

AUDIT RESULTS SUMMARY

GuardDo Pixel 10

ASSESSMENT TYPE	REPORT NO.	ISSUE DATE
Independent Information Security Audit	58690-38598	27.09.2026
Document status. This document is a public summary of the results of the independent assessment. Full Technical Report No. 58690-38598 dated 27.09.2026 contains detailed testing methodologies and procedures, technical materials, and supporting evidence and is subject to restricted distribution. The full technical report is not intended for public distribution and is provided only to authorized parties and interested parties subject to agreement with the auditor.		

1. General Information

Test object: GuardDo Pixel 10 smartphone.

Model: GuardDo Pixel 10

Firmware version (build numbers): #1154 – #1601

Condition of test objects: the devices were provided new, out of the box, in factory configuration; initial setup was performed and documented in the handover and acceptance record.

Number of samples: 6 units in identical configuration.

2. Objective and Scope of the Assessment

Independent verification of four specific manufacturer security claims concerning the hidden data space mechanism, emergency deletion, and the absence of undocumented access paths. The assessment was performed by an external auditor independent of the developer.

3. Threat Model and Limitations

The assessment was conducted within a predefined and agreed threat model. Understanding these boundaries is essential for proper interpretation of the conclusions: this report confirms the product's resilience specifically against the class of threats described below.

Within the threat model (in scope)

- physical access to the device while powered off;
- physical access to the device while powered on and locked (standard profile unlocked; hidden space inaccessible);
- the hidden-space password/PIN is unknown to the attacker;
- the attacker has access to professional mobile forensic platforms (Cellebrite-, MSAB-, and GrayKey-class), JTAG/EDL programmers, and chip-off equipment;
- a network attacker capable of intercepting the device's outbound traffic;
- assessment for undocumented mechanisms that could allow the developer or another third party to access device contents by bypassing standard authentication mechanisms.

Outside the threat model (out of scope)

- social engineering and phishing targeting the user;
- manufacturing and supply-chain attacks;
- attacks through cellular infrastructure (baseband, SS7, and similar);
- discovery of 0-day vulnerabilities in the underlying Android/Pixel OS outside the context of GuardDo customizations;
- full firmware code review (except for targeted review of authentication and encryption modules).

4. Methodology

Testing was performed using relevant elements of recognized industry methodologies:

- OWASP MASTG (Mobile Application Security Testing Guide) — to the extent applicable to testing the device and its firmware;
- NIST SP 800-101 (Guidelines on Mobile Device Forensics) — with respect to data acquisition and analysis.

All actions were documented with the date, tool, tool version, and exact result, while maintaining chain of custody. Before testing began, an agreed test dataset containing unique identifying markers was placed in the hidden space to enable objective verification of any access to or recovery of the data.

5. Assessment Results

The verified claims and the final result for each are presented below. A result of “PASSED” means that none of the methods applied met the predefined failure criterion.

No.	Claim Under Assessment	Assessment Method (Summary)	Result
1	Hidden-space isolation: access to its contents without the password is not possible using logical or physical extraction methods	Logical extraction (ADB/debug interfaces, backup analysis); physical extraction (chip-off, sector-by-sector NAND dump analysis, JTAG/EDL); volatile-memory dump analysis	PASSED
2	No leakage: indicators of the existence or contents of the hidden space are neither stored locally nor transmitted over the network	Analysis of system and application logs, cache, crash reports, and service directories; interception of outbound traffic through a MITM proxy; telemetry analysis	PASSED
3	Irreversibility of emergency deletion: after the function operates as designed, hidden-space data cannot be recovered	Forensic analysis of the NAND dump after wipe; file carving using standard recovery tools; assessment of TRIM/wear-leveling effects	PASSED
4	Absence of a master password or hidden access-recovery mechanisms that bypass the user's standard password entry	Examination of debug interfaces (UART/JTAG) and recovery mode; targeted review of the authentication module for hard-coded credentials	PASSED

6. Final Conclusion

Based on the assessment performed within the agreed threat model and scope of work, the failure criteria were not met for any of the four claims under review. The assessed security mechanisms demonstrated the stated behavior in the tested configuration and on the specified firmware versions.

Limitations of this report. The conclusions apply only to the stated scope of work, threat model, configuration, and firmware versions and do not imply absolute invulnerability of the product. Material changes require reassessment.

7. Audit Information

Assessment period: 10.05.2026 — 20.09.2026

Firmware versions assessed: #1154 – #1601

Report issue date: 27.09.2026

Auditor: MicroTech BG

Report registration number: 58690-38598 dated 27.09.2026

Document ID: MT-58690-38598

Basis for the assessment. The assessment was initiated by Sergey Waigel, who was the customer as of the commencement date. It was subsequently agreed that the final report would be issued to ORANGEPEAK SOFTWARE PROVIDERS - FZCO as the recipient of the assessment results.

Auditor — MicroTech BG Ltd. (MicroTech BG EOOD)

UIC / PIC (Bulstat / Identification Number)	203186658
VAT Number	BG203186658
Registered Address	Office 8, BC-BI, 10 Panagyurishte St., Targovishte 7700, Bulgaria
Email	info@microtechcyber.pro
Official Website	microtechcyber.pro

Recipient of the Final Report — ORANGEPEAK SOFTWARE PROVIDERS - FZCO

Registration Number	85414
License Number	92193
Legal Form	FZCO (limited liability company)
Place of Registration	Dubai Silicon Oasis, Dubai, United Arab Emirates
Licensing / Registration Authority	Dubai Integrated Economic Zones Authority (DIEZA)
Official Websites	guarddo.org, guarddo.ru

This summary has been prepared on the basis of Technical Report No. 58690-38598 dated 27.09.2026, held by the customer and the auditor. The authenticity of this summary may be confirmed upon request to the auditor.

Authorized Representative of the Auditor (MicroTech BG):

Position: Technical Director

/ Krasimir Stoichkov / Date: 27.09.2026

Seal

