R5.3.1
REWIRE Fiches

Title	R5.3.1 REWIRE Fiche III
Document description	This deliverable identifies, documents, and promotes best and good practices aiming at addressing skills and shortages as well as fostering multi-stakeholder partnerships.
Nature	Public
Task	T5.3 REWIRE Fiches
Status	Final
WP	WP5
Lead Partner	EfVET
Partners Involved	All
Date	11/07/2023

Disclaimer:

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

CONTENTS

Table of Tables

Table of Figures

1. INTRODUCTION

Since after completing its first year of implementation, REWIRE partners have been identifying and documenting the most relevant practices at regional, national and European/International levels aimed at addressing skills shortages and mismatches in Cybersecurity, while fostering multi-stakeholder partnerships that gather representatives from different institutions and organisations working in this field, including industry, social partners, education and training providers, and public authorities.
The engagement of such stakeholders with REWIRE is crucial for the achievement of the project result's specific purposes and for its success. In the case of REWIRE Fiches, the purpose is to illustrate the project's skills strategy for Cybersecurity, which includes bringing together lessons from other initiatives focused on this field and strengthening exchange of knowledge and practices between partners and stakeholders.
The above-mentioned practices collected by REWIRE partners are clustered into fourteen (14) thematic categories, to facilitate their identification and documentation:

Table 1 Cybersecurity Best Practices: REWIRE Thematic Categories[1]

- Awareness Campaigns
- Awareness Tools
- Awareness app
- Education, Training & Awareness Prioritization
- Dedicated training programs
- Higher Education Courses
- Establishment of a Cybersecurity Organization
- Bug Bounty Program
- Reporting illegal content tool
- Guide for Businesses
- Establishment of a Cybersecurity Awareness Portal
- Cybersecurity Awareness Portal
- Cybersecurity Exercises Tool
- Establishment of a Cybersecurity Awareness Center

For this third REWIRE Fiches, all partners were invited to analyse the best practices collected so far in all thematic categories, and to assess each practice in terms of **relevance for the enhancement of Cybersecurity awareness** and **transferability to other areas of Cybersecurity fields**, i.e., able to be implemented by different organisations/institutions currently working in Cybersecurity, based on their own expertise and know how in the field.
The perspective of stakeholders on these practices will be addressed in further Fiches.

This document provides information about the methodology and tools used to collect REWIRE partners' assessment, the criteria used for that assessment and the results achieved, allowing the reader to access to a description of the most relevant and transferable best practices selected, including roles and responsibilities of the different stakeholders that implement those practices, duration, funding (where available), and expected results.

[1] Description of each Category is available on **Fiches I** (please access to https://rewireproject.eu/deliverables/#1585669012900-ed0e0ec5-b073 – REWIRE R5.3 Fiches (public).

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

2. BEST PRACTICES SELECTED BASED ON THEIR RELEVANCE AND TRANSFERABILITY POTENTIAL

This section of the Fiches aims to provide information about the methodology used to analyse and assess each Best Practice with contributions from the project partners in the scope of this specific REWIRE task, and to provide a description of the practices that were selected based on the criteria set for that selection.

2.1 Methodology for analysing and assessing the best practices

As previously mentioned, REWIRE partners were requested to analyse all best practices identified so far under the different thematic categories addressed by the project, and to assess each one of them focusing on two specific criteria:

- Relevance for the Cybersecurity awareness enhancement;
- Transferability to other areas of Cybersecurity fields.

To help them on this task, a survey was shared by email with all partners (see ANNEX 1 | REWIRE Survey to partners) sectioned by thematic category, under which each best practice was described in terms of:

- Author
- Funding (if available)
- Scope of the measure (i.e., Regional, National or European/International)
- Roles and responsibilities of stakeholders
- Description of the best practice
- Objectives
- Results
- Related resources (e.g., links for websites or articles that provide more specific information about the practice.

To facilitate the selection of the Best Practices for this third REWIRE Fiches, a Lickert scale was provided in the survey to allow partners to rate each best practice between 1 (Not Relevant / Not Transferable) and 5 (Highly Relevant / Highly Transferable):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Figure 1 REWIRE Identified Best Practices: Assessment Ratings for Relevance and Transferability categories

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

This means that one given practice could be considered Highly Relevant (5) for Cybersecurity awareness enhancement, but Not Transferable (1) to different areas of the field, or Not Relevant (1) but Highly Transferable (5). In these particular examples, the practices were not selected.
To select the best practices, a calculation was made to find the combined average score between Relevance and Transferability, in each practice. Those with **combined average score of 3 (i.e., Relevant /Transferable) or higher** were selected to be part of this Fiches.

2.2 Selected best practices

Considering the above-mentioned methodology and criteria for selecting the best practices identified within the project for this Fiches, the results collected from REWIRE partners' participation in the survey allowed to select a total of **11 Best Practices from 6 thematic categories.**
Below is the description of each selected Best Practice, as was provided in the survey to REWIRE partners, organised by thematic category.
Moreover, at the end of each section of the survey, partners were requested to provide their comments and suggestions regarding the thematic categories and/or about the practices they have analysed. The comments collected are also transcribed in this document due to their relevance for REWIRE project work.

2.2.1 Category | Awareness Campaigns

Practice	***E-Skills Week (or Digital Week)***
Rate (Combined average)	Highly Relevant & Fairly Transferable (3.75)

Author(s)	Latvian Information and Communication Technology Association (LIKTA) & Latvian Digital Skills and Jobs Coalition (LV)
Funding (if available)	EU Innovation and Networks Executive Agency (INEA) CEF TELECOM Calls 2019 - Contract INEA/CEF/ICT/A2019/2065474
Scope of the measure	National
Role and responsibilities of stakeholders	N.A.
Description of the good practice	The Digital Week annual campaign includes both centralised high-level National Coalition member events and debates, which can be followed live on the Internet, as well as events taking place in all Latvian regions: schools, libraries, non-governmental organisations, municipalities and businesses. Participants can also test their digital skills via different self-assessment tools and digital skills competitions.
Objectives	The main objective of the Digital Week in Latvia is to raise awareness of the importance of digital skills among the wider society, as well as to

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	provide practical support for the acquisition of new digital skills for different target audiences.
Results	The Digital Week takes place in Latvia for the 12th year already. Since its start, more than 5.500 face-to-face and online events have been organised, succeeding in bringing together more than 350 000 Latvians. In 11 years of the Digital Week of (2010-2020), over 200 000 Europeans used the Internet for the first time and more than 1 300 000 people have enhanced their digital skills through training events.
Related resources	Website: "Digital Week 2022 opening event in Latvia[2]" Website: Biblio "Digital Week 2022 in Latvia promoting digital skills and digital transformation[3]"

According to one of the survey participants *It is important to emphasize the **effectiveness of utilizing social networks to raise awareness and promote cyber hygiene**. This approach allows for a more approachable and relatable communication of typical threats and cyber hygiene advice. Additionally, considering the evolving nature of cybersecurity threats, **it is recommended to regularly update and refresh the campaign content to address emerging risks and challenges**. Overall, these awareness campaigns have the potential to significantly enhance cybersecurity awareness and foster a culture of cyber hygiene among the general public*.

2.2.2 Category | Awareness Tools

Practice	***Cybersecurity Job Ads Analyzer***
Rate (Combined average)	Highly Relevant / Fairly Transferable (3.16)

Author(s)	Brno University of Technology (CZ) & KTH Royal Institute of Technology (SE)
Funding (if available)	ERASMUS+ Funded Programme (621701-EPP-1-2020-1-LT-EPPKA2-SSA-B 'REWIRE') Ministry of the Interior of the Czech Republic (Grant VJ01030001)
Scope of the measure	International
Role and responsibilities of stakeholders	N.A.
Description of the good practice	The Cybersecurity Job Ads Analyzer is a new free web-based application which has been created to collect and analyse job adverts using a machine learning algorithm. This algorithm enables the detection of the skills required in advertised cybersecurity work positions. The application is both interactive and dynamic allowing for automated

[2] https://digital-skills-jobs.europa.eu/en/latest/news/digital-week-2022-opening-event-latvia

[3] https://www.biblio-project.eu/stories-2/digital-week-2022-in-latvia-promoting-digital-skills-and-digital-transformation/

	analyses and for the underlying database of job adverts to be easily updated.
Objectives	Through the Cybersecurity Job Ads Analyzer, it is possible to explore the cybersecurity skills required in work roles over time, and thereby enable academia and other training providers to better understand and address the needs of the industry.
Results	Free software application, available skills need analysis
Related resources	Website: https://rewire.informacni-bezpecnost.cz/

Practice	***Mana Drošiba (My Safety)***
Rate (Combined average)	Fairly Relevant / Fairly Transferable (3.12)

Author(s)	State Police (LV)
Funding (if available)	N.A.
Scope of the measure	National
Role and responsibilities of stakeholders	Creation and maintenance of *My Safety* website, including uploading of information material, and creation of the app.
Description of the good practice	*Mana Drošiba (My Safety)* is a website of the Latvian Police that shares important information about security to the citizens in Latvia. It includes information about several topics, including cyber security. It addresses information to three main target groups: children and young people, adults, and professionals. There are information and awareness raising material from "how children should behave on the Internet" to "bank call scams". The website also has a "report of security issues" feature, currently under development. The Mobile App "Mana Drošiba" includes information about the traffic and safety on the Internet. Its “Drošība internetā” section provides information and about security issues related to the Internet environment. It is worth to note that the app claims that it targets on users of 4+ years old.
Objectives	This is a website of the State Police, where visitors will find the most important information about security, its risks and recommendations on how to protect themselves and their belongings. Three main target groups Children and adolescents, Adults, Professionals.
Results	More than 18 informative materials for children and young people. More than 25 informative materials for adults. The mobile app has more than 10k downloads.
Related resources	Website: https://www.manadrosiba.lv/ App: http://webapp.vp.gov.lv/privacy.html

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Practice	***Cyber Security Coalition***
Rate (Combined average)	Fairly Relevant / Fairly Transferable (3.12)

Author(s)	Partnership between Academia, Public Authorities and Private Sector (BE)
Funding (if available)	The *Cyber Security Coalition* is a non-profit association (ASBL/VZW) that provides a neutral, non-commercial forum, where cybersecurity professionals can freely exchange in confidence. The Coalition is a member-funded initiative (the European Commission also a member), which fees cover the operating costs and deliverables, such as awareness campaigns, information kits or the publication of guidelines.
Scope of the measure	National
Role and responsibilities of stakeholders	Currently more than 100 key players from across three sectors (academia, public authorities, private sector) are active members contributing to the Coalition in order to build a strong cyber security ecosystem.
Description of the good practice	This Cyber Security Coalition brings together the skills and expertise of the academic world, the private sector and public authorities on a trust-based platform in order to foster information exchange and implementing joint actions, and bolster cybersecurity resilience at the national level.
Objectives	The Coalition focuses on four strategic domains: - Experience sharing (sharing knowledge, best practices, threats and opportunities, operation collaboration); - Peer-to-peer collaboration within a trusted community; - Policy recommendations (issuing recommendations for more efficient policies and guidelines); - Raising awareness (campaigns to raise awareness amongst citizens and organizations).
Results	In addition to awareness campaigns and guides, we can highlight four cybersecurity awareness tool kits (mainly targeting SMEs and organizations): - Interactive Cyber Security E-Learning, via Kahoot; - Start with Cybersecurity: the basics; - SME Security Scan; - Cybersecurity KIT.
Related resources	Website: https://www.cybersecuritycoalition.be/ Cyber Security Coalition Annual Report (2021/2022)[4] Tools : https://www.cybersecuritycoalition.be/tools/

A comment provided by one of the participant partners stated that *it is crucial to highlight the* ***importance of providing organizations with effective tools to raise awareness about cybersecurity****. The availability of educational resources and training*

[4] https://annualreport.cybersecuritycoalition.be/nl/annualreportcybersecuritycoalitionbe/

tools, such as awareness kits, can greatly contribute to ***equipping employees with the necessary knowledge and skills*** *to prevent cybersecurity incidents*.

2.2.3 Category | Awareness App

Practice	***Awareness Kit***
Rate (Combined average)	Fairly Relevant / Fairly Transferable (3.75)

Author(s)	INCIBE (Spanish National Cybersecurity Institute) (ES)
Funding (if available)	NextGeneration EU
Scope of the measure	National
Role and responsibilities of stakeholders	Provide tools to companies to raise awareness
Description of the good practice	Most situations that affect business continuity are due in one way or another to the lack of cybersecurity preparation of those who have to manage the technology. To make up for this weakness, SMEs and micro-enterprises can use this awareness kit, a didactic tool to raise awareness and train employees in the safe use of technology.
Objectives	With the awareness kit, your employees will be able to access educational resources and training tools to avoid cybersecurity incidents that affect companies. This kit has been designed so that its implementation can be carried out by organizations from all sectors, without the need for prior technical knowledge.
Results	Graphical resources and training programmes
Related resources	Website: "Awareness Kit"[5]

According to a participant of the survey *It is important to* ***highlight the potential of mobile applications to enhance cybersecurity awareness and promote cyber hygiene****. (…) It is crucial to ensure that these apps are* ***user-friendly, accessible, and regularly updated*** *to address emerging threats and challenges. Additionally, it is recommended to provide users with* ***clear instructions on how to use the app*** *and how to report any issues or incidents.*

[5] https://www.incibe.es/empresas/formacion/kit-concienciacion

2.2.4 Category | Education, Training and Awareness Prioritization

Practice	***Austrian Cyber Security Strategy (ACSS)***
Rate (Combined average)	Fairly Relevant / Transferable (3)

Author(s)	Bundesministerium für europäische und internationale Angelegenheiten (AT)
Funding (if available)	N.A.
Scope of the measure	International / European
Role and responsibilities of stakeholders	N.A.
Description of the good practice	ACSS is designed to guide efforts to meet cybersecurity challenges as effectively as possible. It serves to implement a major pillar of the current government's policy in this area, also laying the groundwork for a systemic approach to cooperation between government agencies, research institutions and businesses.
Objectives	Cybersecurity issues are increasingly affecting Austrian citizens in every aspect of their daily lives. Cyberspace is not static; indeed, it is constantly evolving. Nevertheless, existing legal frameworks, and in particular the principles of international law, human rights law and humanitarian international law, still apply in the digital realm. Threats and challenges in cyberspace can rarely be contained within national borders. This means that security can only be ensured through a comprehensive cybersecurity policy and close cooperation with all relevant stakeholders. This is what the ACSS is designed to achieve. With its list of specific measures to be implemented, it provides a flexible, effective and inclusive tool for detecting, preventing and dealing with threats and challenges in cyberspace, with the dual aims of achieving the highest possible level of cybersecurity and making the most of the opportunities that digitalisation brings in every area of our lives.
Results	The Steering Group develops an Implementation Plan to carry out the horizontal measures laid down in the ACSS within three months after its adoption by the federal government. The competent bodies are responsible for implementing these measures within their respective mandate. The implementation of measures of the ACSS will be coordinated by the Cyber Security Steering Group. Based on the ACSS, the competent ministries will develop sub-strategies for their sphere of responsibilities. The ministries represented in the Cyber Security Steering Group will submit an Implementation Report to the federal government every two years. The preparation of the Implementation Report will go hand in hand with a review of the Austrian Cyber Security

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	Strategy, which will be revised and updated if necessary. The strategic foundations will be further developed in cooperation with non-state partners
Related resources	Document: "Austrian Cybersecurity Strategy"[6]

Practice	***Technology Pact***
Rate (Combined average)	Fairly Relevant / Fairly Transferable (3)

Author(s)	Ministry of Industry, Business and Financial Affairs, Ministry of Higher Education and Science & Ministry of Children and Education (DK)
Funding (if available)	Finance Act
Scope of the measure	National
Role and responsibilities of stakeholders	Ministry of Industry, Business and Financial Affairs, Ministry of Higher Education and Science, Ministry of Children and Education, DbTF Council and a great number of partners. (Currently based on the report found at https://www.teknologipagten.dk/). The Technology Pact was established in 2018 with the purpose to gather the actors in the Science, Technology, Engineering and mathematics (STEM) area to focus on the lack of Danes with STEM skills and show how different projects and actors work concretely to lift the common social task. The overall strategic direction for the Technology Pact was set by the DbTF Council, which met several times a year, where members discussed existing and potential initiatives and activities. In this context, the Secretariat of the Technology Pact had an advisory role in relation to the Technology Pact Council. Specifically, the secretariat made recommendations for themes and activities, which were then discussed at the Council meetings.
Description of the good practice	The Technology Pact has been created to meet current and future recruitment problems in the so-called STEM subjects.
Objectives	In less than 10 years, Denmark will lack more than 10 000 STEM skills. Therefore, the goal of the Technology Pact is to educate 20 percent more people with STEM skills in 10 years than in 2018, when the Technology Pact was created. The Technology Pact thus works to ensure that the Danes' STEM skills are lifted all the way from cradle to grave, so that we both meet the current, acute recruitment problems in the Danish business community, but also ensure that the next generation wants to take a STEM education. Specifically, the work of the Technology Pact will help to meet a number of objectives that have concrete impact goals attached to them: - More people should be interested in STEM. - 1 million people will participate in the Technology Pact's efforts in 2020. - 350 companies to engage in the Technology Pact by 2020. - More people need to educate themselves in STEM

[6] https://www.cyberwiser.eu/sites/default/files/NCSS%20Austria%202013%20en.pdf

	- 20% more Danes will complete a non-dimensioned higher STEM education in 10 years. - 20% more people need to complete STEM vocational training in 10 years. - More people need to use STEM in jobs - The STEM skills of the workforce must be among Europe's best. - The Danes' problem-solving skills with IT must be on a par with the Nordic countries. - No comprehensive STEM skills recruitment challenges in 10 years.
Results	The Technology Pact's projects have registered over 1.7 million participants in project activities by the end of 2020. The pact's objective of 1,000,000 participants has thus been more than met. As a number of projects were completed in 2020, it is expected that activity in 2021 and 2022 will be lower than in previous years. Based on the projects' current registrations, it is expected that a good 2.7 million will have participated in one of the Technology Pact's projects by the end of 2022.
Related resources	Website: https://www.teknologipagten.dk/om-teknologipagten Article: "The Danish National Strategy for Cyber and Information Security"[7] Document: "The Danish National Strategy for Cyber and Information Security 2022-2024"[8]

Practice	***Cyber Hero Programme***
Rate (Combined average)	Fairly Relevant / Fairly Transferable (3)

Author(s)	Cybersecurity Network Foundation (CSN) & Serbian HE institutions (RS)
Funding (if available)	OSCE and sponsorships
Scope of the measure	National
Role and responsibilities of stakeholders	The project started as a result of ISSES ERASMUS+ project. As the ISSES project ended, the project and its activities were transferred to Cybersecurity Network Foundation for sustainability. Cooperation was established with 15 Serbian HEI and 7 high schools.
Description of the good practice	CyberHero is an educational program which promotes educational and employment opportunities for young IT professionals. The goal is to promote extracurricular activities, various types of training, and competitions for young people in the field of cybersecurity to encourage innovative thinking, skills development, and market-driven competencies. The cornerstone of the Cyber Hero program is the Serbian Cybersecurity Challenge (SCC), a national cybersecurity competition organized for both high school students and students at higher education studying in Serbia.
Objectives	Address cybersecurity skills gap through extracurricular activities for high-school and HEI students.

[7] https://en.digst.dk/strategy/the-danish-national-strategy-for-cyber-and-information-security/
[8] https://en.digst.dk/media/27024/digst_ncis_2022-2024_uk.pdf

Results	National cybersecurity competitions - Serbian Cybersecurity Challenge in 2020, 2021 and 2022. Serbian national team in cybersecurity - participation on ECSC 2022.
Related resources	Website: https://cyberhero.rs Contact email for information: info@cyberhero.rs

2.2.5 Category | Establishment of a Cybersecurity Organisation

Practice	***Nask Academy***
Rate (Combined average)	Fairly Relevant / Fairly Transferable (3)

Author(s)	NASK National Research Institute (PL)
Funding (if available)	N.A.
Scope of the measure	National
Role and responsibilities of stakeholders	NASK Academy is an initiative of the NASK National Research Institute, under which educational and popularizing activities are conducted. It was created in response to the challenges posed by the development of new digital technologies.
Description of the good practice	NASK Academy conducts training, educational and popularizing activities of the Institute and is responsible for its development. The establishment of the Academy was a response to the challenges posed by the development of new digital technologies. The Academy cooperates closely with the Dyżurnet.pl Team, functioning within the structures of NASK, responsible for counteracting harmful and illegal content present on the Internet. The Academy's activities focus on the broadly understood subject of Internet security, in particular its youngest users. The Academy implements both non-commercial projects of a training and educational nature as well as courses and trainings for institutions and enterprises.
Objectives	The activities of the NASK Academy focus on the broadly understood subject of security in the network, in particular its youngest users. The Academy implements educational and training projects for teachers, pedagogues, students of faculties related to information and communication technologies, as well as for parents. The aim of social activities carried out by the Academy is: informing, educating, and building attitudes conducive to the creation and functioning of a safe and friendly Internet. As part of the implemented activities and various projects, the Academy's experts prepare educational and information campaigns, social campaigns, educational campaigns for children and youth, as well as programs and scenarios of classes for parents and professionals.
Results	The material produced by the NASK Academy belong target the following categories: - FOR PARENTS, - WEBINARS,

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	- GAME "RUFUS IN TROUBLE", - CARTOON, - VIDEOS, - SPOTS, - AUDIOBOOKS, - INFOGRAPHICS, - TRAINING FOR EDUCATION. Current projects include: CYBER LESSONS, SELMA - DEFEAT HATE, SCHOOL OF SOCIAL NETWORKS, SAFER INTERNET, BECOME A FRIEND OF YOUR CHILD, FILE AND FOLDER, MAŁOPOLSKA PROJECT and OSE.
Related resources	Website: https://akademia.nask.pl/

Practice	***Securitymaiden.lu***
Rate (Combined average)	Fairly Relevant / Transferable (3)

Author(s)	The Cybersecurity Agency for the Luxembourg Economy and Municipalities (LU)
Funding (if available)	Safer Internet program
Scope of the measure	National
Role and responsibilities of stakeholders	N.A.
Description of the good practice	SECURITYMADEIN.LU contributes to the Luxembourg economy's trustworthiness by providing extensive cybersecurity expertise and solutions to SMEs and companies of all sizes as well as Municipalities through its 3 departments: - CIRCL (Computer Incident Response Center Luxembourg); - CASES (Cyberworld Awareness Security Enhancement Services – Luxembourg); - C3 (Cybersecurity Competence Center – Luxembourg) - in close collaboration with the CYBERSECURITY Luxembourg ecosystem's players.
Objectives	This initiative provides extensive cybersecurity expertise and solutions to SMEs and companies of all sizes as well as Municipalities.
Results	Tools, services, trainings, awareness
Related resources	Website: https://securitymadein.lu/agency/ Link for information: https://securitymadein.lu/contact/

From the perspective of one of the participants REWIRE partner, *The significance of establishing dedicated cybersecurity organizations to address cybersecurity challenges. These organizations can* ***be established at the national or organizational level and can provide a range of services, including incident response, risk management, and***

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

***security assessments**. It is crucial to ensure that these organizations are staffed with experienced cybersecurity professionals and are equipped with the necessary tools and resources to effectively address cybersecurity threats. Additionally, it is **recommended to establish partnerships with other organizations and government agencies** to enhance collaboration and information sharing.*

2.2.6 Category| Cybersecurity Awareness Portal

Practice	***Interactive resources about Cybersecurity***
Rate (Combined average)	Fairly Relevant / Transferable (3)

Author(s)	OSI - Oficina de Seguridad del Internauta (ES)
Funding (if available)	NextGeneration EU
Scope of the measure	National
Role and responsibilities of stakeholders	Provide the contents of the educational resources
Description of the good practice	This initiative by the Oficina de Seguridad del Internauta provides a series of interactive educational resources that offer detection of the different smart devices that exist at home, check and protect the information shared, detect risk situations and analyse the permissions granted to the different applications downloaded.
Objectives	This project aims to aid in learning and testing one's knowledge, protecting from any threat and from cybercriminals.
Results	A series of interactive educational resources for citizens to detect the different smart devices they have at home, check and protect the information they share, detect risk situations and analyse the permissions they grant to the different applications they download. In this way, they will learn and test their knowledge, protecting themselves from any threat and from cybercriminals.
Related resources	Website: Interactive resources about cybersecurity https://www.osi.es/es/recursos-interactivos-sobre-ciberseguridad

3 SUMMARY AND CONCLUSIONS

The main purpose of this document is to provide a detailed description of the best practices identified so far in the partnership, under specific thematic categories, that were considered by REWIRE partners as the most relevant for the Cybersecurity awareness enhancement and, at the same time, the most transferable to other areas of the Cybersecurity field.

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE Cybersecurity Skills Alliance
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

The results of the survey shared with the consortium (the basis for this work), showed that 11 of the 26 best practices listed up until this point of the project implementation period were considered as such, and that these practices belong to 6 of the 14 existent thematic categories – Awareness Campaigns, Awareness Tools, Awareness Apps, Establishment of Cybersecurity Organisation, Education, Training and Awareness Prioritization and Cybersecurity Awareness Portal.

REWIRE invites the readers of this Fiches to access the different links provided in the description of each selected best practice to explore their respective additional information and materials, and to understand how these practices can be an added value for readers' daily activities when it comes to raise awareness for the importance of enhancing Cybersecurity awareness and cyber hygiene and to address emerging risks and challenges.

It is crucial that institutions and organisations that work in this field are equipped with effective tools and have a highly skilled workforce, able to use those tools to raise awareness and to prevent cybersecurity incidents. Such tools may include user-friendly, accessible and updated apps, with clear instructions on how to use them and how to report any incident or issue (should that be the case).

Furthermore, when it comes to establishing dedicated Cybersecurity organisations (crucial to address all of the multiple challenges that this field brings to organisations, institutions and policy/decision makers at regional, national and EU/International levels), it is important that they provide a range of services (such as security assessment, incident responses or risk management) and that they foster partnerships between the different stakeholders to ensure the sharing of information and a harmonised action against those challenges.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

ANNEX 1 | REWIRE SURVEY TO PARTNERS

Dear REWIRE Partners,
One of the main purposes of REWIRE Fiches is to identify, document and promote concrete and relevant practices in Cybersecurity domain that are aimed to address skills shortages and mismatches as well as to foster multi-stakeholder partnerships.
REWIRE Partners selected a set of best practices that were previously collected, focused on the following thematic categories:

- Awareness Campaigns
- Awareness Tools
- Awareness app
- Education, Training & Awareness Prioritization
- Dedicated training programs
- Higher Education Courses
- Establishment of a Cybersecurity Organization
- Bug Bounty Program
- Reporting illegal content tool
- Guide for Businesses
- Establishment of a Cybersecurity Awareness Portal
- Cybersecurity Awareness Portal
- Cybersecurity Exercises Tool
- Establishment of a Cybersecurity Awareness Center

Considering your expertise and know-how on the issues related to Cybersecurity, we kindly ask your participation in this survey, that aims to understand which of the best practices selected by REWIRE Partners are the most relevant and transferable at national and European levels (i.e., can be implemented by organisations/institutions that are currently working on Cybersecurity field).

The results from this survey will be used for the development of the next REWIRE Fiches, hence the importance of your participation! Thus, we kindly ask you to reply to this survey **no later than June 20th, 2023**.

Your participation in this survey is completely voluntary. No personal identifiable information will be collected; therefore, your responses are unable to be tied to your identity. You can read the privacy policy of the REWIRE project here (pages 24-29)

Thank you for your time and cooperation!

Selection of the most relevant and transferable practices

Please read the description of each best practice selected by REWIRE Partners. This description provides information about the role and responsibilities of the different stakeholders involved, duration of the best practice, funding (if applicable) and results achieved.
The best practices are clustered in thematic categories to facilitate your analysis.

CATEGORY: Awareness Campaigns

Practice 1: *ARES - Workshop on Education, Training and Awareness in Cybersecurity (ETACS)*

Author(s)	Brno University of Technology (CZ)
Funding (if available)	Horizon 2020 - SPARTA project #830892 Ministry of the Interior of the Czech Republic, under grant VJ01030001
Scope of the measure	International / European
Role and responsibilities of stakeholders	N/A
Description of the good practice	ETACS is an EU symposium workshop part of the International ARES (Availability, Reliability and Security) Conference, focused on cybersecurity education, training and awareness.
Objectives	The focus of ETACS is on practical research into Higher-Education Cybersecurity curricula, professional training, building of cyber ranges and their coalitions across Europe, methods to assess and raise awareness in cybersecurity, the implementation of systems, and lessons learned. The event aims at gathering representatives from Higher Education (HE) institutions, Vocational Education and Training (VET) providers, industry, government and EU agencies to discuss current problems and solutions, and at allowing for the submission of papers from academia, government and industry, that contribute to cybersecurity education and training.
Results	Publications on Cybersecurity education, experts' opinion exchange, cybersecurity awareness.
Related resources	Website: ARES Conference 2023

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement,** using the Lickert scale in which 1 represents “Not relevant” and 5 represents “Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Practice 2 : *Safe Digital*

Author(s)	Danish Agency for Digitisation & Danish Business Authority (DK)
Funding (if available)	N.A.
Scope of the measure	National
Role and responsibilities of stakeholders	Sikker Digital (https://sikkerdigital.dk) helped to develop the contents of the awareness materials, and to ensure their quality.
Description of the good practice	One stop interface for awareness materials addressing different target groups, including "Cybersecurity Month".
Objectives	Raise awareness of cyber threats and continuously improve awareness of how to cope safety with them.
Results	Collection of over 20 tips and tools for 3 main target groups – Citizens, Companies and Authorities, in Denmark. This initiative includes European Cybersecurity Month (over 40 events). Views in YouTube exceed 40 000. Sikkerdigital.dk traffic volume is 2,354 unique daily. Each visitor makes around 2.14 page views on average (based on "webrate").
Related resources	Website: Sikker Digital DK "What is National Cybersecurity Month?"

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement,** using the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Practice 3: *E-Skills Week (or Digital Week)*

Author(s)	Latvian Information and Communication Technology Association (LIKTA) & Latvian Digital Skills and Jobs Coalition (LV)
Funding (if available)	EU Innovation and Networks Executive Agency (INEA) CEF TELECOM Calls 2019 - Contract INEA/CEF/ICT/A2019/2065474
Scope of the measure	National
Role and responsibilities of stakeholders	N.A.
Description of the good practice	The Digital Week annual campaign includes both centralised high-level National Coalition member events and debates, which can be followed live on the Internet, as well as events taking place in all Latvian regions: schools, libraries, non-governmental organisations, municipalities and businesses. Participants can also test their digital skills via different self-assessment tools and digital skills competitions.
Objectives	The main objective of the Digital Week in Latvia is to raise awareness of the importance of digital skills among the wider society, as well as to provide practical support for the acquisition of new digital skills for different target audiences.
Results	The Digital Week takes place in Latvia for the 12th year already. Since its start, more than 5.500 face-to-face and online events have been organised, succeeding in bringing together more than 350 000 Latvians. In 11 years of the Digital Week of (2010-2020), over 200 000 Europeans used the Internet for the first time and more than 1 300 000 people have enhanced their digital skills through training events.
Related resources	Website: "Digital Week 2022 opening event in Latvia" Website: Biblio "Digital Week 2022 in Latvia promoting digital skills and digital transformation"

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement,** using the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Practice 4: *"ZAŠT!TISE" Awareness building campaign on social media*

Author(s)	RNIDS - Serbian National Internet Domain Registry & CSN - Cybersecurity Network Foundation (RS)
Funding (if available)	Serbian National Internet Domain Registry (RNIDS)
Scope of the measure	National
Role and responsibilities of stakeholders	N.A.
Description of the good practice	National cybersecurity awareness campaign on social networks. Influencers on approachable way talking about typical threats and giving cyber-hygiene advices.
Objectives	Raise awareness and building cyber hygiene culture.
Results	On-going (30.10.2022)
Related resources	Website: https://zastitise.rs

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Any comments/suggestions you would like to provide regarding these best practices?

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CATEGORY: Awareness Tools

Practice 1: *Internet Segura for Kids (is4k)*

Author(s)	INCIBE (Spanish National Cybersecurity Institute) (ES)
Funding (if available)	- EU's NextGenerationEU program - Recovery, Transformation and Resilience Plan (COVID-19 fund) - Digital Spain 2026 - Co-financed by EU "2015 CEF Telecom Call – Safer Internet (2015-CEF-TC-2015-1)": 650.840 €
Scope of the measure	National
Role and responsibilities of stakeholders	N.A.
Description of the good practice	Project focused on the safe use of the internet by young people.
Objectives	Raise awareness and train minors, young people, families, educators and professionals through the development of campaigns, initiatives and nationwide programs focused on a safe use of the internet by children. Offer a helpline advise and assist minors, families, educators and professionals on how to deal with Internet risks: harmful content, harmful contacts and inappropriate behaviour. Organise the Safer Internet Day in Spain. Reduce the availability of criminal content on the Internet, mainly child sexual abuse, by supporting the FCSE.
Results	A set of guidelines targeting at children, their families and educators aimed at preventing risks on internet (including social media); Articles, training modules and other materials for teachers to capacitate them on how to teach, how to correctly use the internet and on how to act in case of a cyberattack.
Related resources	Website: https://www.is4k.es/ Helpline service: https://www.is4k.es/ayuda Contact form: https://www.is4k.es/contacto

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement,** using the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Practice 2: *Cybersecurity Job Ads Analyzer*

Author(s)	Brno University of Technology (CZ) & KTH Royal Institute of Technology (SE)
Funding (if available)	ERASMUS+ Funded Programme (621701-EPP-1-2020-1-LT-EPPKA2-SSA-B 'REWIRE') Ministry of the Interior of the Czech Republic (Grant VJ01030001)
Scope of the measure	International
Role and responsibilities of stakeholders	N.A.
Description of the good practice	The Cybersecurity Job Ads Analyzer is a new free web-based application which has been created to collect and analyse job adverts using a machine learning algorithm. This algorithm enables the detection of the skills required in advertised cybersecurity work positions. The application is both interactive and dynamic allowing for automated analyses and for the underlying database of job adverts to be easily updated.
Objectives	Through the Cybersecurity Job Ads Analyzer, it is possible to explore the cybersecurity skills required in work roles over time, and thereby enable academia and other training providers to better understand and address the needs of the industry.
Results	Free software application, available skills need analysis
Related resources	Website: https://rewire.informacni-bezpecnost.cz/

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Practice 3: *Mana Drošiba (My Safety)*

Author(s)	State Police (LV)
Funding (if available)	N.A.
Scope of the measure	National
Role and responsibilities of stakeholders	Creation and maintenance of *My Safety* website, including uploading of information material, and creation of the app.
Description of the good practice	*Mana Drošiba (My Safety)* is a website of the Latvian Police that shares important information about security to the citizens in Latvia. It includes information about several topics, including cyber security. It addresses information to three main target groups: children and young people, adults, and professionals. There are information and awareness raising material from "how children should behave on the Internet" to "bank call scams". The website also has a "report of security issues" feature, currently under development. The Mobile App "Mana Drošiba" includes information about the traffic and safety on the Internet. Its "Drošība internetā" section provides information and about security issues related to the Internet environment. It is worth to note that the app claims that it targets on users of 4+ years old.
Objectives	This is a website of the State Police, where visitors will find the most important information about security, its risks and recommendations on how to protect themselves and their belongings. Three main target groups Children and adolescents, Adults, Professionals.
Results	More than 18 informative materials for children and young people. More than 25 informative materials for adults. The mobile app has more than 10k downloads.
Related resources	Website: https://www.manadrosiba.lv/ App: http://webapp.vp.gov.lv/privacy.html

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Practice 4: *Cyber Security Coalition*

Author(s)	Partnership between Academia, Public Authorities and Private Sector (BE)
Funding (if available)	The *Cyber Security Coalition* is a non-profit association (ASBL/VZW) that provides a neutral, non-commercial forum, where cybersecurity professionals can freely exchange in confidence. The Coalition is a member-funded initiative (the European Commission also a member), which fees cover the operating costs and deliverables, such as awareness campaigns, information kits or the publication of guidelines.
Scope of the measure	National
Role and responsibilities of stakeholders	Currently more than 100 key players from across three sectors (academia, public authorities, private sector) are active members contributing to the Coalition in order to build a strong cyber security ecosystem.
Description of the good practice	This Cyber Security Coalition brings together the skills and expertise of the academic world, the private sector and public authorities on a trust-based platform in order to foster information exchange and implementing joint actions, and bolster cybersecurity resilience at the national level.
Objectives	The Coalition focuses on four strategic domains: - Experience sharing (sharing knowledge, best practices, threats and opportunities, operation collaboration); - Peer-to-peer collaboration within a trusted community; - Policy recommendations (issuing recommendations for more efficient policies and guidelines); - Raising awareness (campaigns to raise awareness amongst citizens and organizations).

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Results	In addition to awareness campaigns and guides, we can highlight four cybersecurity awareness tool kits (mainly targeting SMEs and organizations): - Interactive Cyber Security E-Learning, via Kahoot; - Start with Cybersecurity: the basics; - SME Security Scan; - Cybersecurity KIT.
Related resources	Website: https://www.cybersecuritycoalition.be/ Cyber Security Coalition Annual Report (2021/2022) Tools : https://www.cybersecuritycoalition.be/tools/

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement,** using the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Any comments/suggestions you would like to provide regarding these best practices?

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CATEGORY: Awareness app

Practice 1: *Awareness Kit*

Author(s)	INCIBE (Spanish National Cybersecurity Institute) (ES)
Funding (if available)	NextGeneration EU
Scope of the measure	National
Role and responsibilities of stakeholders	Provide tools to companies to raise awareness
Description of the good practice	Most situations that affect business continuity are due in one way or another to the lack of cybersecurity preparation of those who have to manage the technology. To make up for this weakness, SMEs and micro-enterprises can use this awareness kit, a didactic tool to raise awareness and train employees in the safe use of technology.
Objectives	With the awareness kit, your employees will be able to access educational resources and training tools to avoid cybersecurity incidents that affect companies. This kit has been designed so that its implementation can be carried out by organizations from all sectors, without the need for prior technical knowledge.
Results	Graphical resources and training programmes
Related resources	Website: "Awareness Kit"

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Practice 2: *Safeonweb mobile app*

Author(s)	CCB - Centre for Cybersecurity Belgium
Funding (if available)	N.A.
Scope of the measure	National
Role and responsibilities of stakeholders	Provide information about computer infections. Hub of cyber threads.
Description of the good practice	*Safeonweb* is an app of the Centre for Cyber Security Belgium (CCB) that allows to receive notifications about computer infections. The CCB receives daily reports from its Cyber Security partners about infections and threats, which are shared in the app to keep the population aware of recent vulnerabilities and threats in Belgium.
Objectives	The aim of Safeonweb is to provide a tool with which people can better prepare against cyber threats.
Results	>100k downloads; 4,4 rating (308 reviews)
Related resources	Website: https://www.safeonweb.be/

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Any comments/suggestions you would like to provide regarding these best practices?

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CATEGORY: Education, Training & Awareness Prioritization

Practice 1: *Austrian Cyber Security Strategy (ACSS)*

Author(s)	Bundesministerium für europäische und internationale Angelegenheiten (AT)
Funding (if available)	N.A.
Scope of the measure	International / European
Role and responsibilities of stakeholders	N.A.
Description of the good practice	ACSS is designed to guide efforts to meet cybersecurity challenges as effectively as possible. It serves to implement a major pillar of the current government's policy in this area, also laying the groundwork for a systemic approach to cooperation between government agencies, research institutions and businesses.
Objectives	Cybersecurity issues are increasingly affecting Austrian citizens in every aspect of their daily lives. Cyberspace is not static; indeed, it is constantly evolving. Nevertheless, existing legal frameworks, and in particular the principles of international law, human rights law and humanitarian international law, still apply in the digital realm. Threats and challenges in cyberspace can rarely be contained within national borders. This means that security can only be ensured through a comprehensive cybersecurity policy and close cooperation with all relevant stakeholders. This is what the ACSS is designed to achieve. With its list of specific measures to be implemented, it provides a flexible, effective and inclusive tool for detecting, preventing and dealing with threats and challenges in cyberspace, with the dual aims of achieving the highest possible level of cybersecurity and making the most of the opportunities that digitalisation brings in every area of our lives.
Results	The Steering Group develops an Implementation Plan to carry out the horizontal measures laid down in the ACSS within three months after its adoption by the federal government. The competent bodies are responsible for implementing these measures within their respective mandate. The implementation of measures of the ACSS will be coordinated by the Cyber Security Steering Group. Based on the ACSS, the competent ministries will develop sub-strategies for their sphere of responsibilities. The ministries represented in the Cyber Security Steering Group will submit an Implementation Report to the federal government every two years. The preparation of the Implementation Report will go hand in hand with a review of the Austrian Cyber Security Strategy, which will be revised and updated if necessary. The strategic foundations will be further developed in cooperation with non-state partners
Related resources	Document: "Austrian Cybersecurity Strategy"

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Practice 2: *Activity area 4.1 Raising the cyber awareness of citizens, state and private sector*

Author(s)	Ministry of Economic Affairs - Republic of Estonia (EE)
Funding (if available)	Ministry of Education, Police and Border Guard Board, Cyber Defence League and TalTech & the Rescue Board
Scope of the measure	National
Role and responsibilities of stakeholders	N.A.
Description of the good practice	The results of the foregoing activities related to raising cyber awareness will be consolidated in a common platform, and possibilities for independent learning will be offered. Cybersecurity will be dealt with in the educational systems at all levels of education as part of developing digital competencies. Additionally, activities for raising awareness aimed at the general public will be carried out. Knowledge and skills of students and teachers will be measured systematically and a supply of training in the field of cybersecurity will be provided for general educational school and vocational school teachers. Finally, a systematic, nationwide platform for government institutions and local governments for raising cyber awareness will be developed.
Objectives	The Estonian society today is not sufficiently well prepared for coping with existing cyber threats – the private and public sectors alike are largely unaware of the risks and needs, in particular at the leadership level. Digital technologies now have such an intertwined role in Estonian society that it is not possible to address all risks through a single planning document. The principles of cybersecurity are already partially integrated into sectoral planning processes. However, the maintenance and development of a sustainable digital environment also requires cross-sectoral focused cooperation. This can only be ensured by means of a strong and coherent sectoral strategy. In addition, the cybersecurity

	strategy plays the role of a communication tool for raising awareness in political decision-making processes, enhancing public-private partnership, and shaping Estonia's international engagement. As a society, Estonia is cyber literate and a future supply of specialists in the field is guaranteed. In 2015, 30% of internet users in Estonia had some contact with a security vulnerability. On the private sector side, the general ability to cope with attacks is reflected by the low awareness of the implementation of security policies, as only 17% of all Estonian companies had implemented security policies as of 2015. For all members of society to be able to operate securely in cyberspace, it is top priority to ensure a future supply of specialists for organizations responsible for cybersecurity, devoting attention to talent search programmes, and formal and continuing education. A clear demand for specialists is seen in three groups – public sector institutions responsible for cybersecurity, vital service providers and enterprise in the cyber field.
Results	Various actions to raise awareness and improve education. Activities for raising awareness aimed at the general public will be carried out. Knowledge and skills of students and teachers will be measured systematically and a supply of training in the field of cybersecurity will be provided for general educational school and vocational school teachers. A systematic, nationwide platform for government institutions and local governments for raising cyber awareness will be developed. The knowledge and skills of the state's mid-level and top officials will be strengthened.
Related resources	Document: "Cybersecurity Strategy – Republic of Estonia"

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement,** using the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Practice 3: *Technology Pact*

Author(s)	Ministry of Industry, Business and Financial Affairs, Ministry of Higher Education and Science & Ministry of Children and Education (DK)
Funding (if available)	Finance Act
Scope of the measure	National
Role and responsibilities of stakeholders	Ministry of Industry, Business and Financial Affairs, Ministry of Higher Education and Science, Ministry of Children and Education, DbTF Council and a great number of partners. (Currently based on the report found at https://www.teknologipagten.dk/). The Technology Pact was established in 2018 with the purpose to gather the actors in the STEM area to focus on the lack of Danes with STEM skills and show how different projects and actors work concretely to lift the common social task. The overall strategic direction for the Technology Pact was set by the DbTF Council, which met several times a year, where members discussed existing and potential initiatives and activities. In this context, the Secretariat of the Technology Pact had an advisory role in relation to the Technology Pact Council. Specifically, the secretariat made recommendations for themes and activities, which were then discussed at the Council meetings.
Description of the good practice	The Technology Pact has been created to meet current and future recruitment problems in the so-called STEM subjects (Science, Technology, Engineering and Mathematics).
Objectives	In less than 10 years, Denmark will lack more than 10 000 STEM skills. Therefore, the goal of the Technology Pact is to educate 20 percent more people with STEM skills in 10 years than in 2018, when the Technology Pact was created. The Technology Pact thus works to ensure that the Danes' STEM skills are lifted all the way from cradle to grave, so that we both meet the current, acute recruitment problems in the Danish business community, but also ensure that the next generation wants to take a STEM education. Specifically, the work of the Technology Pact will help to meet a number of objectives that have concrete impact goals attached to them: - More people should be interested in STEM. - 1 million people will participate in the Technology Pact's efforts in 2020. - 350 companies to engage in the Technology Pact by 2020. - More people need to educate themselves in STEM - 20% more Danes will complete a non-dimensioned higher STEM education in 10 years. - 20% more people need to complete STEM vocational training in 10 years. - More people need to use STEM in jobs - The STEM skills of the workforce must be among Europe's best.

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	- The Danes' problem-solving skills with IT must be on a par with the Nordic countries. - No comprehensive STEM skills recruitment challenges in 10 years.
Results	The Technology Pact's projects have registered over 1.7 million participants in project activities by the end of 2020. The pact's objective of 1,000,000 participants has thus been more than met. As a number of projects were completed in 2020, it is expected that activity in 2021 and 2022 will be lower than in previous years. Based on the projects' current registrations, it is expected that a good 2.7 million will have participated in one of the Technology Pact's projects by the end of 2022.
Related resources	Website: https://www.teknologipagten.dk/om-teknologipagten Article: "The Danish National Strategy for Cyber and Information Security" Document: "The Danish National Strategy for Cyber and Information Security 2022-2024"

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Practice 4: *Cyber Hero Programme*

Author(s)	Cybersecurity Network Foundation (CSN) & Serbian HE institutions (RS)
Funding (if available)	OSCE and sponsorships
Scope of the measure	National
Role and responsibilities of stakeholders	The project started as a result of ISSES ERASMUS+ project. As the ISSES project ended, the project and its activities were transferred to Cybersecurity Network Foundation for sustainability. Cooperation was established with 15 Serbian HEI and 7 high schools.
Description of the good practice	CyberHero is an educational program which promotes educational and employment opportunities for young IT professionals. The goal is to promote extracurricular activities, various types of training, and competitions for young people in the field of cybersecurity to encourage

	innovative thinking, skills development, and market-driven competencies. The cornerstone of the Cyber Hero program is the Serbian Cybersecurity Challenge (SCC), a national cybersecurity competition organized for both high school students and students at higher education studying in Serbia.
Objectives	Address cybersecurity skills gap through extracurricular activities for high-school and HEI students.
Results	National cybersecurity competitions - Serbian Cybersecurity Challenge in 2020, 2021 and 2022. Serbian national team in cybersecurity - participation on ECSC 2022.
Related resources	Website: https://cyberhero.rs Contact email for information: info@cyberhero.rs

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Any comments/suggestions you would like to provide regarding these best practices?

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CATEGORY: Dedicated training programs

Practice 1: *Cyber Security for Blockchain (summer school)*

Author(s)	EIT Digital (SK)
Funding (if available)	EIT
Scope of the measure	Regional
Role and responsibilities of stakeholders	N.A.
Description of the good practice	The Summer School will focus on Smart Contracts and their nearly unlimited use-cases in the financial and public sector. The participants will learn how to use one of the most popular blockchain frameworks, Ethereum, a prominent smart contract platform, and its dominant programming language, Solidity, with emphasis on security issues and cyber security concerns. Also, the student will gain insights into how decentralized finances are connected to ransomware and threats from cybercriminals. On top of that, the participants will understand proactive security measures based on network monitoring and security incident handling based on machine learning.
Objectives	Teach participants the basics of blockchains and smart contracts.
Results	The participants will learn how to use one of the most popular blockchain frameworks, Ethereum, a prominent smart contract platform, and its dominant programming language, Solidity, with emphasis on security issues and cyber security concerns. Also, the student will gain insights into how decentralised finances are connected to ransomware and threats from cybercriminals. On top of that, the participants will understand proactive security measures based on network monitoring and security incident handling based on machine learning.
Related resources	Website: https://summerschool.eitdigital.eu/cyber-security-for-blockchain

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement,** using the Lickert scale in which 1 represents “Not relevant” and 5 represents “Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Any comments/suggestions you would like to provide regarding this best practice?

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CATEGORY: Higher Education Courses

Practice 1: *Cybersecurity Bachelor and Master's degree at MU*

Author(s)	Masaryk University - MU (CZ)
Funding (if available)	The development of courses was partially funded by various grants awarded by the Czech government agencies or EU. Delivery of courses is funded from MU budget.
Scope of the measure	Regional/National/European
Role and responsibilities of stakeholders	Individual courses were developed and are being delivered by academics of the university in cooperation with the main stakeholders in Czech Republic (industry, National cyber and information security agency, National Cyber defence centre, law enforcement agencies, other relevant public institutions). Some courses on cybercrime are based on curricula developed by United Nations Office for Drugs and Crime. Some stakeholders are also directly involved in delivering individual lectures.
Description of the good practice	Cybersecurity studies at Masaryk University take advantage of the multidisciplinary nature of the university and, therefore, in addition to technical aspects of security, they also focus on political, legal, social science or economic aspects. The study programmes and their courses are designed in accordance with the framework of qualifications in cybersecurity, which was proposed for the Czech Republic in a project by Masaryk University. In addition to the interdisciplinary nature, the study programmes also offer a very practical approach through hands-on courses that use the infrastructure of the Cyber range lab and platform, digital and network forensics labs, cryptography and Internet of Things (IoT) labs for practical demonstrations and teaching. Courses are also prepared and delivered with practitioners from the public and private spheres who also participate in teaching.
Objectives	The aim is to provide multidisciplinary and practical training in cybersecurity to help build a solid workforce in this field, and to meet the strategic objectives formulated in the National Cyber Security Strategy and the Framework of Qualifications in Cyber Security in the Czech Republic.
Results	Masaryk University has been providing cyber security education in specific fields for more than five years. During this period, it has produced hundreds of graduates who are mainly employed in the private and public sector and have contributed significantly to building cyber security mechanisms and market in the Czech Republic. At the same time, the study programmes and their courses are continuously updated based on current technological, security and regulatory developments.
Related resources	Website: https://www.muni.cz/en/bachelors-and-masters-study-programmes/26540-kyberbezpecnost

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Practice 2: *Information Security Services Education in Serbia – ISSES*

Author(s)	University of Novi Sad / University of Belgrade (UB) / University of NiÅ¡ (UNI) / Unicom Telecom Ltd (UT) / Subotica Tech – College of Applied Sciences (VTS) / Innovation Center Of The University Of Niš Ltd (ICUN) (RS) Faculty of organization and informatics (FOI), University of Zagreb (HR) Budapest University of Technology and Economics (BME) (HU) Polytechnic University of Milano (Polimi) (IT)
Funding (if available)	Funded by the Author Universities
Scope of the measure	National
Role and responsibilities of stakeholders	N.A.
Description of the good practice	The goal of the ISSES project is to improve the higher education capacities in the field of Information Security in the Republic of Serbia. Entirely new courses are developed, which raise the competitiveness of students graduating at the participating HEIs in Serbia. The project team also developed state-of-the-art laboratories which will allow the students to gain hands-on experience directly transferrable to the information security industry.
Objectives	Develop a MSc program and laboratories.

Results	- 13 brand-new courses developed with support from leading international partners
	- 2 study programs in accreditation (UNS & VTS)
	- 2 study modules (UNI & FON)
	  ○ 1 accredited in 2019
	  ○ 1 in accreditation
	- >100 students enrolled in new courses @ ETF
	- >100 students enrolled in DF course @ UNS

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	- 7 labs founded at 4 higher education institutions (HEI) - 2 national hackathons organized with new challenges - Multiple network security and crypto challenges developed - 8 industrial control system security challenges and drills developed
Related resources	Website: https://isses.etf.bg.ac.rs/about/

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Any comments/suggestions you would like to provide regarding these best practices?

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CATEGORY: Establishment of a Cybersecurity Organization

Practice 1: *Nask Academy*

Author(s)	NASK National Research Institute (PL)
Funding (if available)	N.A.
Scope of the measure	National
Role and responsibilities of stakeholders	NASK Academy is an initiative of the NASK National Research Institute, under which educational and popularizing activities are conducted. It was created in response to the challenges posed by the development of new digital technologies.
Description of the good practice	NASK Academy conducts training, educational and popularizing activities of the Institute and is responsible for its development. The establishment of the Academy was a response to the challenges posed by the development of new digital technologies. The Academy cooperates closely with the Dyżurnet.pl Team, functioning within the structures of NASK, responsible for counteracting harmful and illegal content present on the Internet. The Academy's activities focus on the broadly understood subject of Internet security, in particular its youngest users. The Academy implements both non-commercial projects of a training and educational nature as well as courses and trainings for institutions and enterprises.
Objectives	The activities of the NASK Academy focus on the broadly understood subject of security in the network, in particular its youngest users. The Academy implements educational and training projects for teachers, pedagogues, students of faculties related to information and communication technologies, as well as for parents. The aim of social activities carried out by the Academy is: informing, educating, and building attitudes conducive to the creation and functioning of a safe and friendly Internet. As part of the implemented activities and various projects, the Academy's experts prepare educational and information campaigns, social campaigns, educational campaigns for children and youth, as well as programs and scenarios of classes for parents and professionals.
Results	The material produced by the NASK Academy belong target the following categories: FOR PARENTS, WEBINARS, GAME "RUFUS IN TROUBLE", CARTOON, VIDEOS, SPOTS, AUDIOBOOKS, INFOGRAPHICS, TRAINING FOR EDUCATION. Current projects include: CYBER LESSONS, SELMA - DEFEAT HATE, SCHOOL OF SOCIAL NETWORKS, SAFER INTERNET, BECOME A FRIEND OF YOUR CHILD, FILE AND FOLDER, MAŁOPOLSKA PROJECT and OSE.
Related resources	Website: https://akademia.nask.pl/

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Practice 2: *Securitymaiden.lu*

Author(s)	The Cybersecurity Agency for the Luxembourg Economy and Municipalities (LU)
Funding (if available)	Safer Internet program
Scope of the measure	National
Role and responsibilities of stakeholders	N.A.
Description of the good practice	SECURITYMADEIN.LU contributes to the Luxembourg economy's trustworthiness by providing extensive cybersecurity expertise and solutions to SMEs and companies of all sizes as well as Municipalities through its 3 departments: - CIRCL (Computer Incident Response Center Luxembourg); - CASES (Cyberworld Awareness Security Enhancement Services – Luxembourg); - C3 (Cybersecurity Competence Center – Luxembourg) - in close collaboration with the CYBERSECURITY Luxembourg ecosystem's players.
Objectives	This initiative provides extensive cybersecurity expertise and solutions to SMEs and companies of all sizes as well as Municipalities.
Results	Tools, services, trainings, awareness
Related resources	Website: https://securitymadein.lu/agency/ Link for information: https://securitymadein.lu/contact/

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Practice 3: *Cybersecurity Network Foundation (CSN)*

Author(s)	CSN - Cybersecurity Network Foundation (RS)
Funding (if available)	OSCE
Scope of the measure	National
Role and responsibilities of stakeholders	N.A.
Description of the good practice	Cybersecurity Network Foundation (CSN) formerly informally known as the "Petnica Group", was developed along the process of establishing a regulatory and institutional framework for the cyber security in Serbia. Over time, this community has developed into an informal, multi-stakeholder network that regularly holds meetings from 2015 involving wide range of actors from the public and private sectors, academia and civil society. From the very beginning, the community focused on strengthening public-private partnerships and supporting the development of adequate cybersecurity policies and strategic frameworks in the Republic of Serbia. The CSN is formally established as a foundation in 2020.
Objectives	Center for the exchange of information, knowledge and practice, as a support group in case of incidents due to personal contacts between its members, and as a group of potential partners in future projects and programs in the field of cyber security.
Results	Successful public-private partnership which connects all the cybersecurity related stakeholders in Serbia
Related resources	Website: https://cybersecurityserbia.rs

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Any comments/suggestions you would like to provide regarding these best practices?

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CATEGORY: Bug Bounty Program

Practice 1: *Coordinated Vulnerability Disclosure Policy (CVDP) and vulnerability rewards program*

Author(s)	CCB - Centre for Cybersecurity Belgium (BE)
Funding (if available)	N.A.
Scope of the measure	National
Role and responsibilities of stakeholders	Centre for Cybersecurity Belgium (CCB) is the national authority for cybersecurity in Belgium. There are no official stakeholders in CVDP, but CCB place themselves as an optional coordinator in the process.
Description of the good practice	A Coordinated Vulnerability Disclosure Policy (CVDP) is a set of rules determined in advance by an organisation responsible for IT systems that allows participants (or "ethical hackers") with good intentions to identify potential vulnerabilities in its systems or to provide it with all relevant information about them. A vulnerability rewards program (or "bug bounty" program) covers all rules set by a responsible organization to give rewards to participants who identify vulnerabilities in the technologies it uses.
Objectives	To encourage the implementation of bug bounty programs, providing information in form of: FAQ, Good Practices, Legal Aspects, Brochure and example CVD policy
Results	No results provided, since all of this CVDP efforts are to give information and encourage the stakeholders
Related resources	Website: https://ccb.belgium.be/en/coordinated-vulnerability-disclosure-policy-and-vulnerability-detection-reward-program-bug-bounty

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents “Not relevant” and 5 represents “Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents “Not transferable” and 5 represents “Highly transferable”:

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Any comments/suggestions you would like to provide regarding this best practice?

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CATEGORY: Reporting illegal content tool

Practice 1: *Spletno Oko*

Author(s)	Hotline Spletno Oko is part of the Safer Internet Centre, which is coordinated by the University of Ljubljana, Faculty of Social Sciences, in cooperation with partners Arnes, Slovenian Association of Friends of Youth and Centre MISSS (Youth Information and Counselling Centre of Slovenia) (SI)
Funding (if available)	Co-funded by the European Health and Digital Executive Agency (HaDEA). Financial support also comes from the Government Information Security Office.
Scope of the measure	National
Role and responsibilities of stakeholders	N/A
Description of the good practice	Spletno Oko provides a portal to report any controversial content or incident related to children sexual abuse. The portal allows to report those incidents or unauthorized content occurred or published not only in websites, but also via Social Networks, email or other channels, enlarging the scope of the reporting.
Objectives	The hotline realizes its mission by meeting the following GOALS: - Hotline operation, which allows anonymous report of illegal content on the internet; - Raising awareness about illegal online content; - Fast and effective processing of received reports; - Cooperation with other hotlines around the world, to share reports and best practices;
Results	- 846 received videos - 2268 hate speech incidents. Some additional statistics were found about key results in numbers for the year 2019. In that year, it received more than 770 hate speech reports. August was the record month with more than 200 received reports. More than 90 of those reports were forwarded to the police. The record month was also August, with 29 reports forwarded to the police.
Related resources	Website: https://www.spletno-oko.si/ Link for information: https://www.spletno-oko.si/o-prijavni-tocki/kontakt

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Any comments/suggestions you would like to provide regarding this best practice?

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CATEGORY: Guide for Businesses

Practice 1: *Cyberguide*

Author(s)	CCB - Centre for Cybersecurity Belgium (which relies on FPS -Federal Public Service- Chancellery of the Prime Minister) (BE)
Funding (if available)	Public, developed by CCB, but with the sponsorship of Cyber Security Coalition (partnership between key players from the academic world, the public authorities and the private sector) and other entities. Funding amount not available.
Scope of the measure	National
Role and responsibilities of stakeholders	Implemented in collaboration with Cyber Security Coalition
Description of the good practice	This guide provides a quick list of security controls that might or should be implemented. We have developed a list of 12 cyber security topics with basic and advanced cybersecurity recommendations SMEs can use to reduce exploitable weaknesses and vulnerabilities and defend against data breaches and cyber-attacks.
Objectives	The objective of the guide is to provide SMEs with an overview of basic and more advanced cyber security measures. This guide should enable SMEs to improve their cyber security levels, reduce cyber security risks, mitigate vulnerabilities and improve their resilience. It will provide an easy framework so that small and medium-sized enterprises can safely integrate their businesses into a worldwide round-the-clock marketplace.
Results	Review your information security plan at least annually to constantly improve the security of your organization's information. Carrying out an evaluation, which is an overview of the advances made in the security plan, its potential improvements as well as its additions, is healthy for the whole organization. The security plan on an annual basis with management. This will allow us to correct and complete but also improve the awareness of your management regarding the importance of information security and data protection.
Related resources	Website: https://cyberguide.ccb.belgium.be/en

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Any comments/suggestions you would like to provide regarding this best practice?

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CATEGORY: Establishment of a Cybersecurity Awareness Portal

Practice 1: *CyberKid*

Author(s)	Cyber Crime Unit (EL)
Funding (if available)	Hellenic Republic
Scope of the measure	National
Role and responsibilities of stakeholders	The mission of the Cyber Crime Division includes the prevention, investigation and suppression of crime and antisocial behaviour, committed through the Internet or other electronic media. The Cyber Crime Division is an independent central service, which reports directly to the Chief of the Hellenic Police. The Cyber Crime Division consists of five departments which cover the whole range of users' online protection and cyber security: - Unit of Administrative Support and Information Management; - Unit of Innovative Actions and Strategy; - Unit of Electronic and Telephone Communication Security and Protection of Software and Intellectual Property Rights; - Unit of Minors Internet Protection and Digital Investigation; - Unit of Special Cases and Internet Economic Crimes Prosecution.
Description of the good practice	An initiative of the Ministry of the Interior and Administrative Reconstruction and the Hellenic Police Headquarters, which was launched by the Cyber Crime Division, sponsored by the mobile phone, landline and internet services company "WIND HELLAS", as part of an information and awareness campaign about Internet safety, addressed to children up to 18 years old and to their parents.
Objectives	*Cyberkid* aims to help the public become familiar with the new technologies and more specifically with the Internet. The main purpose of creating Cyberkid is to promote the positive aspects of the Internet, such as having access to useful information and entertainment. Another purpose is to inform of the possible dangers hiding on the Internet.
Results	Digital Playground
Related resources	Website: https://www.cyberkid.gov.gr/en/

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Any comments/suggestions you would like to provide regarding this best practice?

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CATEGORY: Cybersecurity Awareness Portal

Practice 1: *Interactive resources about Cybersecurity*

Author(s)	OSI - Oficina de Seguridad del Internauta (ES)
Funding (if available)	NextGeneration EU
Scope of the measure	National
Role and responsibilities of stakeholders	Provide the contents of the educational resources
Description of the good practice	This initiative by the Oficina de Seguridad del Internauta provides a series of interactive educational resources that offer detection of the different smart devices that exist at home, check and protect the information shared, detect risk situations and analyse the permissions granted to the different applications downloaded.
Objectives	This project aims to aid in learning and testing one's knowledge, protecting from any threat and from cybercriminals.
Results	A series of interactive educational resources for citizens to detect the different smart devices they have at home, check and protect the information they share, detect risk situations and analyse the permissions they grant to the different applications they download. In this way, they will learn and test their knowledge, protecting themselves from any threat and from cybercriminals.
Related resources	Website: Interactive resources about cybersecurity https://www.osi.es/es/recursos-interactivos-sobre-ciberseguridad

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Practice 2: *ConcienciaT*

Author(s)	CSIRT-CV - ICT Security Centre of the Comunitat Valenciana (ES)
Funding (if available)	FEDER – European Commission
Scope of the measure	Regional
Role and responsibilities of stakeholders	Orchestrate different initiatives and campaigns proposed by the Valencian Government and the Incident Response Centre
Description of the good practice	The portal brings together a multitude of information for all audiences, levels, and ages, from infographics to help mothers and fathers manage their children's use of social or mobile networks, to advanced tool guides for security analysts on auditing of systems or detection of advanced threats.
Objectives	This new platform was created to improve the skills and knowledge of Valencian society in terms of cybersecurity, always from a practical point of view and with direct transfer of the knowledge acquired to the personal and work life of each individual.
Results	The contents are in various formats, such as simple tips in infographic or poster format, free online courses, fun videos or tutorials to configure applications step by step or electronic books for more extensive topics.
Related resources	Website: https://concienciat.gva.es/

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5
	X			

Any comments/suggestions you would like to provide regarding these best practices?

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CATEGORY: Cybersecurity Exercises Tool

Practice 1: *KYPO (Kybernetický polygon)*

Author(s)	Masaryk University (CZ)
Funding (if available)	At National and European levels
Scope of the measure	National/European/International
Role and responsibilities of stakeholders	Upon initiative of the National Cybersecurity Competence Centre (NC3) at the Masaryk University
Description of the good practice	KYPO (Kybernetický polygon) is an open-source cyber range platform. It was developed based on open-source tools at NC3 and is actively used at the institute for organising cybersecurity exercises. An important feature of the platform is that it is available open source, although onboarding is at the moment mostly based on one-to-one sessions and manual labour. Content, in the form of configurations, is not provided at the moment.
Objectives	Facilitate education and training
Results	Exercises are held two to four times a year, with smaller exercises taking place a couple of times a month, and are offered to public authorities, businesses and education providers.
Related resources	Website: https://digikoalice.cz/iniciativy/kyberneticky-polygon-muni/

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5
		X		

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5
		X		

Any comments/suggestions you would like to provide regarding this best practice?

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CATEGORY: Establishment of a Cybersecurity Awareness Center

Practice 1: *Secure Internet Center / Centro Internet Segura (SIC) Awareness Center*

Author(s)	National Cybersecurity Center (CNCS) in partnership with other entities (PT)
Funding (if available)	Public
Scope of the measure	National
Role and responsibilities of stakeholders	N.A.
Description of the good practice	The center offers Massive Open Online Courses (MOOCS). Any citizen can, free of charge, acquire skills in cyber hygiene via the offered courses. The courses are available on the NAU platform and address various topics such as the main threats in cyberspace, the care to be taken in the use of technologies, the problem of misinformation or what to do to consume information online safely, social networks, security and privacy.
Objectives	Raise awareness for online threats.
Results	Over 90000 citizens enrolled in MOOCs. The results of the awareness actives are presented in the report.
Related resources	Website: https://www.internetsegura.pt/ E-learning courses: https://www.internetsegura.pt/recursos/cursos/355

Please rate the described practice in terms of level of **relevance for the Cybersecurity awareness enhancement, using** the Lickert scale in which 1 represents "Not relevant" and 5 represents "Highly relevant):

Not relevant 1	Slightly relevant 2	Relevant 3	Fairly relevant 4	Highly relevant 5

Please rate the described practice in terms of level of **transferability to other areas of Cybersecurity fields,** using the Lickert scale in which 1 represents "Not transferable" and 5 represents "Highly transferable":

Not transferable 1	Slightly transferable 2	Transferable 3	Fairly transferable 4	Highly transferable 5

Any comments/suggestions you would like to provide regarding this best practice?

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union