|  |  |
| --- | --- |
| **ITUPublications** | **International Telecommunication Union** |
| Resolutions | Standardization Sector |
|  |
|  |
|  | WORLD TELECOMMUNICATION STANDARDIZATION ASSEMBLY New Delhi, 15-24 October 2024 |
|  | Resolution 50 – Cybersecurity |



FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of tele­com­mu­ni­ca­tions, and information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU‑T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

© ITU 2024

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

RESOLUTION 50 (Rev. New Delhi, 2024)

Cybersecurity

(Florianópolis, 2004; Johannesburg, 2008; Dubai, 2012; Hammamet, 2016;
Geneva, 2022; New Delhi, 2024)

The World Telecommunication Standardization Assembly (New Delhi, 2024),

recalling

*a)* Resolution 130 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, on strengthening the role of ITU in building confidence and security in the use of information and communication technologies (ICTs);

*b)* Resolution 174 (Rev. Busan, 2014) of the Plenipotentiary Conference, on ITU's role with regard to international public policy issues relating to the risk of illicit use of ICTs;

*c)* Resolution 179 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, on ITU's role in child online protection;

*d)* Resolution 181 (Guadalajara, 2010) of the Plenipotentiary Conference, on definitions and terminology relating to building confidence and security in the use of ICTs;

*e)* Resolutions 55/63 and 56/121 of the United Nations General Assembly (UNGA), which established the legal framework on combating the criminal misuse of information technologies;

*f)* UNGA Resolution 57/239, on creation of a global culture of cybersecurity;

*g)* UNGA Resolution 64/211, on creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures;

*h)* UNGA Resolution 41/65, on principles relating to remote sensing of the Earth from outer space;

*i)* UNGA Resolution 76/19, on developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies;

*j*) UNGA Resolution 70/125, on the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society (WSIS);

*k)* Resolution 45 (Rev. Kigali, 2022) of the World Telecommunication Development Conference (WTDC), on mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam;

*l)* Resolution 52 (Rev. New Delhi, 2024) of this assembly, on countering and combating spam;

*m)* Resolution 58 (Rev. New Delhi, 2024) of this assembly, on encouraging the creation and enhancement of national computer incident response teams (CIRTs), in particular for developing countries[[1]](#footnote-1)1;

*n)* that ITU is the lead facilitator for WSIS Action Line C5 in the Tunis Agenda for the Information Society (Building confidence and security in the use of ICTs);

*o)* the cybersecurity-related provisions of the WSIS outcomes,

considering

*a)* the crucial importance of telecommunication/ICT infrastructure and its application to practically all forms of social and economic activity;

*b)* that the legacy public switched telephone network has a level of inherent security properties because of its hierarchical structure and built-in management systems;

*c)* that Internet Protocol (IP) networks provide reduced separation between user components and network components if adequate care is not taken in the security design and management;

*d)* that the converged legacy networks and IP networks are therefore potentially more vulnerable to intrusion if adequate care is not taken in the security design and management of such networks;

*e)* that cybersecurity is a cross-cutting issue, and the cybersecurity landscape is complex and dispersed, with many different stakeholders at the national, regional and global levels with responsibility for identifying, examining and responding to issues related to building confidence and security in the use of telecommunications/ICTs;

*f)* that the considerable and increasing losses which users of telecommunication/ICT systems have incurred from the growing problem of cybersecurity alarm all developed and developing nations of the world without exception;

*g)* that the fact, *inter alia*, that critical telecommunication/ICT infrastructures are interconnected at the global level means that inadequate infrastructure security in one country could result in greater vulnerability and risks in others and, therefore, cooperation is important;

*h)* that the number and methods of cyberthreats and cyberattacks are growing, as is dependence on the Internet and other networks that are essential for accessing services and information;

*i)* that standards can support the security aspects of all telecommunications/ICTs;

*j)* that ensuring the safety and security of emerging telecommunications/ICTs is vital for a secure cyberspace, making the development of security standards for them essential;

*k)* that in order to protect global telecommunication/ICT infrastructures from the threats and challenges of the evolving cybersecurity landscape, coordinated national, regional and international action is required for prevention, preparation, response and recovery in respect of cybersecurity incidents;

*l)* the work undertaken and ongoing in ITU, including in ITU Telecommunication Standardization Sector (ITU‑T) Study Group 17 and ITU Telecommunication Development Sector (ITU‑D) Study Group 2, and under the Kigali Action Plan adopted by WTDC (Kigali, 2022);

*m)* that ITU‑T has a role to play, within its mandate and competencies, in regard to *considering k)* of this resolution,

considering further

*a)* that Recommendation ITU‑T X.1205 provides a definition, a description of technologies and network protection principles;

*b)* that Recommendation ITU‑T X.805 provides a systematic framework for identifying security vulnerabilities, and Recommendation ITU‑T X.1500 provides the cybersecurity information exchange (CYBEX) model and discusses techniques that could be used to facilitate the exchange of cybersecurity information;

*c)* that ITU‑T and the Joint Technical Committee for information technology (JTC 1) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), as well as several consortia and standards-development entities already have a significant body of published materials and ongoing work that is directly relevant to this topic, which needs to be considered;

*d)* the importance of considering security in the use of telecommunications/ICTs as a continuous and iterative process, built into products from the beginning and continuing throughout every phase of their lifetime;

*e)* that an iterative, risk-based approach incorporating a combination of technological, process and human-based factors is key to strengthening security and resilience in the use of telecommunications/ICTs – by enabling cybersecurity practices to be developed and applied as needed to address constantly evolving threats and vulnerabilities – while also supporting innovation and emerging telecommunications/ICTs,

recognizing

*a)* the operative paragraph of Resolution 130 (Rev. Bucharest, 2022) instructing the Director of the Telecommunication Standardization Bureau (TSB) to intensify work within existing ITU‑T study groups;

*b)* that Resolution 71 (Rev. Bucharest, 2022) of the Plenipotentiary Conference adopted the strategic plan for the Union for 2024-2027, including Strategic Goal 1 (Universal Connectivity: Enable and foster universal access to affordable, high-quality and secure telecommunications/ICTs), under which the Union will focus on achieving universally accessible, affordable, high-quality, interoperable and secure telecommunication/ICT infrastructure, services and applications;

*c)* that standards are a key component of Pillar 2 (technical and procedural measures) of the ITU Global Cybersecurity Agenda (GCA), which promotes international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the use of telecommunications/ICTs, considering security aspects throughout the whole lifecycle of the standards-development process;

*d)* the challenges that States, in particular in developing countries, face in building confidence and security in the use of telecommunications/ICTs,

recognizing further

*a)* that an increasing range and variety of cyberattacks, such as phishing, pharming, scan/intrusion, distributed denials of service, web-defacements and unauthorized access, are emerging, evolving and having significant impacts;

*b)* that a range of vectors may be used to distribute bot-malware and carry out cyberattacks;

*c)* that sources of attacks are sometimes difficult to identify;

*d)* that critical cybersecurity threats in software and hardware may require timely vulnerability management, timely hardware and software updates and appropriate assignment of access rights to prevent attacks;

*e)* that securing data is a key component of cybersecurity as data are often the target in cyberattacks;

*f)* that cybersecurity is a fundamental element of building confidence and security in the use of telecommunications/ICTs;

*g)* the increasingly widespread access to telecommunications/ICTs worldwide, in particular the Internet, and use thereof by minors,

noting

*a)* the vigorous activity and interest in the development of telecommunication/ICT security standards and ITU‑T Recommendations in ITU‑T Study Group 17, the lead ITU‑T study group on security and identity management, and in other standardization bodies, including the Global Standards Collaboration group;

*b)* that there is a need for national, regional and international strategies and initiatives to be harmonized to the extent possible, in order to avoid duplication and to optimize the use of resources;

*c)* that, in addition to other cyberthreats, the cybersecurity aspects of protection of data and personally identifiable information (PII) have emerged as a major issue for Member States;

*d)* the significant and collaborative efforts by and among governments, the private sector, civil society, the technical community and academia, within their respective roles and responsibilities, to build confidence and security in the use of telecommunications/ICTs,

resolves

1 to continue to give this work high priority within ITU‑T, in accordance with its competencies and expertise, including promoting common understanding among governments and other stakeholders of building confidence and security in the use of telecommunications/ICTs at the national, regional and international level;

2 that ITU‑T study groups continue to evaluate existing and evolving ITU‑T Recommendations, according to their mandates in Resolution 2 (Rev. New Delhi, 2024) of this assembly, and refer security issues with respect to robustness of design and operation, and potential for exploitation by malicious parties, to ITU‑T Study Group 17 for consideration, and take into account new and emerging telecommunication/ICT services and technologies to be supported by the global telecommunication/ICT infrastructure;

3 that ITU‑T continue to raise global awareness of security in telecommunications/ICTs, through the development of ITU‑T Recommendations and technical reports, within its mandate and competencies, which support cybersecurity procedures, technical policies and standards frameworks, and of the importance of protecting telecommunications/ICTs against cyberthreats and malicious cyberactivity, in order to enhance organizations' development of security-related capabilities among personnel, and also continue to promote cooperation among appropriate international and regional organizations in order to enhance exchange of technical information in the field of telecommunication/ICT security, with the twin objectives of managing cybersecurity risks and protecting telecommunications/ICTs;

4 that ITU‑T should consider the needs of users and developers when developing outputs that could be used to promote cybersecurity for emerging technologies for telecommunications/ICTs;

5 that ITU‑T should consider the importance of capacity building in facilitating the adoption of standards to support cybersecurity, in particular, but not exclusively, for developing countries;

6 that ITU‑T should coordinate and collaborate with ITU‑D in this regard, both within the context of ITU‑D Study Question 3/2 (Securing information and communication networks: Best practices for developing a culture of cybersecurity) and within the context of the capacity-building work of the Telecommunication Development Bureau (BDT);

7 that relevant ITU‑T study groups should keep pace with the development of new and emerging telecommunication/ICT services and technologies, according to their mandates, in order to alert ITU‑T Study Group 17 to areas that may require new ITU‑T Recommendations, supplements and technical reports to address challenges related to cybersecurity and its aspects of data and PII protection;

8 that ITU‑T continue work on the development and improvement of terms and definitions related to building confidence and security in the use of telecommunications/ICTs, including the term "cybersecurity";

9 that global, consistent and interoperable processes for sharing information related to incident response should be promoted;

10 that ITU‑T study groups continue to liaise with standards organizations and other bodies active in this field and encourage the engagement of experts in ITU's activities in the area of building confidence and security in the use of telecommunications/ICTs;

11 that security aspects should be considered throughout the ITU‑T standards-development process;

12 that secure, trusted and resilient telecommunication/ICT networks and services should be developed and maintained to enhance confidence in the use of telecommunications/ICTs;

13 that the cyber-resilience of telecommunication/ICT networks and systems should be considered a priority in telecommunication/ICT network infrastructure and application development,

instructs Study Group 17 of the ITU Telecommunication Standardization Sector

1 to promote studies on cybersecurity, including its aspects of data and PII protection for new and emerging telecommunication/ICT services and technologies, in order to counter vulnerabilities in the use of the global telecommunication/ICT infrastructure, by developing ITU‑T Recommendations, supplements and technical reports, as appropriate;

2 to support the Director of TSB in maintaining the ICT Security Standards Roadmap, which should include work items to progress standardization work related to cybersecurity, and its aspects of data and PII protection, and the security compendium, which should include the list of ITU‑T Recommendations and terms and definitions, and share this with relevant groups of the ITU Radiocommunication Sector and ITU‑D as the mission of the ITU‑T lead study group for security;

3 to lead joint coordination activities on confidence and security among all relevant ITU study groups and other standards-development organizations, as appropriate;

4 to collaborate closely with all other ITU‑T study groups, establish an action plan for assessing existing, evolving and new ITU‑T Recommendations to address constantly evolving security threats and vulnerabilities to encourage resilience of telecommunication/ICT networks from cyberattacks, and continue to provide regular reports on security of telecommunications/ICT to the Telecommunication Standardization Advisory Group;

5 to continue to define a general/common set of security capabilities throughout every phase of the development lifecycle, such as requirements, design, implementation, verification, release and maintenance, of information system/network/application/service products, including organizations' development of security-related capabilities among personnel, so that, consequently, security by design (security capabilities and features available by design) could be achieved for systems/networks/applications from day one;

6 to continue to design one or more security frameworks or reference architectures with security functional components, including considering security interoperability among different types of systems, which could be considered as the basis of security architecture design for various systems/networks/applications in order to improve the quality of ITU‑T Recommendations on security, and provide security design references for potential applications in global telecommunication/ICT infrastructure;

7 to continue to develop and support cooperative cybersecurity analysis and tools for incident management, in order to support the work of CIRTs, in particular in developing countries;

8 to consider meeting requirements, as they are established, to develop technical standards in support of efforts for enhancing cybersecurity for minors;

9 to consider ongoing changes in telecommunications/ICTs and regularly review and revise existing ITU‑T Recommendations related to network security, in order to adapt to new security requirements and respond to new network security threats;

10 to provide the best practices for evaluating and improving cybersecurity, including its aspects of data and PII protection, in evolving telecommunication/ICT infrastructure;

11 to conduct an assessment on the impact of new and emerging telecommunications/ICTs, from the perspective of cybersecurity, identifying gaps and recommending strategies for secure adoption and use,

instructs the Director of the Telecommunication Standardization Bureau

1 to continue to maintain, in building upon the information base associated with the telecommunication/ICT Security Standards Roadmap and ITU‑D efforts on cybersecurity, and with the assistance of other relevant organizations, an inventory of national, regional and international initiatives and activities to promote, to the maximum extent possible, the worldwide harmonization of strategies and approaches in this critically important area, including the development of common approaches in the field of cybersecurity;

2 to contribute to annual reports to the ITU Council on building confidence and security in the use of telecommunications/ICTs, as specified in Resolution 130 (Rev. Bucharest, 2022);

3 to report to the Council on the progress of activities on the telecommunication/ICT Security Standards Roadmap;

4 to continue to recognize the role played by other organizations with experience and expertise in the area of cybersecurity including, *inter alia*, the cybersecurity aspects of the data and PII protection standards, and coordinate with those organizations as appropriate;

5 to continue the implementation and follow-up of relevant WSIS activities on building confidence and security in the use of telecommunications/ICTs, in collaboration with the other ITU Sectors and in cooperation with other organizations and all relevant stakeholders, as a way to share information and best practices on national, regional and international non-discriminatory cybersecurity-related initiatives globally;

6 to cooperate with the Secretary-General's GCA and other global or regional cybersecurity projects, as appropriate, in promoting capacity building and developing relationships and partnerships with various regional and international cybersecurity-related organizations and initiatives, as appropriate, and to invite all Member States, in particular developing countries, to take part in these activities and to coordinate and cooperate with these different activities;

7 to support the Director of BDT in overseeing the development of ITU‑T Recommendations and potentially other tools that the Member States, in particular developing countries, can use to anticipate rapid responses in the event of major incidents, and in helping these bodies to propose action plans using a suitable framework, as appropriate and upon request, to increase their protection, taking into account mechanisms and partnerships;

8 to support relevant ITU‑T Study Group 17 activities related to strengthening and building confidence and security in the use of telecommunications/ICTs, and to coordinate this work with the ITU‑D study groups and with the relevant programme activities;

9 to disseminate information to all stakeholders and increase stakeholders' understanding of cybersecurity through the organization of training programmes, forums, workshops, seminars, etc., as appropriate, on ITU‑T Recommendations and implementation guidelines for policy-makers, regulators, operators and other stakeholders, in particular from developing countries, to raise awareness and identify needs in collaboration with the Director of BDT;

10 to work with the regional telecommunications organizations in order to deliver knowledge and expertise to wider audiences more effectively;

11 to consider, whenever possible, raising awareness by holding workshops concurrently with the meetings of the respective regional groups of ITU‑T study groups, or events in coordination and collaboration with the Director of BDT and ITU regional offices alongside these meetings, where appropriate,

invites Member States, Sector Members, Associates and Academia, as appropriate

1 to collaborate closely in strengthening regional and international cooperation and support, taking into account Resolution 130 (Rev. Bucharest, 2022), with a view to enhancing confidence and security in the use of telecommunications/ICTs, in order to mitigate risks and address threats;

2 to cooperate and participate actively in the implementation of this resolution and the associated actions;

3 to participate in relevant ITU‑T study group activities to develop cybersecurity standards and guidelines in order to build confidence and security in the use of telecommunications/ICTs;

4 to utilize relevant ITU‑T Recommendations, technical reports and supplements;

5 to continue to contribute to ITU‑T Study Group 17 work on cybersecurity risk and cyberdefence management approaches, within the remit of ITU;

6 to continue to engage in initiatives to encourage the active participation of women in ITU‑T cybersecurity-related activities and leadership roles;

7 to adopt and support the implementation of cybersecurity measures for new and emerging telecommunication/ICTs within their jurisdictions, encouraging a secure and resilient environment for all users.

1. 1 These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. [↑](#footnote-ref-1)