|  |  |
| --- | --- |
| **Regional Preparatory Meeting for WTDC-17 for Europe (RPM-EUR)**  | P:\SUP\Logos\Post-150th Anniv\ITU-logo-UNblue.jpg |
| **Vilnius, Lithuania, 27-28 April 2017** |
|  |  |
|  | **Document** **RPM-EUR17/****37-E** |
| **27 April 2017** |
| **Original:** **English** |
|  |
| **Montenegro** |
| REGIONAL INITIATIVE ON ENHANCING TRUST AND CONFIDENCE IN THE USE OF ICTS |

|  |
| --- |
| **Priority area:**Priority setting for Regional Initiatives, related projects and financing mechanisms**Summary:**Child online protection (COP) has been addressed as a global concern by the International Telecommunication Union (ITU) for many years with sustained cooperation through a network of partners who have put forward tools and mechanisms to further enhance collaboration and implement actions at the regional and national levels. The Sustainable Development Goals cover the issue of child online protection.Awareness Forums and platforms for dialogues for the youth and for experts have been provided on an annual basis as part of the existing regional initiatives, including the European one. Furthermore projects for the implementation of computer incident response teams (CIRTs) have been undertaken together with a surveys of initiatives by countries. Europe region is also home to expertise in this specific area which can be shared within the region and internationally through various platforms.Taking into account results achieved during the implementation of the Regional Initiaitve from 2015 and 2017, it is proporsed to retain and reinforce regional initiative for Europe on enhancing trust and confidence in use of ICTs.**Expected results:**TDAG is requested to examine this document.**References:**WTDC Resolution 17 (Rev. Dubai, 2014) |

**Proposal**

To reiterate the need to maintain ITU assistance to countries in need through actions on building capacity to effectively protect national infrastructure and citizens from cyber attacks including awareness especially to youth and children, enhancing relevant organization structures to manage and respond to incidents, assessment of Government commitment and country preparedness, elaboration and review of strategic action plan with alignment to regional and national socio economic development vision and SDGs

**Summary:**

Child online protection (COP) has been addressed as a global concern by the International Telecommunication Union (ITU) for many years with sustained cooperation through a network of partners who have put forward tools and mechanisms to further enhance collaboration and implement actions at the regional and national levels. The Sustainable Development Goals, especially Goals 4, 5, 9 and 16, cover the issue of child online protection. Goal 9, in particular, on building resilient infrastructure, promoting inclusive and sustainable industrialization and fostering innovation, demands responsible usage of information and communications technologies.

Awareness Forums and platforms for dialogues for the youth and for experts have been provided on an annual basis as part of the existing regional initiatives, including the European one. Furthermore projects for the implementation of computer incident response teams (CIRTs) have been undertaken together with a surveys of initiatives by countries. Europe region is also home to expertise in this specific area which can be shared within the region and internationally through various platforms.

Taking into account the results achieved during the implementation of the Regional Initiaitve from 2015 and 2017, it is proposed to retain and reinforce the Regional Initiative for Europe on Enhancing trust and confidence in use of ICTs.

**Expected results:**

Assistance to the countries in need in the following:

- Providing regional platforms for building human capacities in filed of enhancing confidence and trust in use of ICTs, including those addressing Child Online Protection

- Sharing of country and regional best practices, case studies and conducting surveys on enhancing trust and confidence in the use of ICTs

- Elaborating or reviewing National Cybersecurity Strategies

- Conducting Cybersecurity assessments

- Setting up or enhancing National Computer Incident Response Teams

- Conducting simulation exercises such as cyberdrills at national and regional level

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_