

ICS 35.030
CCS L80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 42582-2023

**Information security technology - Personal information security
testing and evaluation specification in mobile internet
applications (App)**

信息安全技术 移动互联网应用程序（App）个人信息安全测评规范

Issued on: May 23, 2023

Implemented on: December 1, 2023

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

1 Scope	1
2 Normative references	1
3 Terms and Definitions	1
4 Abbreviations	2
4 Evaluation Environment and Tools	5
7 Evaluation of Organizational Personal Information Security Management Requirements	56
7 Result judgment	67
73 Reference	75

Foreword

This document is in accordance with the provisions of GB/T 1:1-2020 "Guidelines for Standardization Work Part 1: Structure and Drafting Rules for Standardization Documents" drafting: Please note that some contents of this document may refer to patents: The issuing agency of this document assumes no responsibility for identifying patents: This document is proposed and managed by the National Information Security Standardization Technical Committee (SAC/TC260): This document was drafted by: China Institute of Electronic Technology Standardization, China Network Security Review Technology and Certification Center, First Research Institute of the Ministry of Public Security Research Institute, Beijing Information Security Evaluation Center, China Electronics Technology Group Corporation Fifteenth Research Institute, National Computer Network Emergency Technology Handling Association Investigation Center, Beijing Baidu Netcom Technology Co., Ltd., Beijing Bangbang Security Technology Co., Ltd., China Academy of Information and Communications Technology, Beijing Zhizhangyike Technology Co., Ltd., Digital Currency Research Institute of the People's Bank of China, China Mobile Communications Group Co., Ltd., Qi Anxin Wangshen Information Technology (Beijing) Co., Ltd., Beijing Hanhua Feitian Xinan Technology Co., Ltd., Beijing Qihoo Technology Co., Ltd., Shaanxi Province Network and Information Security Evaluation Center, Institute of Information Engineering, Chinese Academy of Sciences, National Information Technology Security Research Center, Beijing UnionPay Gold Card Technology Co., Ltd., Beijing Transportation University, Xi'an Jiaotong University, China Automotive Engineering Research Institute Co., Ltd., Beijing Douyin Information Service Co., Ltd., Daily Interactive Co., Ltd: Co., Ltd., Venustech Information Technology Group Co., Ltd., OPPO Guangdong Mobile Communication Co., Ltd., Shenzhen Tencent Computer System Co., Ltd., Beijing Zhiyou Network Security Technology Co., Ltd., Quanzhi Technology (Hangzhou) Co., Ltd., Jiangsu Tongfudun

Information Security Technology Co., Ltd: Company, Zhongke Sharp Eye (Tianjin) Technology Co., Ltd: The main drafters of this document: Hu Ying, Liu Xing, Fan Bo, Yao Xiangzhen, Gao Chao, Yan Yan, Xin Jianfeng, Han Yu, Fan Hong, Li Yuan, Liu Jian, Dong Jingjing, Lin Xingchen, Wang Yiyu, Li Xiaoxue, Wang Haitang, Deng Ting, Fang Ning, Wang Danhui, Li Biao, Song Lingwei, Qiu Qin, Zhao Shuai, Peng Gen, Yao Yinan, Yang Jing, Du Dan, Wu Dongyu, Li Yu, Wang Wei, Fan Ming, Li Guangping, Yang Xiaohan, Dong Lin, Shi Jing, Li Teng, Xu Yongtai, Han Yun, Wang Xiesi, Wang Dejie, Zhao Hongyu: Information Security Technology Mobile Internet Application (App) Personal Information Security Evaluation Specifications

1 Scope

GB/T 42582-2023 specifies how the personal information practices of a mobile app are tested and evaluated. China removes apps from the stores for collecting more than they need, and the removals are decided by an assessment against the Personal Information Protection Law and the related standards - which means the assessment method is, in effect, the enforcement. What it looks at is not the privacy policy but the behaviour: what the app actually sends, when it asks for consent, and whether refusing a permission stops it working. The standard sets the evaluation process, methods, environment and tools, then the content of the evaluation: the collection, storage and use of personal information, the rights of the data subject, the entrusted processing, sharing, transfer and public disclosure, and the handling of personal information security incidents. It took effect on 1 December 2023.

This document specifies the evaluation process for personal information security evaluation of mobile Internet applications based on GB/T 35273-2020: and methods for evaluating various safety requirements: This document is applicable to guide third-party evaluation agencies to evaluate personal information security of mobile Internet applications, and to supervise The department supervises and manages the personal information security of mobile Internet applications, and mobile Internet application operators carry out personal information security: Refer to the implementation of the full self-assessment:

2 Normative references

The contents of the following documents constitute the essential provisions of this document through normative references in the text: Among them, dated references For documents, only the version corresponding to the date is applicable to this document; for undated reference documents, the latest version (including all amendments) is applicable to this document:

GB/T 25069-2022 Information Security Technical Terminology

GB/T 35273-2020 Personal Information Security Specifications for Information Security

Technology

GB/T 41391-2022 Information Security Technology Mobile Internet Application (App) Basic Requirements for Collection of Personal Information

3 Terms and Definitions

Defined in GB/T 25069-2022, GB/T 35273-2020 and GB/T 41391-2022 and the following terms and definitions apply in this document: 3:

1 Applications running on mobile smart terminals:

Note: Including mobile smart terminal presets, downloaded and installed applications and applets: 3:

2 Mobile internet application owner, manager or provider: 3:

3 Software libraries to assist in software development: NOTE: A software development kit typically includes a collection of related binaries, documentation, examples, and tools: 3:

4 Privacy Policyprivacypolicy Text describing the rules governing the handling of personal information by mobile internet applications:

Note: For the content contained in the personal information protection policy, see 5:5 in GB/T 35273-2020: