems is required
- Good command of written and spoken English and Serbian language
- Previous experience in projects financed by the World Bank or the IFIs would be an advantage
- Certificates regarding cyber/digital security (CISSP, CISM, CISA, or equivalent) is required
- Related certifications and related experience such as HCISPP, ISO/IEC 27001, NIST or CCNA certificate are advantage

The evaluation of the candidates will be based on the following selection criteria:

- Specific experience relevant for the assignment 60 points
- Qualifications for the assignment 40 points

Reporting requirements

The consultant shall report to the PCU Coordinator and the Ministry of Health officials as required.

The consultant shall submit the following reports:
Monthly comprehensive reports which will be the basis for payment and will be submitted at the end of each month.
Ad hoc reports as requested by the PCU Coordinator, and/or the Ministry of Health.

All reports should be submitted in English and/or Serbian language, as required.