|  |  |  |  |
| --- | --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **International telecommunication union**  **Telecommunication Standardization Bureau** | |  |
|  | | Geneva, 23 July 2025 | |
| **Ref:** | TSB Circular 50  SG17/XY | **To:**  - Administrations of Member States of the Union  **Copy to:**  - ITU-T Sector Members;  - ITU-T Associates of Study Group 17;  - ITU Academia  - The Chair and Vice-Chair of ITU-T Study Group 17;  - The Director of the Telecommunication Development Bureau;  - The Director of the Radiocommunication Bureau | |
| Tel: | +41 22 730 6206 |
| Fax:  E-mail: | +41 22 730 5853  [tsbsg17@itu.int](mailto:tsbsg17@itu.int) |
| **Subject:** | **Member State consultation on Determined draft new Recommendations** **ITU T X.1062 (ex X.shcd), X.1238 (ex X.sgc-rcs), X.1128 (ex X.mt-feature), X.1129 (ex X.mt-integrity), X.1130 (ex X.tg-fdma), X.1457 (ex X.str-irs), X.1753 (ex X.gdsml), X.1649 (ex X.sgmc), and revised Recommendations ITU-T X.1250 and X.1631, proposed for approval at the meeting of ITU‑T Study Group 17, Geneva,** **3-11 December 2025** | | |

Dear Sir/Madam,

1 ITU-T Study Group 17 (Security) intends to apply the Traditional Approval Procedure as described in Section 9 of WTSA Resolution 1 (Rev. Geneva, 2022) for the approval of the above-mentioned draft Recommendations at its next physical meeting, Geneva, 3-11 December 2025. The agenda and all relevant information concerning the ITU-T Study Group 17 meeting will be available in Collective letter [4/17](https://www.itu.int/md/T25-SG17-COL-0004/en).

2 The titles, summaries and locations of the draft ITU-T Recommendations proposed for approval can be found in **Annex 1**.

TSB NOTE 1 – No ITU-T A.5 justification has been submitted for any of these determined texts.

TSB NOTE 2 – As of the date of this Circular, no IPR statement had been received by TSB for any of these determined texts. For up-to-date information, members are invited to consult the IPR database at [www.itu.int/ipr/](http://www.itu.int/ipr/).

3 This Circular initiate the formal consultation with ITU Member States on whether these texts may be considered for approval at the upcoming meeting, in accordance with clause 9.4 of Resolution 1. Member States are kindly requested to complete and return the form in **Annex 2** by 2359 hours UTC on **21 November 2025.**

4 If 70% or more of the replies from Member States support consideration for approval, one Plenary session will be devoted to apply the approval procedure. Member States that do not assign authority to proceed should inform the Director of TSB of the reasons for this opinion and indicate the possible changes that would enable the work to progress.

Yours faithfully,

Seizo Onoe  
Director of the Telecommunication  
Standardization Bureau

**Annexes:** 2

Annex 1  
Summary and location of Determined draft new Recommendations   
ITU T X.1062 (ex X.shcd), X.1238 (ex X.sgc-rcs), X.1128 (ex X.mt-feature), X.1129 (ex X.mt-integrity), X.1130 (ex X.tg-fdma), X.1457 (ex X.str-irs), X.1753 (ex X.gdsml), X.1649 (ex X.sgmc), and revised Recommendations ITU-T X.1250 and X.1631

# Draft new Recommendation ITU-T X.1062 (ex X.shcd) [[SG17-R6](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0006)]

Framework for security human capability development

## Summary

Cybersecurity is a vast and constantly evolving subject that requires continuous learning and skill development. This Recommendation specifies a framework for security human capability development to provide guideline for the development of security practitioners and professionals by developing their competencies and recognising their security skills and knowledge in an organization.

# Draft new Recommendation ITU-T X.1238 (ex X.sgc-rcs) [[SG17-R7](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0007)]

Guidelines for countering spam over Rich Communication Service (RCS) messaging

## Summary

This Recommendation specifies guidance and technical enablers supporting Rich Communication Service (RCS) providers to prevent spam distribution on the basis of RCS specificities and defines spam prevention and control mechanism supported by RCS client.

This Recommendation quotes the RCS architecture as defined in GSMA [b-GSMA RCC.07] and focuses on how to mitigate spam risks of RCS messaging.

# Draft new Recommendation ITU-T X.1128 (ex X.mt-feature) [[SG17-R8](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0008)]

Security features for assessment of mobile terminal security

## Summary

Mobile terminals especially smartphones are changing people's work and lifestyle. For example, mobile payments are experiencing rapid growth as consumers use mobile terminals as part of their modern dynamic lifestyles; more enterprises support employees accessing enterprise services with personal mobile terminals; etc. However, mobile terminal security is a big challenge for mobile application services as such. For example, users may unknowingly expose their terminals to malware and put sensitive data at risk of data breaches.

This Recommendation provides security features to assess mobile terminal security and information on how relevant stakeholders could use the security features in this Recommendation.

# Draft new Recommendation ITU-T X.1129 (ex X.mt-integrity) [[SG17-R9](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0009)]

Security guidelines for mobile terminal integrity protection

## Summary

The goal of mobile terminal integrity protection is to ensure that a mobile terminal behaves in an expected manner. That means, hardware, firmware and software (e.g. operating system, pre-installed apps) on the mobile terminal have not been compromised by any means or in any way. If an attacker compromises firmware or software, or modifies the configuration of hardware (e.g. ROM, retention cells), or changes the hardware (e.g. flash memory), the attacker could control or subvert functionality of the mobile terminal.

When a mobile terminal switches on, it begins with a boot phase to verify hardware components and load one or more software modules. After that, the mobile terminal enters a runtime phase and reaches an operational state, in which the mobile terminal is ready for its intended purpose. In order to fix the vulnerabilities and weaknesses of firmware/software (FW/SW), the mobile terminal needs to be updated from time to time. This is called FW/SW update phase. Each of these phases is an opportunity for an attacker to introduce security threats to the integrity of mobile terminal.

This Recommendation analyses security threats to mobile terminal during the boot phase, runtime phase and FW/SW update phase, and defines security requirements and provides security guidelines for mobile terminal integrity protection.

# Draft new Recommendation ITU-T X.1130 (ex X.tg-fdma) [[SG17-R10](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0010)]

Technical guidelines for detecting malicious activities of mobile applications

## Summary

With the widespread use of mobile devices and applications, APPs have become a primary vector for malicious activities. For example, malicious APPs may disguise themselves as legitimate credit or shopping applications to deceive users. To detect and prevent such malicious activities, traditional approaches rely on APP Store reviews and alerts from security software installed in the mobile device. However, this solution faces several challenges. While APP Store reviews can help block malicious applications, attackers continuously develop new techniques to evade detection and bypass APP Store reviews. In addition, some malicious applications are distributed through third-party platforms where they entice users to download and install them. Mobile security software primarily focuses on detecting viruses and application vulnerabilities making it difficult to effectively identify malicious applications specifically designed to carry out malicious activities.

Malicious applications on mobile devices typically operate through four stages: download, installation, execution, and payment inducement. Each stage presents distinct risks.

During the download and installation stage, malicious applications often disguise themselves as legitimate applications to evade detection by security software. They may also implant trojans on the mobile device during this phase.

In the execution stage, these applications may steal user information through the implanted trojans or trick users into voluntarily disclosing sensitive data by mimicking legitimate applications.

In the payment inducement stage, malicious applications often build trust by offering small rewards or profits through various schemes. Once user trust is established, they lure users into transferring money. In some cases, the deception is direct, for example, by masquerading as legitimate shopping applications to exploit unsuspecting users.

The entire process of detecting and preventing malicious activities is highly complex, requiring close coordination between mobile devices and applications. This Recommendation analyses the characteristics and risks of malicious applications across multiple stages, including download, installation, execution and payment inducement, and provides a comprehensive technical solution for detecting and preventing malicious activities, based on the interactions between mobile devices and applications.

# Draft new Recommendation ITU-T X.1457 (ex X.str-irs) [[SG17-R11](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0011)]

Security threats and requirements for information recommendation service

## Summary

Information recommendation service is widely used in different websites and applications. For example, educational information recommendation service is an important factor in realizing educational information sharing. In the massive educational information, users can quickly find the educational information resources they need, meet users' learning needs, and bring users a good learning experience. However, the security issues involved in information recommendation service cannot be ignored, e.g. data integrity threats, data poisoning, evasion attacks, etc.

This Recommendation provides an analysis of security threats and requirements for information recommendation service. It identifies security threats involved in information recommendation service and specifies security requirements that address these security threats.

# Draft new Recommendation ITU-T X.1753 (ex X.gdsml) [[SG17-R12](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0012)]

Guidelines for data security using machine learning in big data infrastructure

## Summary

In big data infrastructure, there are many security threats in the process of data collection, storage, processing, and management. How to dynamically and intelligently monitor, analyse, and respond to data security threats is a problem to be solved in big data infrastructure. Machine learning has the capabilities of automatic learning and pattern recognition, which can discover potential security threats and abnormal behaviours from a large amount of data so that proactive defensive measures can be taken. Using machine learning to enhance data security has gradually become a necessary technology for big data infrastructure.

This Recommendation analyses data security threats in big data infrastructure and scenarios where machine learning can be applied to data security protection in big data infrastructure and provides guidelines for using machine learning to protect data security of big data infrastructure.

# Draft new Recommendation ITU-T X.1649 (ex X.sgmc) [[SG17-R14](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0014)]

Security guidelines for multi-cloud

## Summary

This Recommendation provides an overview of multi-cloud, including its definition and its background of emerging. This Recommendation also analyses security risks and specifies appropriate guidelines for multi-cloud to mitigate security risks.

# Draft revised Recommendation ITU-T X.1250 [[SG17-R15](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0015)]

Baseline capabilities for enhanced identity management and interoperability

## Summary

This document outlines key provisions for developing and deploying structured, interoperable identity management systems within telecommunications and IT networks, ensuring privacy and compliance with regional policies. It covers topics such as structured identity management models for secure and efficient identity exchanges, the protection and provisioning of identity attributes, and the discovery of identity service providers. It also addresses interoperability among identity platforms, security measures for threat mitigation, auditing for compliance, and the importance of usability and scalability. The overall goal is to create robust, transparent, and adaptable identity management systems that enhance trust, security, and user experience in digital interactions while aligning with regulatory standards.

# Draft revised Recommendation ITU-T X.1631 [[SG17-R13](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T25-SG17-R-0013)]

Information security controls based on ISO/IEC 27002 for cloud services

## Summary

The guidelines contained within this Recommendation | International Standard are in addition to and complement the guidelines given in ISO/IEC 27002:2022.

Specifically, this Recommendation | International Standard provides guidance supporting the implementation of information security controls for cloud service customers (CSCs) and cloud service providers (CSPs). Some guidance are for CSCs who implement the controls, and others are for CSPs to support the implementation of those controls. The determination of the appropriate information security controls and the extent of the utilisation of the guidance provided will depend on the results of the relevant risk assessment and the existence of any legal, regulatory, contractual, or other cloud-computing specific information security requirements.

Annex 2  
Subject: Member State response to TSB Circular 50:  
Consultation on Determined draft new Recommendations ITU T X.1062 (ex X.shcd), X.1238 (ex X.sgc-rcs), X.1128 (ex X.mt-feature), X.1129 (ex X.mt-integrity), X.1130 (ex X.tg-fdma), X.1457 (ex X.str-irs), X.1753 (ex X.gdsml), X.1649 (ex X.sgmc), and revised Recommendations ITU-T X.1250 and X.1631

|  |  |  |  |
| --- | --- | --- | --- |
| **To**: | Director of the  Telecommunication Standardization Bureau,  International Telecommunication Union  Place des Nations  CH 1211 Geneva 20, Switzerland | **From**: | [Name]  [Official role/title]  [Address] |
| **Fax**: | +41-22-730-5853 | **Fax**: |  |
| **E-mail**: | [tsbdir@itu.int](mailto:tsbdir@itu.int) | **E-mail**: |  |
|  |  | **Date**: | [Place,] [Date] |

Dear Sir/Madam,

With respect to the Member State consultation on the Determined draft text(s) listed in TSB Circular 195, I would like to advise you of the opinion of this Administration, which is set out in the table below.

|  | **Select one of the two boxes** |
| --- | --- |
| **Draft new Recommendation X.1062 (ex X.shcd)** | **assigns authority** to Study Group 17 to consider this text for approval (in which case, select one of the two options ⃝):  ⃝ No comments or suggested changes  ⃝ Comments and suggested changes are attached |
| **does not assign authority** to Study Group 17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |
| **Draft new Recommendation X.1238 (ex X.sgc-rcs)** | **assigns authority** to Study Group 17 to consider this text for approval (in which case, select one of the two options ⃝):  ⃝ No comments or suggested changes  ⃝ Comments and suggested changes are attached |
| **does not assign authority** to Study Group 17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |
| **Draft new Recommendation X.1128 (ex X.mt-feature)** | **assigns authority** to Study Group 17 to consider this text for approval (in which case, select one of the two options ⃝):  ⃝ No comments or suggested changes  ⃝ Comments and suggested changes are attached |
| **does not assign authority** to Study Group 17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |
| **Draft new Recommendation X.1129 (ex X.mt-integrity)** | **assigns authority** to Study Group 17 to consider this text for approval (in which case, select one of the two options ⃝):  ⃝ No comments or suggested changes  ⃝ Comments and suggested changes are attached |
| **does not assign authority** to Study Group 17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |
| **Draft new Recommendation X.1130 (ex X.tg-fdma)** | **assigns authority** to Study Group 17 to consider this text for approval (in which case, select one of the two options ⃝):  ⃝ No comments or suggested changes  ⃝ Comments and suggested changes are attached |
| **does not assign authority** to Study Group 17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |
| **Draft new Recommendation X.1457 (ex X.str-irs)** | **assigns authority** to Study Group 17 to consider this text for approval (in which case, select one of the two options ⃝):  ⃝ No comments or suggested changes  ⃝ Comments and suggested changes are attached |
| **does not assign authority** to Study Group 17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |
| **Draft new Recommendation X.1753 (ex X.gdsml)** | **assigns authority** to Study Group 17 to consider this text for approval (in which case, select one of the two options ⃝):  ⃝ No comments or suggested changes  ⃝ Comments and suggested changes are attached |
| **does not assign authority** to Study Group 17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |
| **Draft new Recommendation X.1649 (ex X.sgmc)** | **assigns authority** to Study Group 17 to consider this text for approval (in which case, select one of the two options ⃝):  ⃝ No comments or suggested changes  ⃝ Comments and suggested changes are attached |
| **does not assign authority** to Study Group 17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |
| **Draft revised Recommendation X.1250** | **assigns authority** to Study Group 17 to consider this text for approval (in which case, select one of the two options ⃝):  ⃝ No comments or suggested changes  ⃝ Comments and suggested changes are attached |
| **does not assign authority** to Study Group 17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |
| **Draft revised Recommendation X.1631** | **assigns authority** to Study Group 17 to consider this text for approval (in which case, select one of the two options ⃝):  ⃝ No comments or suggested changes  ⃝ Comments and suggested changes are attached |
| **does not assign authority** to Study Group 17 to consider this text for approval (reasons for this opinion and an outline of possible changes that would enable the work to progress are attached) |

Yours faithfully,

[Name]

[Official role/title]

Administration of [Member State]

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