

**Document Number: V1.1/C/ALC5**

Note: This document consolidates the comments received by WSIS Stakeholders from the 9th October to 17th November. All the detailed submissions are available at:

<http://www.itu.int/wsis/review/mpp/pages/consolidated-texts.html>

This serves as an input to the 2nd Physical meeting and could be considered as the proposal for the 1st draft to be considered by the meeting.

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 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.

**2. Pillars**

1. Encourage greater cooperation at the national, regional and international levels among all stakeholders in building confidence and security in the use of ICTs.
2. Developinternational frameworks for cooperation, focused on the elaboration of norms and principles that promote mutually reinforcing goals of greater security and protection against cyber-attacks, and the protection of universal human rights - in particular the rights to freedom of expression, access to information and privacy, along with the right of access to communication/ICT.
3. 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.
4. 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.
5. Continue to encourage the building of a “culture of security 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.
6. Promote, through international multistakeholder frameworks if needed, respect for privacy rights, data and consumer protection, including for applications and services hosted on cloud-based platforms.
7. Ensure special emphasis for protection of the vulnerable, especially children, online; In this regard, governments and other stakeholders, especially civil society, should work together to help the vulnerable enjoy the benefits of ICTs in a safe and secure environment.
8. Recognize the importance of the concept of “security by design”, especially amongst the business sector when providing products and services.
9. 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.
10. Promote the development of assessment criteria, and related monitoring for the confidence and security in the use of ICTs.
11. Recognizing the national cyber sovereignty of countries and respecting the national cyber security of countries by all of the stakeholders.

**3. Targets**

1. 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.
2. Building transborder space of confidence and security in the Internet at the international and regional levels by 2020.
3. Ensuring [maximum] level of child on-line protection by 2020.