System and Organization Controls 3 (SOC 3) Report

Report on the Yandex ID System relevant to Security, Availability, Confidentiality

1 March 2021 – 28 February 2022

Table of Contents

Report of Independent Service Auditors

To the Management of LLC Yandex

Scope

We have examined LLC Yandex's (hereinafter "Yandex" or "service organization") accompanying assertion titled "Assertion of Yandex's Management" ("assertion") that the controls within Yandex ID system ("system") were effective throughout the period 1 March 2021 to 28 February 2022, to provide reasonable assurance that Yandex's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service organization's responsibilities

Yandex is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Yandex's service commitments and system requirements were achieved. Yandex has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Yandex is also responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service auditors' responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Yandex's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Yandex's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

OOO PricewaterhouseCoopers Advisory
White Square Office Center 10 Butyrsky Val Moscow, Russia, 125047
T: +7 (495) 967-6000, F:+7 (495) 967-6001, www.pwc.ru

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Yandex's Yandex ID system were effective throughout the period 1 March 2021 to 28 February 2022, to provide reasonable assurance that Yandex's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

OOO PricewaterhouseCoopers Advisory

Moscow, Russian Federation

25 April 2022

Yandex LLC
ul. Lva Tolstogo, 16
119021 Moscow, Russia
Tel.: +7 (495) 739-70-00
Fax: +7 (495) 739-70-70
yandex.com
info@yandex-team.ru

Assertion of Yandex Management

We, LLC Yandex (hereinafter “Yandex”), are responsible for designing, implementing, operating, and maintaining effective controls within Yandex ID system (the “system”) throughout the period 1 March 2021 to 28 February 2022, to provide reasonable assurance that Yandex’s service commitments and system requirements relevant to security, availability and confidentiality were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period 1 March 2021 to 28 February 2022, to provide reasonable assurance that Yandex’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Yandex’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period 1 March 2021 to 28 February 2022, to provide reasonable assurance that Yandex’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A. Yandex's description of the boundaries of Yandex ID system

Overview of Operations

Business Description and Service Overview

Yandex is a technology company that builds intelligent products and services powered by machine learning. The company aims to help consumers and businesses better navigate the online and offline world. Since 1997, Yandex has delivered world-class, locally relevant search and information services. Additionally, Yandex has developed market-leading on-demand transportation services, navigation products, and other mobile applications for millions of consumers across the globe.

Yandex ID service allows users to use a unified interface for authentication in Yandex services and controlling their information stored by Yandex (favorite addresses for delivery, mask of primary bank account number for subscriptions, etc.). Yandex ID also implements authentication with third parties, including supporting a standard OAuth mechanism. Before 1 April 2021, the Yandex ID service' name was Yandex.Passport.

Yandex ID is maintained with coordinated efforts of the group of Yandex companies, which are: Yandex LLC, which provides the service; Yandex.Technologies LLC, whose employees develop and maintain the source code and deployment infrastructure of Yandex ID; Yandex DC LLC, Yandex DC Vladimir LLC and Yandex Oy which are responsible for maintenance of data centers with hardware used by Yandex ID.

Yandex ID is available for users on https://passport.yandex.com/ and https://passport.yandex.ru/, and also on local domains. The list of addresses might be changed.

Yandex ID processes authentication requests sent by other Yandex services and apps as well as third-party software using OAuth protocol, securely stores the information provided by users and provide it to Yandex services to make personalized experiences possible, makes every effort to maintain availability of the service and user data to users.

Yandex ID Scope Boundary

Yandex ID provides the services described above using the following components included in scope for this report:

- External
  - Yandex ID website
- Internal
  - Blackbox
  - Yandex ID API
  - Yandex accounts database
  - Tech support (Admin) interface

Yandex ID website

Yandex ID website is the main avenue of interaction between users and Yandex ID functions. On the Yandex ID website users have personal area with information about the data that Yandex ID stores and possibility to manage it (add, change or delete). In personal area of Yandex ID website users have information about devices that have been granted access to Yandex data. Also users have possibility to configure authorization methods for their Yandex ID account.

The website is available in English, Russian, Ukrainian, Kazakh, Belorussian and Tatar languages.

Yandex ID API

Yandex ID API is provided for any Yandex service (including Yandex ID website) to interact with user data, access is limited and need to be preliminary approved. Every request meant to alter or add to user data is passed to this Yandex ID API.

Blackbox

Blackbox is an internal service with exclusive read access to databases containing user data and the log of changes to user data. Every process that requires reading from these databases (including requests from internal Passport API) must route the requests through Blackbox.

Yandex accounts database

Yandex accounts database (distributed among data centers) is the storage of the user data. It is the primary database for interacting with user data, and it serves as the source of the most recent version of data provided by users or recorded on their behalf.

Tech support (Admin) interface

Tech support interface is an internal web service that allows authorized Yandex personnel to access user data to resolve access issues, view the change history for Yandex accounts and manipulate internal meta information for accounts.

Components of the System

Infrastructure

Yandex maintains infrastructure that includes the data centers and offices, network, and hardware as well as operational software that support Yandex ID service. Yandex established infrastructure maintenance processes including security monitoring and incident management process, monitoring of the Yandex ID functionality and stability of work. Analysis of Yandex ID service capacity and testing of fault tolerance is periodically performed. Backups of Yandex ID data are maintained and monitored to ensure successful replication.

Yandex ID service is distributed across Yandex's data centers located in Russia and Finland. Data centers are protected from environmental threats and unauthorized physical access. Access to premises is provided based on approved request and periodically reviewed in order to ensure consistency with job responsibilities and to revoke access when an individual no longer requires access.

All data centers established the unified procedures for physical security, protection of environmental threats controls and infrastructure equipment monitoring. Yandex ID recovery plan is established, tested and annually reviewed.

Software

Development and maintenance of Yandex ID employs a variety of software products, created outside of Yandex and in-house:

- Operating systems, used on servers and workstations:
  - Windows
  - Linux
  - macOS
- Database:
  - Yandex ID accounts database – Percona Server for MySQL

- Web applications:
    - Yandex ID website, including social networks integration, OAuth frontend, and the internal administrative web interface.
    - Blackbox.
    - General Yandex ID API for communicating with the account database.

People

The following functional groups and teams are relevant to the Yandex ID:

- Group of authorization systems development.
- Front-end team, responsible for the development of the Yandex ID website.
- Backend development and maintenance.
- Core services development team, responsible for writing and reviewing code for Blackbox and internal Passport API.
- System administrators, responsible for availability and consistency of Yandex ID services, as well as hardware management.
- Quality assurance engineers, who perform automatic and manual testing of Yandex ID code and interfaces.
- Authorization service support. Support specialists, responsible for responding to user inquiries and resolving issues with authorization, including restoring access to accounts.
- Yandex ID is overseen by executives who manage Yandex infrastructure as a whole.

Responsibilities and access of these groups are explicitly outlined and isolated. Yandex's management structure is set up to have clear reporting lines and management responsibilities. Each manager is responsible for ensuring that specific activities of their team are conducted in a control-oriented environment incorporating company policies and procedures. All policies and procedures for an area are reviewed periodically by the relevant managers.

Data

Principal user data is stored in the accounts database, accessed by other Yandex ID components as needed.

All user data is recognized as confidential and can be divided into:

- Identifying personal details (name, phone numbers, email addresses etc.)
- User settings applicable for Yandex services, both universal (preferred interface language, location etc.) and service-specific (primary delivery address, favorite places, reward points etc.).

Yandex ID users retain control and ownership of their own data. Users get access to their personal area of Yandex ID after entering a password, they also have possibility to use authorization with text message confirmation codes and two-factor authentication (one-time password and pin code which the user sets when setting up two-factor authentication).

A user's information is deleted from Yandex ID service upon user's request. Before the data is deleted, the user verifies their password and enters a CAPTCHA. Upon successful verification, the account pending deletion is quarantined for 30 days, during which the user can restore access to their account. After the quarantine, if the user no longer has any other contractual relationship with Yandex, all information except their phone number (which is used for antifraud purposes) is deleted. Phone numbers are automatically deleted after three years of retaining.

Until the user initiates the deletion of their account service protects confidential information from erasure and destruction by complex security measures such as limited access to data and continuous back-up procedures.

Decommissioned storage hardware (hard-disk drives) is disposed of information and physically destroyed. The short grout procedure is necessary to update the firmware of the drives to the current version and to erase the information on the disk before placing it in the operational reserve (warehouse). All drives intended for leaving Yandex ID service perimeter must undergo the preparation procedure in test stands without fail.

User entity responsibilities

There are no complementary user entity controls that are applicable. However, as it is communicated on Yandex ID website in order to protect their own data, users are expected to follow general guidelines:

- Protect their authentication data:
  - Not disclose passwords or authentication codes to third parties.
  - Install and maintain antivirus software on devices used for authentication with Yandex services.
  - Log in only on trusted devices, or reliably erase any records (cookies etc.) from untrusted devices.
  - Allow access to Yandex account data only to trusted OAuth applications.
  - Securely log out after completing each session of operating Yandex services.
- Pay attention to security notifications from Yandex:
  - Follow up with every notification about suspicious activity and make sure to clearly understand if further investigation is needed.
  - Change password and check ways to automatically restore access to it as soon as unexplained activity is found.
- Monitor Yandex ID announcements or changes in Yandex's User Agreement and Privacy Policy (if any) and evaluate the impact on their ongoing procedures and users' internal controls.
- Promptly inform Yandex of any instances of unauthorized (not allowed by the user) access to Yandex ID service through the user's account and/or any breach (alleged breach) of confidentiality of the chosen means of access to his/her account.
- When requesting deletion of an account, Yandex ID users are responsible for analysis what other services connected to Yandex ID they used, and deletion of their data from other services (if required).

Attachment B. Principal Service Commitments and System Requirements

Service Commitments

Commitments are declarations made by management to customers regarding the performance of Yandex ID. Commitments to customers are communicated via Yandex ID service description and User Agreement for Yandex Services:

- Security commitments, to protect user data from both unauthorized remote and physical access.
- Confidentiality commitments, to restrict access to user data only to people who need to access it according to development and support guidelines.
- Availability commitments, to make every effort to maintain availability of the service and user data to users to make sure that users' data is accessible to users without significant interruptions.

System Requirements

Yandex designs its processes and procedures to meet its objectives for its Yandex ID service. Those objectives are based on the service commitments that Yandex makes to user entities, the laws and regulations that govern the provision of the Yandex ID service and the financial, operational and compliance requirements that Yandex has established for the services.

Yandex established the standardized processes and system requirements, which include, but are not limited to, the following:

- Access Security: Yandex maintains data access and logical security policies, designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Access to systems is restricted based on the principle of least privilege.
- Vulnerability Management: The implementation of the new functionality is coordinated with the Information Security Service. The production service is weekly scanned for a vulnerability scanning system.
- Change Management: Production systems are only changed after proper testing and approval. To maintain a degree of separation between approved and untested releases, distinct environments are implemented: a development environment and a test environment that do not contain real user data, a pre-stable environment for final quality assurance, and a production environment. The roles for developing changes, testing, and implementing them in a production environment are segregated.
- Incident Management: Yandex infrastructure and service monitoring includes processes for detecting and localizing information security events.
- Data Security: Yandex implements and maintains technical and organizational measures to protect customer data.