**Document Number: V2.1/C/ALC5**

Note: This document compiles all the submissions received from WSIS Stakeholders between 19th December 2013 to 24th January 2014. All the detailed submissions are available at

http://www.itu.int/wsis/review/mpp/pages/consolidated-texts.html (reference: purple documents).

This document also includes the main outcomes of the second physical meeting .

The document serves as an input to the third physical meeting of the WSIS+10 MPP.

**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 …]

* **Japan, Government:**
* **ISOC, Civil Society:** [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 to create trusted and safe ICTs environments, where all stakeholders can fully enjoy the benefits from new technologies in full confidence .**Canada, Government:** [Confidence, safety, trust and security in the use of ICTs are among the main pillars and prerequisites for building theinformation 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 opinion and expression and privacy rights. ]

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

* **Internet Democracy Project, CDT, IFLA and Access, Civil Society**

 Confidence, 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 the use of ICTs more secure for everyone, especially the vulnerable, but also endeavor to build an information society that enables equitable access to, and trust and confidence in ICTs, by ensuring respect for universal human rights [in particular the right to privacy[Enshrined in Article 19], enshrined in the Universal Declaration of Human Rights, the International Covenant for Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights.

* **Brazil, Government:** [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 enables equitable access and ensures protection for universally accepted fundamental human rights.

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

* **Center of Technology and Society, Civil Society:**

[Access, confidence 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 enables equitable access and ensures protection for universally accepted fundamental human rights

[as enshrined in the Universal Declaration of Human Rights, the International Covenant for Civil and Political Rights, and the International Covenant on Economic, Cultural, and Political Rights.]

* **ICANN, Civil Society:** [Confidence, safety, trust and security in the use of knowledge and information technologies are among the main pillars and prerequisites for enabling the information society. We should all collectively strive not only to make knowledge and information technologies 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 …]

**2. Pillars**

**[New Pillar, Uruguay Government]:** Strengthen existing mechanisms at national, regional and international level for cooperation in building confidence and security in the use of ICTs. *🡪**We agree with all the [ ]*

1. Encourage greater cooperation at the national, regional and international levels among all stakeholders in building confidence and security in the use of ICTs.
* **Czech Republic, Government**: Encourage greater cooperation at both regional and international levels among all stakeholders in building confidence and security in the use of ICTs.
* **Internet Democracy Project, CDT, IFLA and Access, Civil Society:** Encourage greater cooperation at the national, regional and international levels among all stakeholders in building confidence and security in the use of ICTs, in particular through the establishing and strengthening of national and regional Computer Incident Response Teams (CIRTs) and regional and international coordination among them.
* **ICANN, Civil Society:** Encourage greater cooperation and collaboration at the national, regional and international levels among all stakeholders in building confidence and security in the use of knowledge and information technologies.
1. 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. ]
* **Czech Republic, Government**: Use, promote and develop international [legal] frameworks [(legal or other)]for cooperation, focused on the elaboration of norms and principles that promote greater security and protection in the use of ICT, l human rights, - as well as the right of access to ICT.
* **Japan, Government:** Use, promote and develop international multi-stakeholder frameworks for cooperation,, respect for privacy rights, data and consumer protection.
* **ISOC, Civil Society:**  Promote frameworks that reinforce greater safety and confidence in the use of ICTs. **Canada, Government:**
* **Internet Democracy Project, CDT, IFLA and Access, Civil Society:** Use, promote, and develop international frameworks for cooperation among all stakeholders focused on the elaboration of norms and principles that promote the mutually reinforcing goals of greater security and confidence in the use of ICTs and the protection of universal human rights.
* **Brazil, Government:** Use, promote and develop international legal and transparent frameworks for cooperation, and regulation focused on the elaboration of norms and principles that promote both greater security and protection of universal human rights in the use of ICTs.
* **Center of Technology and Society, Civil Society:**

Use, promote and dDevelop international frameworks for cooperation, and regulation focused on the elaboration of norms and principles that promote both greater security and the protection of universal human rights in the use of ICTs.

* **ICANN, Civil Society:** Use, promote and develop international [legal] frameworks [(legal or other)]for cooperation, and collaboration focused on norms and principles that promote mutually reinforcing goals of a healthy, sustainable and resilient knowledge and information technology ecosystem. . [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. ]

**United Kingdom, Government:** Use, promote and develop international frameworks for cooperation 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, -

1. 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.
* **Japan, Government:** Assist developing and least developed countries to participate in global standards development bodies and processes.
* **ISOC, Civil Society:** Assist developing and least developed countries to participate in the development of these frameworks.
* **Internet Democracy Project, CDT, IFLA and Access, Civil Society:** Support greater development and implementation of international standards for security, and assisting developing and least developed countries to participate in global standards development bodies and processes.
* **ICANN, Civil Society:** Support greater development and implementation of globally interoperable standards for knowledge and information technologies; encourage their adoption and to their adherence. Assist developing and least developed countries to participate in global standards development bodies and processes.
* **United Kingdom, Government:** 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.
1. 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.]
* **Czech Republic, Government**: Encourage and strengthen support for the establishment of 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.]
* **Japan, Government:** Encourage and strengthen support for the establishment of national and regional Computer Security Incident Response Teams (CSIRTs) for incident management and regional and international coordination among them, for real-time handling and response of incidents.

**Internet Democracy Project, CDT, IFLA and Access, Civil Society:**

* **Center of Technology and Society, Civil Society:**

Encourage and strengthen support for the establishment of national and regional Computer Incident Response Teams (CIRTs) for incident management and promote coordination among them at the regional and global level.

* **ICANN, Civil Society:** 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, and their connection to global networks. [Also, promote collaboration among CIRTs at the regional and global level by encouraging their participation in regional and global projects and organizations.]
* **United Kingdom, Government:** Encourage and strengthen support for the establishment of 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.]
1. 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.
* **Japan, Government:** Continue to encourage the building of a “culture of cybersecurity” at the national, regional and international levels through awareness raising and training to developing and least developed countries in this regard.
* **ISOC, Civil Society:** Continue to encourage the building of a “culture of cybersecurity” marked by shared responsibility and collective action 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.
* **Canada, Government:** Continue to encourage the building of a “culture of cyber security ” 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.
* **Internet Democracy Project, CDT, IFLA and Access, Civil Society:** Continue to encourage the building of a “culture of cybersecurity [in the use of ICTs]” at the national, regional and international levels through awareness raising and training, especially for the general public - providing assistance to developing and least developed countries in this regard.
* **Brazil, Government:** Continue to encourage the building of a “culture of cybersecurity [in the use of ICTs]”, including capacity building of and implementation of security measures 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.
* **Center of Technology and Society, Civil Society:** Continue to encourage tcapacity building for and implementation of security measures at the national, regional and international levels through awareness raising and training, especially for the general public - providing assistance to developing and least developed countries in this regard.
* **ICANN, Civil Society:** Continue to encourage the building of a “culture of cybersecurity [in the use of knowledge and information technologies]” at the national, regional and international levels through [public-private partnerships and collaboration initiatives], awareness raising and training, especially for the general public - providing assistance to developing and least developed countries in this regard.
1. 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].

**Japan, Government:**

* **Canada, Government:** Promoterespect for privacy rights, data and consumer protection, [in particular for applications and services hosted on cloud-based platforms].
* **Internet Democracy Project, CDT, IFLA and Access, Civil Society:**
* **Brazil, Government:** Promote, through international [frameworks/ [legal , respect for the right to privacy, data and consumer protection, [in particular for applications and services hosted on cloud-based platforms].

**Center of Technology and Society, Civil Society:**

* **ICANN, Civil Society:** Promote, through international [multistakeholder] collaboration [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].
* **United Kingdom, Government:** Promote, respect for privacy rights, data and consumer protection, [in particular for applications and services hosted on cloud-based platforms].
1. 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.
* **Czech Republic, Government**: Ensure special emphasis to prevention 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.
* **Japan, Government:** Ensure special emphasis for protection and empowerment of the vulnerable people, especially children, online. In this regard, governments and other stakeholders, should work together to help all to enjoy the benefits of ICTs in a safe and secure environment.
* **Canada, Government:** Ensure special emphasis for protection and empowerment of the vulnerable people, especially children, online. In this regard, governments and other stakeholders, ,should work together to help all to enjoy the benefits of ICTs in a safe and secure environment.

**Internet Democracy Project, CDT, IFLA and Access, Civil Society:**

* **Center of Technology and Society, Civil Society:**  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 the vulnerable to enjoy the benefits of ICTs in a safe and secure environment.
* **ICANN, Civil Society:** 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 knowledge and information technologies in a healthy, stable and resilient environment.
1. Recognize the importance of the concept of “security by design”,[ especially amongst the business sector] when providing products and services.
* **Czech Republic, Government**: R
* **Internet Democracy Project, CDT, IFLA and Access, Civil Society:** Recognize the importance of the concept of “security by design”, especially amongst the private sector when providing products and services.
* **Brazil, Government:** Recognize the importance of the concept of “security by design”, including privacy and user rights concerns, especially amongst the business sector when providing products and services.
* **Center of Technology and Society, Civil Society:**  Recognize the importance of the concept of “security and privacy by design”both at private and public sectorswhen providing products and services.
1. [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.]
* **IFIP, Civil Society:**

In order to improve confidence and security in ICTs, ensure that ICT’s development and implementation is carried out by practitioners who are recognized as skilled and competent in ICT.

**Japan, Government:**

* **Canada, Government:**
* **Internet Democracy Project, CDT, IFLA and Access, Civil Society:**
* **Brazil, Government:**
* **Center of Technology and Society, Civil Society:**
* **ICANN, Civil Society:** [Ensure that critical infrastructure is managed by professionals so that trust can be assured. Knowledge and information technology professionalism means operating at a higher standard of practice than that which may be in place today. This will mean that professionals in this field 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, to provide trust and assurances in the management in this area.]
* **United Kingdom, Government:** [Ensure that critical infrastructure is managed by professionals in ICT so that trust can be assured. ICT professionalism may mean operating at a higher standard of ICT practice than that which may be in place today. Encourage ICT professionals to undertake ongoing continuing professional development, commit 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.]
1. Promote the development of assessment criteria to measure and monitor the, confidence and security aspects in the use of ICTs.
* **Czech Republic, Government**:
* **Japan, Government:**
* **Internet Democracy Project, CDT, IFLA and Access, Civil Society:** Promote the development of assessment criteria to measure and monitor confidence and security aspects in the use of ICTs.
* **Center of Technology and Society, Civil Society:** Promote the development of assessment criteria to measure and monitor the, and related monitoring for the confidence and security aspects in the use of ICTs.
* **ICANN, Civil Society:** Promote the development of assessment criteria to measure and monitor the, confidence and security aspects in the use of knowledge and information technologies.
1. [Recognizing the national cyber sovereignty of countries and respecting the national cyber security of countries by all of the stakeholders.]
* **Japan, Government:**
* **Canada, Government:**
* **Internet Democracy Project, CDT, IFLA and Access, Civil Society:**

**Center of Technology and Society, Civil Society:**

**United Kingdom, Government:**

k bis) [State sovereignity 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 ].

* **Japan, Government:**
* **Canada, Government:** State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.
* **Internet Democracy Project, CDT, IFLA and Access, Civil Society:** [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 ].
* **Center of Technology and Society, Civil Society:**
* **ICANN, Civil Society:** [State sovereignty and international norms and principles that flow from sovereignty applied to state conduct of knowledge and information technology related activities and to their jurisdiction over knowledge and information infrastructure within their territory, respecting the global interoperable nature of this infrastructure and the networks that connect them with the greater transnational ecosystem].

l) S]

* **Japan, Government**:
* **Internet Democracy Project, CDT, IFLA and Access, Civil Society:**

**Brazil, Government:**

1. [Promote confidence and trust in electronic environments/[cyberspace] globally by encouraging secure cross border flows of information, including electronic documents.]
* **Japan, Government:**
* **Internet Democracy Project, CDT, IFLA and Access, Civil Society:**
* **ICANN, Civil Society:** [Promote confidence and trust in electronic environments/[cyberspace] globally by encouraging secure cross border flows of knowledge and information, including electronic documents.]
* APIG: new m) Recognize the need for **international agreement to cooperate on security matters** and to avoid unilateral assertions of national laws and to avoid extra-territorial actions. In this context, states shall individually and collectively endeavour to ensure the security and robustness of international telecommunication networks in a manner that respects and upholds their human rights obligations, and they should consider best practices regarding human rights, in particular those put forward by civil society organizations.

**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.]
* **Czech Republic, Government**: a) [Overall readiness in the field of confidence and security in the use of ICTs in all countries should be improved – 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.

b) Building transborder space of confidence and security in the Internet at the international and regional levels by 2020.

c) Ensuring [maximum] level of child on-line protection by 2020.]

**Japan, Government:**

**Canada, Government:**

b) c)

* **Internet Democracy Project, CDT, IFLA and Access, Civil Society:**

a) b) c)

a) By 2020 all countries should have appropriate national structures and/or CIRTs, and increased cooperation between CIRTs at regional international levels.

* **Brazil, Government:**

a) [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.

b) Building transborder space of confidence and security in the Internet at the international and regional levels by 2020.

c) Ensuring [maximum] level of child on-line protection by 2020.]

d) Establishing one CSIRT point of presence in each Autonomous System in coordination with national/regional CSIRT by 2020.

* **ICANN, Civil Society:**

a) [Overall readiness in the field of confidence and security in the use of knowledge and information technologies 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 knowledge and information technologies should take into account the current level of penetration of these technologies

b) Building transborder and transnational space of confidence and security in the Internet at the international and regional levels by 2020.

c) Ensuring [maximum] level of child on-line protection by 2020.]

* **Uruguay, Government:** By 2020, 100% of member states have established a national Computer Incident Response Team that cooperate at regional and international level