

**PUBLIC CALL FOR SMALL AND MEDIUM-SIZED ENTERPRISES FOR PARTICIPATION IN CYBERSECURITY TRAINING AND TECHNICAL ASSISTANCE**

**Guidelines for Applicants**

July 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 small, and medium-sized enterprises, that forms backbone of the country's economy comprising 97% of all registered businesses, confronts various vulnerabilities. Limited resources inhibit SME ability to invest in robust cybersecurity measures, while outdated technology infrastructure exacerbates these challenges.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 SMEs 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 SMEs 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 SMEs 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 programme seeks to empower SMEs to navigate the evolving cyber threat landscape effectively.

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

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

The aim of the programme is to assist SMEs in strengthening their cyber-security resilience. This includes enhancing their understanding of cyber threats and the severe consequences of inadequate resilience, while equipping participants with practical knowledge and skills to build robust defense mechanisms. During the programme, participants will have the opportunity to work with trained local cyber security experts, conducting practical analysis of their companies' cyber security posture. By fostering cyber security awareness and providing hands-on strategies, SMEs will be better equipped to safeguard their operations and reduce potential cyber security risks.

This Public Call encompasses two lots that companies can apply to:

**Lot 1: Fundamentals Cyber Security Training**

* Training on Cyber Resilience for Small and Medium-sized Enterprises: Fundamentals and Practical Strategies;
* This training will provide an introduction to cybersecurity and data privacy, covering fundamental concepts. It will address common threats faced by companies, including typical cyber-attacks like phishing, ransomware, and social engineering, as well as those specific to SMEs based on experiences from Czech and EU companies. Participants will learn about the development of cyber-attacks, how to recognize threats, and essential rules for protection, but also conduct SMEs' cybersecurity risk assessments and analysis with support of local cyber security experts, producing security recommendations;
* Each SME will have 2 participants: one in a managerial (decision-maker) role and one internal tech (IT) specialist;
* The expected training duration is 2 days. On the first day, participation is expected from both management and tech specialist roles. On the second day, only the presence of the tech specialist is anticipated.

**Lot 2: Intermediate Cyber Security Training**

* Business Cyber Defender Training;
* Training will comprehensively cover essential cybersecurity practices, including proper document backup procedures, secure remote access setups, and other necessary tools to safeguard SMEs' networks, systems, and data. It aims to empower participants in assuming the role of "Business Cyber Defender" within their companies. This includes enhancing their ability to identify cybersecurity risks and propose mitigation measures. Additionally, the training will focus on equipping them with skills to effectively communicate cybersecurity basics to their colleagues;
* Each SME will have 1 participant, a SME internal tech (IT) specialist;
* The expected training duration is 2 days.

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

After the training, selected SMEs will be provided with the opportunity to receive tailored technical assistance, offering high-level expertise to identify key risks in their business and take necessary preemptive actions to enhance overall cybersecurity. The selection will be based on their demonstrated motivation, involvement in conducting a cybersecurity maturity assessment, and readiness to commit resources to fully utilize the technical assistance. This assistance will be delivered online using relevant digital communication tools and channels.

**Note: Interested companies need to choose and apply to only one of the two available lots.**

The following results are expected through the implementation of this Public Call:

* Up to 15 SMEs from various industries have improved cyber security awareness and acquired cyber security fundamentals;
* Up to 15 SMEs from various industries have increased their internal capacities to Business Cyber Defender level;
* Up to 8 SMEs have received technical assistance, identified the main risks in their business, and undertaken the necessary preemptive actions to improve the overall cyber security.

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

Eligible SMEs for support under this Public Call are legal entities as follows:

* Registered as a business entity - d.o.o. (*proof: a copy of the registration of a company*);
* Registered on the territory of BiH (*proof: copy of latest company registration*);
* Have accrued profit in 2023 (*proof: 2023 financial statement provided*);
* Have more than 9 and fewer than 250 employees on the date of the publication of this Public Call (*proof: 2023 financial statement provided*);
* The company representatives are expected to be in good command of English language;
* The Internal Tech Specialist representing the SME is expected to possess a strong technical background (*proof: CV of an internal tech specialist*);
* The owner or responsible person does not hold a public office position or is employed in government institutions.

Ineligible applicants will not be further considered. Once the applicant's eligibility has been confirmed, **additional qualitative criteria** are evaluated, focusing on the applicant's motivation and cybersecurity relevance. This assessment will be conducted in accordance with the following scoring table:

|  |  |
| --- | --- |
| Qualitative criteria – scoring table | |
| **MOTIVATION** | Max no. of points 20 |
| What is the motivation for applying?  *Strong motivation demonstrated through clear goals and enthusiasm (20 points); Lack of clarity in motivation (0 points).* | 15 |
| Has the company had previous experience with cyber-attacks?  *Yes (5 points); No (0 points).* | 5 |
| **CYBERSECURITY RELEVANCE** | Max no. of points 20 |
| Is the company processing sensitive data that must be protected from unauthorized access to safeguard the privacy?  *Yes (5 points); No (0 points).* | 5 |
| How advanced is server infrastructure?  *Basic - minimal or no dedicated servers (0 points),*  *Intermediate - dedicated servers with moderate hardware specifications (3 points);*  *Enterprise - multiple servers or a data center (5 points)* | 5 |
| Does a company have external connections (VPN) with other entities (service providers, suppliers etc.)?  *Yes (5 points); No (0 points).* | 5 |
| Are there certain legal requirements that the company needs to fulfill that deal with cybersecurity?  *Yes (5 points); No (0 points).* | 5 |
| **OTHER** |  |
| Is one of applicant representatives a woman and/or youth?  *Yes (10 points); No (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 eligibility 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.

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 training on cyber-security for SME is as follows:

|  |  |
| --- | --- |
| **Activities** | **Dates (indicative)** |
| **Public call for SMEs for participation in Cyber Security Training and Technical Assistance for published** | 8 July 2024 |
| **Deadline for submitting applications** | July 17 2024 |
| **Public Call results published** | July 19 2024 |
| **Fundamentals training delivered** | July 24 & 25 2024  July 29 & 30 2024 |
| **Intermediate training delivered** | Aug 01 & 02 2024 |
| **Technical assistance delivered** | Aug to Oct 2024 |

1. **SUBMISSION**

The deadline for submission of applications is July 17 2024.

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

* Filled-in and signed version of the application form (in Word and PDF format);
* Registration of the legal entity with a clearly expressed current ownership structure (initial registration decision and current extract from the court register);
* Financial reports for the last year (2023), signed and certified by an authorized accountant. The reports should include the income statement, balance sheet, and cash flow statement;
* Signed declaration that the owner and the responsible person of the applicant do not hold public office;
* Curriculum Vitae (CV) of company representatives containing relevant professional experience
  + SME applying to Lot 1: CV for a management/decision-maker professional, and CV for an internal tech specialist;
  + SME applying to Lot 2: CV of an internal tech specialist;

All applications must be submitted by email to [**registry.ba@undp.org**](mailto:registry.ba@undp.org). 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](http://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)**.**