

**Document Number: WSIS+10/4/33**

**Note: This document is a clean version of the 1st reading to facilitate discussions in the 4th Physical meeting to be held on 14-17 April 2014.**

**Document Number: V2/C/ALC5**

Note: This document is the **result of the first reading of the document number V1.1/C/ALC5**

and reflects the changes and comments received at the second physical meeting of the WSIS+10 MPP. This document is available at: <http://www.itu.int/wsis/review/mpp/pages/consolidated-texts.html>

This document has been developed keeping in mind the [Principles](http://www.itu.int/wsis/review/mpp/pages/consolidated-texts.html).

Please note that the Geneva Declaration and the Geneva Plan of Action still remain valid until further decisions by the General Assembly.

Draft WSIS+10 Vision for WSIS Beyond 2015

С5. Building confidence and security in the use of ICTs

1. **Vision**

[Confidence, safety, trust and security in the use of ICTs are among the main pillars and prerequisites for building the information society. We should all collectively strive not only to make ICTs safer for everyone, especially the vulnerable, but also endeavor to build an information society that everyone can have equitable access to, have trust in and feel confident about by ensuring universal human rights, including the right to freedom of expression and privacy. ]

[Enshrined in Article 19 of the ICCPR and other international documents and other important human rights like right to education …]

1. **Pillars**
2. Encourage greater cooperation at the national, regional and international levels among all stakeholders in building confidence and security in the use of ICTs.
3. Use, promote and develop international [legal] frameworks [(legal or other)]for cooperation, and regulation focused on the elaboration of norms and principles that promote mutually reinforcing goals of greater security and protection in the use of ICT. [against cybercrime cyber-attacks/ malicious cyber activity and the protection of universal human rights, - [in particular , the right to education , to development, to culture, to religious freedom, and the rights of to freedom of expression, access to information and privacy, ]as well as the right of along with the right of access to communication/ICT without discrimination. ]
4. Support greater development and implementation of international standards for security; encourage their adoption and to their adherence. Assist developing and least developed countries to participate in global standards development bodies and processes.
5. Encourage and strengthen support for the establishment of [authorized] national and regional Computer Incident Response Teams (CIRTs) for incident management and regional and international coordination among them, for real-time handling and response of incidents, especially for national critical infrastructures, including information infrastructure. [Also, promote collaboration among CIRTs at the regional and global level by encouraging their participation in regional and global projects and organizations.]
6. Continue to encourage the building of a “culture of cybersecurity [in the use of ICTs]” at the national, regional and international levels through [public-private partnerships], awareness raising and training, especially for the general public - providing assistance to developing and least developed countries in this regard.
7. Promote, through international [multistakeholder] [frameworks/ approach] [legal and /or multistakeholder] [if needed], respect for privacy rights, data and consumer protection, [in particular for applications and services hosted on cloud-based platforms].
8. Ensure special emphasis for protection and empowerment of the vulnerable people, especially children, online. In this regard, governments and other stakeholders, [especially civil society], should work together to help all to enjoy the benefits of ICTs in a safe and secure environment.
9. Recognize the importance of the concept of “security by design”, [especially amongst the business sector] when providing products and services.
10. [Ensure that critical infrastructure is managed by professionals in ICT so that trust can be assured. ICT professionalism means operating at a higher standard of ICT practice than that which may be in place today. This will mean that ICT professionals will undertake ongoing continuing professional development, commitment to a code of ethics and professional conduct and have regard to the society which they serve and which will hold them accountable, in this way trust will be assured.]
11. Promote the development of assessment criteria to measure and monitor the, confidence and security aspects in the use of ICTs.
12. [Recognizing the national cyber sovereignty of countries and respecting the national cyber security of countries by all of the stakeholders.]

k bis) [State sovereignty and international norms and principles that flow from sovereignty applied to state conduct of ICT related activities and to their jurisdiction over ICT infrastructure within their territory ].

l)

m) [Promote confidence and trust in electronic environments/ [cyberspace] globally by encouraging secure cross border flows of information, including electronic documents.]

1. **Targets**
2. [Overall readiness in the field of confidence and security in the use of ICTs in all countries should be improved by 40% by 2020 – with specific focus on developing countries, including least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. The assessment of readiness in the field of confidence and security in the use of ICTs should take into account the current level of penetration of ICTs.
3. Building transborder space of confidence and security in the Internet at the international and regional levels by 2020.
4. Ensuring [maximum] level of child on-line protection by 2020.]