Project idea form - small projects

Version 2.1

Registration no. (filled in by MA/JS only) _____

Project Idea Form

Date of submission 04/06/2025

1. Project idea identification

Project idea name	AI-Supported Cybersecurity For public services
Short name of the project	BALTIC SHIELD
Previous calls	yes ◉ no ○
Short name of the previous project	BALTIC SHIELD
Seed money support	yes ○ no ◉

2. Programme priority

1. Innovative societies

3. Programme objective

1.1. Resilient economies and communities

4. Potential lead applicant

Name of the organisation (original)	Turun ammattikorkeakoulu
Name of the organisation (English)	Turku University of Applied Sciences
Website	*(max. 250 characters incl. spaces)*

Country	FI
Type of Partner	Higher education and research institution

Contact person 1	
Name	Jarkko Paavola
Email	jarkko.paavola@turkuamk.fi
Phone	040 355 0335
Contact person 2	
Name	Heidi Tuominen
Email	heidi.tuominen@turkuamk.fi
Phone	050 462 0887

Which organisation(s) in the planned partnership take part in a project within the Interreg Baltic Sea Region Programme for the first time? Please list the respective partners.

N/A

5.1 Specific challenge to be adressed

COVID-19 forced the acceleration of digitization processes in many sectors. New solutions are constantly being implemented, the aim of which is to increase the efficiency and digitize the functioning of the services and institutions. Automation of local government processes undoubtedly increases the convenience and comfort of citizens and employees. However, have the newly implemented solutions adequately taken care of the important issue of cybersecurity? Progressing digitalization poses many security challenges for public institutions. Therefore, it is necessary to implement appropriately actions for safeguarding the well-being and safety of communities.
We are increasingly witnessing cyberattacks targeting government bodies. The digitization of many administrative processes opens the door to hackers who effectively exploit the weak points of security systems. According to TrendMicro 2023 report, government is the first industry affected by malware campaigns. Despite this, many local bodies have not developed or implemented a formal cybersecurity policy or remediation strategy.
The Baltic countries are particularly vulnerable since Russian invasion of Ukraine have been emerged.

BSR have been facing higher risk of cyber-attacks and new types of malicious cyber activities. These cyber-attacks harming region`s economy, social security and resilience. Alarming rate of cybercriminals trying to collect data, influence operations as well as to conduct financial fraud which causes vulnerable economies and diminish social cohesion in the region.
Resilience of public services is of crucial importance for the society. Therefore, it has been defined as one sector for CER and NIS2 directives. The resilience of public services depends on cybersecurity skills. In the face of the growing threat of cyberattacks that exploit the internal infrastructure imperfections, it is the human factor that plays a decisive role and is a major gap in cybersecurity preparedness.
The project is intended to help public authorities with this challenge. Developed support will increase the effectiveness and resilience of public authorities to cyberattacks, enabling them to prioritize the implementation of preventive measures and proactively respond to threats.

5.2 Focus of the call

The cities involved in the project are small cities with large rural areas. Usually smaller cities have less human resources, allowing them to hire cybersecurity professionals and invest in advanced cybersecurity tools.

6. Transnational relevance

There are no geographical boundaries in the cyberspace. Collateral damage from cyberattack will propagate within seconds between different countries. The Baltic countries face a growing cyber threat. In 2023, attacks on public administration and important critical infrastructure facilities became more and more frequent.
Currently, Member States' cybersecurity capabilities and involvement in this field vary. International cooperation and exchange of experiences, solutions and expert knowledge are necessary to equalize the level and face the upcoming threats together. Only a comprehensive and coherent cybersecurity ecosystem is able to meet the needs of consumers in terms of online security.
Strengthening cross-border cooperation in cybersecurity was one of the important defense issues examined by the Bureau of the Nordic Council in December 2022 and 2023.
Crucial will be also building the bridge between the key actors representing the scientific sector, public institutions and the private sector. To achieve the best results, these sectors must work together
The jointly developed solution in the project thanks to the participation and support of various countries and sectors with different levels of knowledge, common and different problems and challenges after cross-border comprehensive pilot, thorough evaluation and refinement will be a tool that can be used and replicate comprehensively by each local government of the BSR region.

7. Specific aims to be adressed

Building trust that could lead to further cooperation initiatives

The consortium's composition is new but well-considered. With the experience gained from this project, the same consortium can continue to collaborate on similar themes in the future.

Initiating and keeping networks that are important for the BSR

Enhancing cybersecurity in the Baltic Sea Region is crucial both now and in the future.

Bringing the Programme closer to the citizens

The project's results are concrete and easily disseminated to other cities in the Baltic Sea region, making the program more accessible and beneficial to citizens.

Allowing a swift response to unpredictable and urgent challenges

Cybersecurity is the responsibility of every employee. Preparing for and anticipating threats through training enables a swift response to potential risks and attacks.

8. Target groups

Target groups are public authorities, companies providing cybersecurity services to those authorities and higher education institutions

	Please use the drop-down list to define up to five target groups that you will involve through your project's activities.	Please define a field of responsibility or an economic sector of the selected target group	Specify the countries and regions that the representatives of this target group come from.
1.	Local public authority	Municipalities	Finland
2.	Regional public authority	Regional authorities	Finland, Lithuania, Latvia
3.	Higher education and research institution	Universities of Applied Sciences, Universities	Finland
4.	NGO	NGOs supporting public authority tasks	Finland, Lithuania, Latvia

5. Small and medium enterprise	Companies providing cybersecurity services to public authorities	Finland, Lithuania, Latvia

9. Contribution to the EU Strategy for the Baltic Sea Region

Please indicate if your project idea has the potential to contribute to the implementation of the Action Plan of the EU Strategy for the Baltic Sea Region (https://eusbsr.eu/implementation/).

yes ◉ no ◯

Please select which policy area(s) of the EUSBSR your project idea contributes to most.

PA Safe

PA Innovation

The MA/JS may share your project idea form with the respective policy area coordinator(s) of the EUSBSR. You can find contacts of PACs at the EUSBSR website (https://eusbsr.eu/contact-us/).

☐ If you disagree, please tick here.

10. Partnership

The consortium will be built to able achieving the agreed project objectives and deliverables. Almost finalised Consortium already involves universities and NGOs that have the appropriate know-how and expertise to develop the proposed solutions, as well as carry out project activities. The main and most important component of the Consortium will also be the public sector - local and regional authorities, which are the main target group and which will support the development of solutions so that they are tailored to their needs, successfully tested and evaluated. Public sector partners will be involved as both main Partners and Associated Partners.
The consortium is geographically balanced - countries constituting as a “Baltic Shield” are and will be involved – this includes Partners coming from Finland, Latvia, Lithuania.
The lead partner will be Turku University of Applied Sciences.

11. Workplan

As part of WP, BALTIC SHIELD Toolkit will be developed, consisting of components aimed at increasing the cybersecurity competence and responsiveness of public authorities.
The 1st component will be development of a competency framework based on EU Cybersecurity Strategy constituting as a baseline for the Cyber Training Curriculum. Curriculum will consist of

modules focusing on i.a. Risk Assessment, Data Protection, User Awareness and Cybersecurity Integration. This learning materials will also be the content for the learning management system including self-paced learning, interactive exercises, workshop schemes. The materials will be prepared in English and, thanks to AI, it will be possible to translate them into other languages
The 2nd component will be Cybersecurity Policy Roadmap, which will guide public authorities in development and improvement of internal policies and IT landscape towards new EU policies and national regulations incl. NIS2 directive.
The WP will include activities aimed not only at increasing the competences of stakeholders already involved in pilots, but also at conducting online and stationary workshops and advocacy and replication activities with neighboring municipalities and regions. The aim of these activities is to familiarize officials with cyber threats and solutions developed as part of the project.
Furthermore, in order to build a bridge between the key actors representing different sectors two Cybersecurity Forums will be organized. Representatives of public authorities, universities, research institutions, NGOS and SMEs will be invited to the events. The events will be international and will bring together various competences in one place working on a common cybersecurity challenge. The forums will build a platform for discussion and exchange of best practices to jointly ensuring cybersecurity of the Baltic Region. BALTIC SHIELD Toolkit will also be presented during the events to promote and enhance the project results.

12. Planned budget

ERDF budget (planned expenditure of partners from the EU)	EUR 500,000.00
Norwegian budget (planned expenditure of partners from Norway)	*EUR XXX*
Total budget (including preparatory costs)	**EUR 500,000.00**

13. Project consultation

Please indicate if you wish to have a consultation (online meeting) with the MA/JS to discuss your project idea

yes ◉ no ◯

14. Questions to the MA/JS

Questions related to the content of the planned project	*(max.1.000 characters incl. spaces)*
Questions related to	*(max.1.000 characters incl. spaces)*

budgeting and expenditure

Any other questions *(max. 1.000 characters incl. spaces)*

15. Additional information

(max. 1.000 characters incl. spaces)

Your account in BAMOS+

Please remember that to officially submit your application you need to access our electronic data exchange system BAMOS+. More information about the process of applying for your account in BAMOS+ you will find here:
https://interreg-baltic.eu/gateway/bamos-account