kaspersky

Security, availability, confidentiality and data protection in the development and distribution of AV bases: **SOC 2 Audit Management Summary**

One of the Big Four global auditing firms audited Kaspersky's development and distribution processes of AV bases in 2019 and again in 2022, with a deadline of April 28, in accordance with SOC 2 Type 1 under the guidelines of the standard developed by the American Institute of Certified Public Accountants (AICPA) (AICPA Professional Standard).

The audit demonstrates that Kaspersky complies with the principles and policies of:
(i) security;
(ii) availability;
(iii) confidentiality; and
(iv) privacy
in the development and distribution of AV bases.

The auditor analyzed and evaluated the description and documentation provided by Kaspersky. In addition, the described and implemented system controls were verified in productive operation.

The service auditor performed a total of 72 test scenarios for the assessment (C_ELC_01 - C_GCC_61; see the tables on pages 32-69 in the audit report) and concluded that Kaspersky met all test criteria without exception.

In addition to reviewing the documentation and descriptions, the audit included:

- interviewing the managers responsible for the aforementioned processes, Kaspersky's internal audit teams, and the employees involved;
- observation and review of activities in daily operations; and
- inspection of all Kaspersky documents and records *(including standard reports as configured in the system; parameter-driven reports generated by Kaspersky systems; user-defined reports that are not part of the standard application, such as scripts, report writers, and so on).*

In particular, the following SOC2 Criteria (CC) were considered in the audits:

- CC on system operation: Kaspersky uses state-of-the-art detection and control procedures to identify changes to configurations that may lead to the accidental or deliberate introduction of vulnerabilities. Kaspersky monitors system components and the operation of these components for anomalies that indicate malicious actions, system malfunctions, or errors that could affect the company's ability to ensure protection objectives.

  Every change to the source code goes through a dedicated review process to confirm its integrity and security. The review process for creating updates involves Kaspersky experts outside Russia – including Kaspersky teams in the U.S. and Canada (p. 19).

- **CC for risk mitigation:** Kaspersky identifies, develops, and implements all necessary risk mitigation measures that may result from potential business disruptions. The company continuously assesses all potential risks with regard to suppliers and the entire supply chain. The auditor also reviewed the procedure for updating the process

and structure descriptions to ensure that they describe the roles, their responsibilities and the sequence of actions in the index file creation process.

- **CC related to logical and physical access controls:** this specifically addresses how Kaspersky authorizes, modifies, or revokes access to data, software, functions, and other protected information assets based on roles, responsibilities, or system design. Kaspersky fully incorporates the concepts of least privilege and separation of duties to achieve the highest protection objectives.
- **CC related to control environment:** including commitment to integrity and ethical values.
- **CC related to communication and information:** the auditor reviewed, among other things, whether (and, if so – how) Kaspersky communicates with external parties about matters that affect the functioning of internal control.
- **CC related to control activities:** The auditor reviewed, among other things, the extent to which Kaspersky develops and implements control activities to reduce risks to a level consistent with the protection objectives.
- **CC related to change management.**
- **CC for monitoring controls.**
- **CC for risk assessment.**

The report also provides supplementary information on Kaspersky's transparency and trustworthiness activities, in particular, specific activities under its Global Transparency Initiative (GTI).

You can request the 74-page audit report, dated April 28, 2022, from your Kaspersky contact.

The report consists of the following five sections:

Section I: *Independent Service Auditor's Report (pages 3-6)*

Section II: *AO Kaspersky Lab management statement (pages 7-8)*

Section III: *Management's Description of the System (pages 9-24)*

Section IV: *Independent Service Auditor's Information Except Control Objectives and Control Activities (pages 25-69)*

Section V: *Additional Information from Kaspersky (pages 70-73)*