

**PUBLIC CALL FOR NATIONAL PROFESSIONALS FOR PARTICIPATION IN**

**TRAIN-THE-TRAINERS PROGRAM ON CYBERSECURITY FOR MSMEs**

May 2024

1. **BACKGROUND INFORMATION**

In light of Bosnia and Herzegovina's increasing reliance on information and communication technologies (ICTs), cybersecurity emerges as a critical concern impacting various sectors of society. The inadequacy of localized responses to these threats underscores the necessity for international cooperation and the development of robust cybersecurity frameworks.

Despite the imperative nature of cybersecurity, Bosnia and Herzegovina faces significant challenges in this domain. The absence of a comprehensive legislative and strategic framework for cybersecurity, encompassing areas such as cybercrime prevention, data management and protection, online safety for children, and privacy safeguards, leaves the nation vulnerable to emerging threats. These gaps were underscored in the European Union's 2021 Progress Report for Bosnia and Herzegovina, which highlighted the country's insufficient capacity to address cybersecurity threats effectively.

The private sector in Bosnia and Herzegovina, particularly micro, small, and medium-sized enterprises (MSMEs), that forms backbone of the country's economy comprising 97% of all registered businesses, confronts various vulnerabilities. Limited resources inhibit MSME ability to invest in robust cybersecurity measures, while outdated technology infrastructure exacerbates these challenges. SMEs' position within supply chains renders them susceptible to attacks aimed at disrupting critical business operations. The absence of formal security policies leaves SMEs without clear guidelines for protecting their digital assets, leaving them particularly vulnerable to cyberattacks.

Additionally, a lack of awareness among SMEs about cybersecurity risks and best practices further compounds their vulnerability. The digital maturity of these enterprises in terms of cybersecurity readiness remains alarmingly low. In response to the challenges posed by the COVID-19 pandemic, UNDP in Bosnia and Herzegovina developed the Digital Pulse, a self-assessment tool aimed at evaluating the digital maturity of companies across six key business areas, including cybersecurity. Analysis of response data from over 400 companies revealed a glaring lack of systemic approaches to cybersecurity, with nearly 90% of businesses lacking proper measures. Additionally, approximately 70% of MSMEs lack a robust data backup system, relying instead on basic antivirus and firewall software bundled with their operating systems. Moreover, 65% of respondents expressed doubts regarding the cybersecurity competencies of their employees.

These findings underscore the urgent need for enhanced cybersecurity awareness and training among MSMEs in Bosnia and Herzegovina. Addressing these concerns, UNDP's Sustainable Growth Sector, in collaboration with the Czech-UNDP Partnership for SDGs, aims to launch a pilot initiative in 2023 and 2024. The primary objective of this initiative is to bolster cybersecurity awareness and resilience of MSMEs by providing comprehensive training to selected companies and trainers from relevant institutions across the country.

The initiative will also offer technical assistance to participating companies, enabling them to identify key cybersecurity risks and implement preemptive measures to enhance their overall cybersecurity posture. By bridging the existing skill gaps and fostering a culture of cybersecurity awareness, this program seeks to empower MSMEs to navigate the evolving cyber threat landscape effectively.

1. **PURPOSE OF THIS PUBLIC CALL AND EXPECTED RESULTS**

This public call is open to all nationals of Bosnia and Herzegovina who fulfill the required criteria and have demonstrated interest to participate in the training programme envisaged under this Public Call.

The aim of the training-of-trainers programme is to establish a national cohort of cyber-security MSME trainers from relevant training centers who can offer training and advisory services to private sector companies and support them in strengthening their cyber-security resilience.

The training will gather 10 consultants/trainers, and will cover three modules spanning over 5 days, including:

* Day 1: Introduction to Cybersecurity for Trainers
  + *Let’s get everyone on the same fundamental knowledge level.*
  + Fundamental terminology and concepts: CIA Triad, Risk Management
* Day 2: Micro, small and Medium Enterprise Risks, Threats & Mitigations
  + *The most common threats for MSME and how to mitigate them with limited resources.*
  + People, Process and Technology recommendations e.g. Security Awareness, 3rd Party Management, Incident Planning and Response, Patching, Security Monitoring and more.
* Day 3: Technical Audits and Processes to be executed in MSME
  + Run these technical audits in your enterprise to discover fundamentals security gaps
    - Active Directory Security Audit
    - External Attack Surface Audit
    - Asset Security Baseline Audit
* Day 4: Tools for MSME & Daily Security Operations
  + Affordable security solutions for your business to deploy and leverage.
    - Manage daily Security Operations with Wazuh XDR.
    - Run your own educational phishing campaigns with GoPhish
* Day 5: Expanding Topics & Wrap-Up (IoT Security, EU Legislation Briefly, Cybersecurity Trainings and more)

This training-of-trainers aims to enable business development support organizations (BDSOs) providers to provide dedicated cyber security training and consulting to MSMEs, thus improving their service line offer to the private sector. BDSOs will receive a package of ready-to-use learning materials based on the cybersecurity curriculum developed for MSMEs and a methodological approach and guidance to perform MSMEs' cybersecurity risk assessments and analysis with security recommendations.

The training program is designed to equip future trainers with the materials, concepts, and understanding necessary to address the complex cybersecurity issues faced by MSMEs. To fully comprehend these complexities, participants are expected to engage in further reading and practice both during and after the training.

After successfully completing the training, all participants will receive a formal certificate of completion.

1. **ELIGIBILITY, REQUIREMENTS AND THE SELECTION PROCESS**

The selection of participants of ToT Program on Cyber Security for MSMEs will be conducted on the basis of mandatory and additional qualitative criteria.

As part of the **mandatory (elimination) criteria,** theApplicants must fulfill the following:

* **Education:** Applicants are required to hold a minimum of a high school diploma or bachelor’s degree in Computer Science, Information Systems, or a related technical field.
* **Experience:** Applicants are required to have proven track record of supporting businesses or providing trainings and/or technical assistance to businesses.
* **Language requirements:** Applicants are expected to be in good command of English language.

Applications that do not meet the mandatory criteria will not be further considered.

Once the applicant's compliance with the mandatory criteria has been confirmed, **additional qualitative criteria** will be evaluated, focusing on the applicant's motivation and relevant experience. This assessment will be conducted in accordance with the following scoring table:

|  |  |
| --- | --- |
| Qualitative criteria – scoring table | |
| **MOTIVATION OF THE APPLICANT** | Max no. of points 20 |
| What is the motivation for applying?  *Strong motivation demonstrated through clear goals and enthusiasm (15 points); Lack of clarity in motivation (0 points).* | 15 |
| Does the applicant demonstrate an interest in leadership and fostering the local professional cyber-security community?  *Notable interest (5 points); Low interest (0 points)* | 5 |
| **EXPERIENCE OF THE APPLICANT** | Max no. of points 35 |
| How experienced is the applicant in providing technical assistance or educational services to MSMEs?  *Extensive experience (15 points); Some experience (10 points); No experience (0 points).* | 15 |
| Is the applicant affiliated with education centres or other bodies providing technical assistance or education to MSMEs?  *Affiliated (10 points); Not affiliated (0 points).* | 10 |

The decision to reject the application or not to select the applicant may be based on one or more of the following reasons:

* The application was received after the submission deadline;
* The applicant does not meet the basic requirements of the Public Call;
* The application is incomplete or otherwise does not meet the requirements;
* The application meets the conditions and criteria but was not selected due to a low score and/or after the application of basic selection criteria.

The top 10 ranked applicants will be included in this ToT program.

If a higher number of applicants have the same score, priority will be given to those that are better rated in the MOTIVATION OF THE APPLICANT section.

Applicants will be notified of the results of the public call via e-mail.

The indicative timeframe for finalizing the selection process and the delivery of ToT on cyber-security for MSME is as follows:

|  |  |
| --- | --- |
| **Activities** | **Dates (indicative)** |
| **Call for partcipation in ToT Program on Cyber Security for MSMEs published** | May 28 2024 |
| **Deadline for submitting applications** | June 10 2024 |
| **Public Call results published** | June 14 2024 |
| **First module of ToT delivered** | June 20 & 21 2024 |
| **Second Module of ToT delivered** | June 27 & 28 2024 |
| **Third Module of ToT delivered** | July 5 2024 |

1. **SUBMISSION**

The deadline for submission of applications is June 10 2024.

As part of the submission, each applicant must submit the following documents:

* Curriculum Vitae (CV) with relevant professional experience
* Copy of university diploma
* Filled-in and signed application form

All applications must be submitted by email to [**registry.ba@undp.org**](mailto:registry.ba@undp.org)with the subject line "Application for participation in train-the-trainers program on cybersecurity for MSMEs".

Incomplete applications shall not be taken into consideration.

1. **Additional information**

The Public Call with guidelines and application documents is available on the UNDP BiH website: www.ba.undp.org.

All inquiries regarding this Public Call must be submitted exclusively via email, no later than 2 days before the deadline for submitting applications, clearly indicating the title of the Call in the subject line, to the following email address: to [registry.ba@undp.org](mailto:registry.ba@undp.org).