REWIRE
CYBERSECURITY SKILLS ALLIANCE

Co-funded by the Erasmus+ Programme of the European Union

**REWIRE** - Cybersecurity Skills Alliance

**A New Vision for Europe**

# R5.3.1 REWIRE Fiches

| | |
|---|---|
| **Title** | R5.3.1 REWIRE Fiches |
| **Document description** | This document 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** | 19/05/2022 |

| **Revision history** | Author(s) | Contributor(s) | Delivery date | Summary of changes and comments |
|---|---|---|---|---|
| **Version 01** | Ainhoa Segurola Uli (EfVET), Valentina Chanina (EfVET) | Sara Ricci (BUT), Yianna Danidou (EUC) | 28/02/2022 | Draft inputs from partners |
| **Version 02** | Ainhoa Segurola Uli (EfVET), Valentina Chanina (EfVET) | Argyro Chatzopoulou (ApiroPlus Solutions), Fotini Georga (HLSA) | 24/03/2022 | First draft of the collection of initiatives from partners |
| **Version 03** | Ainhoa Segurola Uli (EfVET), Valentina Chanina (EfVET) | Argyro Chatzopoulou (ApiroPlus Solutions), Petros Portokalakis (TUC), Manos Athanatos (TUC) | 09/04/2022 | Draft of collection of initiatives and actions |
| **Version 04** | Ainhoa Segurola Uli (EfVET), Valentina Chanina (EfVET) | Argyro Chatzopoulou (ApiroPlus Solutions), Petros Portokalakis (TUC), Manos Athanatos (TUC) | 25/04/2022 | First complete draft for reviewing |



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

| | | | | |
|---|---|---|---|---|
| **QA Review** | Kahl Gunter (TÜV Austria), Dirma Virgilijus (INFOBALT) | | 18/05/2022 | REWIRE Quality Assurance Review |
| **Final Version** | Ainhoa Segurola Uli (EfVET), Valentina Chanina (EfVET) | | 19/05/2022 | Final version after QA review |

## Disclaimer:

# CONTENTS





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

# 1. INTRODUCTION

New technologies and the digital world develop at such a fast speed that sometimes we cannot even process and deal with the greatest success we would like to. That rapid development also leads to an increase of cyberattacks, but it is not the only factor that causes this increment. In fact, COVID-19 is probably the clearest and most recent example of it and its impact has been a challenge to all of us [1]. Cybersecurity has seen the need to be reinforced and strengthened. However, there are still several skills shortages, gaps and mismatches. According to the $(ISC)^2$, "despite another influx of 700,000 professionals into the cybersecurity workforce, the 2021 study shows that global demand for cybersecurity professional continues to outpace supply" [2].

To document and promote concrete best and good practices that aim to address skills shortages and mismatches as well as fostering multi-stakeholder partnerships, it is first necessary to identify a wide range of initiatives or actions that have been carried out with the same objective. In this way, a much broader spectrum is obtained and will help to finally select the most effective and promising cases.

This report is therefore the first of a series of them that will form the REWIRE Fiches. It compiles a first collection that has been carried out by reviewing the cybersecurity strategies of multiple European countries, from which different initiatives and actions have been identified and selected.

Independently and pending a more comprehensive analysis in the lifetime of the REWIRE project, this report will highlight two aspects above all others: the categories created to group the initiatives selected, and the example of one of the initiatives that could later be classified as a concrete good practice.

This report is structured as follows:

- Section 2 describes the methodology that has been followed to develop this report.
- Section 3 examines and provides a short description of the different categories that have been created to facilitate the identification and collection of the initiatives selected.
- Section 4 offers an overview of the initial results obtained from the categorization process.
- Section 5 showcases one of the collected initiatives and highlights its features and characteristics.
- Section 6 reconsiders the previous sections and provides few conclusions.

# 2. METHODOLOGY

In the preparation of this report, a series of steps have been followed – all of them consecutive and linked – to obtain the desired result. In total, the report has required a five-step process, as follows:

1. **Definition of purpose:** The first step consisted of structuring and detailing the aim of this report, which included understanding the overall goal.



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. **Review of the cybersecurity strategies in different countries:** The second step of the process was to investigate the cybersecurity strategies of different European countries and find the appropriate information to proceed with the next step.
3. **Identification and selection of the initiatives:** To give continuity to the review of the different cybersecurity strategies, the next step was to identify and select those initiatives that met the requirements to achieve the objective of this report. It is important to stress that only official actions of the national cybersecurity authorities of each country have been considered.
4. **Categorization:** The fourth step was to make a compilation of the collected initiatives or actions and include them in different categories according to the purpose of each of them. In this way, this report covers a total of 16 categories, which will be explained later in this report.
5. **Analysis of the results:** The fifth and last step was to analyze the different categories and set out on a percentage scale the relationship between them and the number of initiatives or activities in each category.

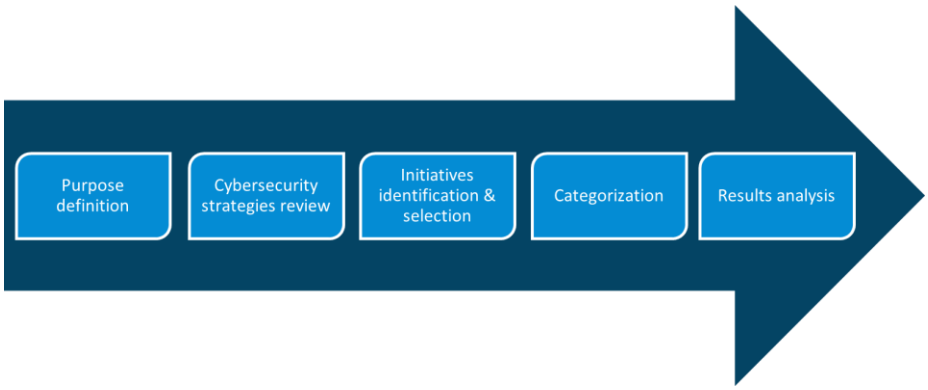


*Figure 1. Methodology used for this report.*

# 3. CATEGORIES

This report has aimed to collect as many initiatives or actions as possible, with the anticipation that it will be used as a basis for further study and analysis and will serve the purpose of this part of the REWIRE project, that is to identify and promote best and good practices aiming at addressing skills and shortages as well as fostering multi-stakeholder partnerships.
The existence of the skills gap and shortages in the field of cybersecurity is undeniable, as is the effort made over the last years to address this challenge at the European level. For the elaboration of this report, as briefly explained in the previous chapter, initiatives implemented by different countries that aimed at least one way of addressing the skills gap and shortages were analyzed.
To facilitate and simplify the collection of all of them, we proceeded to group and categories them according to their general objective. In total, we obtained sixteen categories, named: awareness campaigns (1), education, training and awareness prioritization (2), higher education courses (3), awareness tools (4), establishment of a cybersecurity organization (5), dedicated training programs (6), bug bounty programs (7), reporting illegal content tools (8), guide for businesses (9), establishment of a cybersecurity awareness portal (10), cybersecurity awareness portal (11), partnership between academic world, public authorities



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

and private sector (12), awareness app (13), teach the teachers (14), cybersecurity exercises tool (15), and establishment of a cybersecurity awareness center (16).

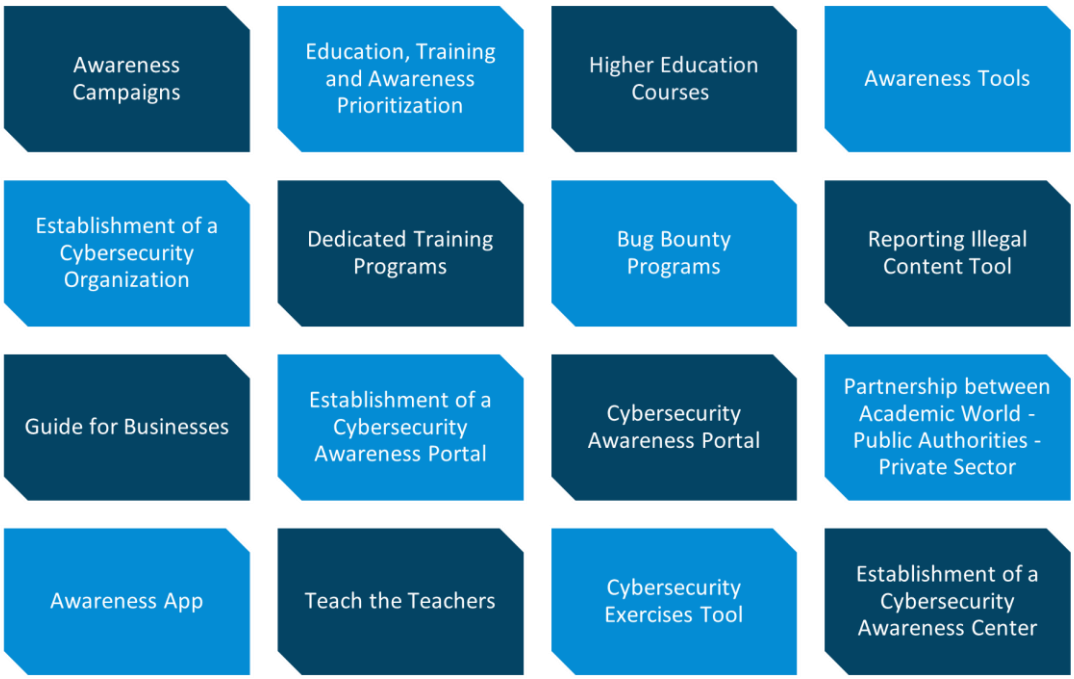


***Figure 2. Categorization of the identified initiatives.***

We will now proceed to briefly describe each of the categories, although the names themselves give a clear idea of the type of actions or initiatives that could be included in them.

## 3.1. Awareness Campaigns

Among the different types of initiatives or actions that countries in Europe have been taking, the most frequent and of which the largest number we have identified are those that aim to raise awareness amongst citizens in general and students at different education levels.
In total, there were 35 awareness campaigns identified in 23 different countries from the European Union. Some of them are campaigns designed *per se* as a form of awareness-raising, while others are part of the framework of activities within a cybersecurity organization, for example.

## 3.2. Education, Training and Awareness Prioritization

The initiatives included in this category involve those actions aimed at giving priority to the educating, training, and raising awareness on cybersecurity and digitalization. Most of them are part of the national cybersecurity strategies of each country, especially on the creation of a safe use of cyberspace.
The total number of actions regarding education, training and awareness prioritization is of 29, distributed among 21 countries.



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

## 3.3. Higher Education Courses

At higher educational level, initiatives have become more and more common. This category includes bachelor's and master's degrees, among which students will have not only a theoretical part, but also a practical one through internships done at the end of the different degrees. Providing the correct education in cybersecurity will allow to prepare students become proficient workers in the present field to protect the European Infrastructure Area.
The total number of courses founded in higher education is of 198 (although this number is in constant change due to the introduction of new courses). Among those 198, 137 higher education courses were found on ENISA's CyberHEAD database [3] and 61 advanced training courses on CONCORDIA's map [4].

## 3.4. Awareness Tools

The awareness tools play a crucial role in cybersecurity and are highly relevant to contain security systems so as to prevent cyberattacks.
In this case, there a total of 22 actions regarding awareness tools have been collected, distributed in 10 different countries.

## 3.5. Establishment of a Cybersecurity Organization

This category refers to the initiatives or actions that aim to build an organization that could serve as the reference to different institutions and stakeholders in the field of cybersecurity. In Europe, we have identified up to now 8 countries that have established a cybersecurity organization, and there are in total 12 of them.

## 3.6. Dedicated Training Programs

Education is a key part of addressing the skills gap and shortages in cybersecurity. Therefore, creating training programs is one of the categories we included in this issue. Dedicated training programs seem to be more appealing for most of the students for different reasons: on one hand, they have a shorter duration compared to other educational possibilities; on the other hand, these kinds of courses tend to be more practical than theoretical.
In this case, we have identified and selected 11 training programs that take place in 10 different countries.

## 3.7. Bug Bounty Programs

Bug bounty programs (BBP), known also as vulnerability rewards programs (VRP), are initiatives that offer a reward to those individuals who discover and report software bugs [5]. Many websites, organisations and software developers included this action, by which users can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities [6]. In the case of member state countries of the EU, the programs implemented are vulnerability disclosure programs (VDP). Unlike VRPs,



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

vulnerability disclosure programs [7] do not reward money, yet there are cases where they reply with a formal letter or a small token of appreciation.
We selected 8 programs distributed in 8 European countries.

## 3.8. Reporting Illegal Content Tools

Approaching the categories in which a smaller number of initiatives or actions were found and/or selected, but that have also a great importance, we included the reporting of illegal content. Illegal web pages and content can be found everyday and everywhere on the internet, and all of them can damage the life of many citizens all over the Union by stealing money, fake news, and so on.
In this aspect, we selected 5 initiatives or actions that serve as tools to report illegal content, and that are existent in 5 different countries.

## 3.9. Guide for Businesses

The category Guide for Businesses includes few initiatives that include tools and guides for businesses to prevent their organizations from suffering harmful activities or attacks. They are thought to bring businesses and organizations with the right and proper information, to maintain their security and be protected from the unknown.
There were 3 different initiatives selected for this category, distributed in two countries (Belgium and Norway).

## 3.10. Establishment of a Cybersecurity Awareness Portal

This category refers to the initiatives taken by some countries with the aim of establishing a cybersecurity awareness portal. These tools are of great interest to be able to have an overview of the issues and measures concerning cybersecurity.

## 3.11. Cybersecurity Awareness Portal

Similar to the previous category, we found some existing cybersecurity awareness portals that have the same objectives. These portals provide citizens with the necessary information about cybersecurity and help everyone to be aware of the issues and concerns about it.
For this category, we have selected two initiatives implemented by 2 different countries.

## 3.12. Partnership between Academic World – Public Authorities – Private Sector

The skills gap and shortages in cybersecurity requires, with no doubt, cooperation between different actors. For this reason, we have included a category for the partnership between the academic world, public authorities and private sector. However, these partnerships do not seem to be very noticeable, thus we identified and selected only two initiatives.



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

### 3.13. Awareness App

A different category where 2 actions were selected is the one referring to apps created with the purpose of raising awareness among citizens. These apps are a very useful and practical way of making everyone more aware of the importance of this issue and could have a great impact in addressing the skills gap and shortages.

### 3.14. Teach the Teachers

The lack of preparedness among teachers is another of the factors that affect the skills gap in cybersecurity education. Therefore, it is essential to have teachers that are correctly and highly skilled and prepared in the cybersecurity field. For this reason, the category Teach the Teachers would encompass initiatives or actions that aim to prepare and teach the teachers. For this category, we selected 2 initiatives implemented by 2 European countries.

### 3.15. Cybersecurity Exercises Tool

One of the last categories, in which only one initiative has been included for the time being, is the one that refers to the cybersecurity exercises tools. This category involves initiatives or actions that developed a tool to practice the theory learnt in cybersecurity with simulated exercises or practices.

### 3.16. Establishment of a Cybersecurity Awareness Centre

Finally, we included an initiative that aims to establish a cybersecurity awareness center. The importance of creating these centers is due to the need of having an organisation in which all the issues and data could be collected.

## 4. RESULTS

After identifying and selecting the multiple initiatives and categorizing them as we have seen above, the next step was to check the content of each of the categories, which would give us an idea of which types of activities or actions are stronger or, at least, more frequent up to now. The content of each category refers to the number of initiatives or actions that were identified and/or selected within each one of them. In total, 162 initiatives or actions were collected, and afterwards they were divided to include each one within their correspondent or appropriate category.
As we will see in the chart below, the differences between the different categories and the corresponding number of initiatives or actions are greater or lesser between them, but overall existent and noticeably visible.
The following chart represents the percentage of initiatives identified in each category in a descending order, namely, starting from the category with the most initiatives to the one with the least of them.



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

| Row Labels | Count of Activity or Action or Entity Present |
|---|---|
| Awareness campaigns | 21,60% |
| Education, Training & Awareness Prioritization | 17,90% |
| HE Courses | 14,81% |
| Awareness Tools | 13,58% |
| Establishment of a Cybersecurity Organization | 7,41% |
| Dedicated training programs | 6,79% |
| Bug Bounty Program | 4,94% |
| Reporting illegal content tool | 3,09% |
| Guide for Businesses | 1,85% |
| Establishment of a Cybersecurity Awareness Portal | 1,85% |
| Cybersecurity Awareness Portal | 1,23% |
| Partnership between Academic World - Public Authorities - Private Sector | 1,23% |
| Awareness app | 1,23% |
| Teach the teachers | 1,23% |
| Cybersecurity Exercises Tool | 0,62% |
| Establishment of a Cybersecurity Awareness Center | 0,62% |
| **Grand Total** | **100,00%** |

Without further analysis, the table clearly shows that there is a big difference between awareness campaigns (21,60%) and, for example, cybersecurity exercises tools or the establishment of a cybersecurity awareness center (0,62%).

# 5. SLOVAK SAFER INTERNET CENTRE

In this chapter we will provide a detailed example of 1 of the 162 initiatives or actions we selected. As the next steps will be to identify, document and promote good and best practices that aim to address the skills gap and shortages in cybersecurity, we consider it useful to detail what kind of features or characteristics we have considered for that purpose. The case we are going to present here is therefore the so-called “Slovak Safer Internet Centre” or SK SIC, which was created in Slovakia.

The Slovak Safer Internet Centre has three different dimensions:

- Awareness centre
- Helpline
- Hotline


*Figure 3. Composition of the SK SIC*



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 Slovak Safer Internet Centre is, overall, an awareness center that aims to strengthen awareness through campaigns and resources targeted to children, parents, teachers, etc. The main objective of these awareness campaigns is to give children and young people the needed digital skills and tools to take advantage and experience a safe use of the Internet, promoting awareness of parents and children themselves. In addition, SK SIC provides feedback – both qualitative and quantitative – at the European level based on the evaluation of the impact of their work. Finally, the Slovak Safer Internet Centre also establishes and maintains partnerships and promotes dialogue and exchange of information among different stakeholders at a national level.
The Slovak Safe Internet Centre has been operating since 2007 and in the past years, it has been positioned very high in protecting children and the youth in virtual space. The most remarkable effects or results of the SK SIC are: 1) contributing to best practices in Europe and globally through the number of tools developed; 2) operating eight websites, five social media pages that encompass millions of views and downloads; 3) disseminating almost one million offline tools; 4) training adults and children and empowering young people.

| | |
|---|---|
| **Name** | Slovak Safer Internet Centre (SK SIC) |
| **Country** | Slovakia |
| **Target group** | Citizens |
| **Objectives** | 1. Inform children, parents, and teachers about better and safer use of the Internet<br>2. Build enhanced digital resource centres in cooperation with third parties (schools, industry). |
| **Description** | The SK SIC was founded in 2007 and has been implementing the goals and aims of the Safer internet and Safer internet Plus programme since then. Zodpovedne.sk centre (Slovak Safer Internet Centre) is responsible for raising awareness on the safe use of the Internet, mobile communications and new technologies and crime-control performance. The website also has a section on threats, e.g. intolerance on the web, cyber bullying, to which schoolchildren may be exposed to. |
| **Measurable results (if any)** | 1. Developed 1,856 tools<br>2. Operates 8 websites and 5 social media pages, having in total 14,1 million view and almost 7 million downloads of online tools.<br>3. Trained over 50,000 adults and 123,000 children/youth.<br>4. Received over 20 awards. |
| **Website** | https://www.zodpovedne.sk/index.php/en/ |

***Table 1. Slovak Safer Centre***



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

# 6. SUMMARY AND CONCLUSIONS

The principal goal of this report was to collect different initiatives or actions that aim to address the skills gap and shortages in cybersecurity. The methodology for the report was developed in a five-step process, as follows:

- Definition of the purpose
- Review of the cybersecurity strategies in different countries
- Identification and selection of the initiatives
- Categorization
- Analysis of the results

In summary, 162 initiatives were identified and/or selected during the process and then categorized into 16 different groups, depending on their objectives or uses of each. We have seen that some categories include a higher number of initiatives or actions, which implies that more efforts are done on certain aspects than others to address the same issue, which is the skills gap and shortages in cybersecurity.

Based on this report and the research done before writing it, we believe that European countries have been working to address the cybersecurity skills gap. However, the problem persists and much more seems to be needed to deal with it. Consequently, the next steps of the REWIRE project on this side will be to conduct a survey and deepen the analysis and research of the initiatives collected for this report. The final result will consist of identifying, documenting and promoting good and best practices aiming at addressing skills and shortages as well as fostering multi-stakeholder partnerships.



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. REFERENCES

[1] Nabe, C. (2020, December 15). *Impact of COVID-19 on Cybersecurity*. Deloitte Switzerland. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

[2] (ISC)$^2$ (2021). Cybersecurity Workforce Study, 2021. Retrieved in April 2022 from https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

[3] ENISA. Cybersecurity Higher Education Database (CyberHEAD). https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead#/

[4] CONCORDIA. Courses and trainings for professionals map. https://www.concordia-h2020.eu/map-courses-cyber-professionals/

[5] Tech Target Contributor (2017, July). *Bug Bounty Program.* Techtarget. https://www.techtarget.com/whatis/definition/bug-bounty-program

[6] Google Bug Hunters. Google and Alphabet Vulnerability Reward Program (VRP) Rules. https://bughunters.google.com/about/rules/6625378258649088/google-and-alphabet-vulnerability-reward-program-vrp-rules

[7] YesWeHack. Vulnerability Disclosure Policy. https://www.yeswehack.com/companies/how-vdp-works-vulnerability-disclosure-policy/



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

# 8. LIST OF ABBREVIATIONS AND ACRONYMS

| Abbreviation | Explanation/ Definition |
|---|---|
| BBP | Bug Bounty Program |
| CyberHEAD | Cybersecurity Higher Education Database |
| CONCORDIA | Cyber security cOmpeteNce fOr Research anD InnovAtion |
| EfVET | European Forum of Technical and Vocational Education and Training |
| ENISA | European Union Agency for Cybersecurity |
| SK SIC | Slovak Safer Internet Centre |
| TUC | Technical University of Crete |
| VDP | Vulnerability Disclosure Program |
| VRP | Vulnerability Rewards Program |

*Table 2. List of abbreviations and acronyms*



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

# 9. LIST OF FIGURES



# 10. LIST OF TABLES





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