Yandex

System and Organization Controls 3 (SOC 3) Report

Report of the Yandex.Passport System relevant to security, availability, confidentiality

September 1, 2019 – February 29, 2020

Table of Contents

Independent Service Auditor’s Report

To: 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.Passport system (“system”) were effective throughout the period September 1, 2019 to February 29, 2020, 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 Auditor’s 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.

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 achieve the service organization's service commitments and system requirements based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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.Passport system were effective throughout the period September 1, 2019 to February 29, 2020 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

24 April 2020

Yandex

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.Passport system (system) throughout the period September 1, 2019 to February 29, 2020, 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 September 1, 2019 to February 29, 2020, 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 September 1, 2019 to February 29, 2020, to provide reasonable assurance that Yandex's service commitments and system requirements were achieved based on the applicable trust services criteria.

Anton Karpov, CSO Yandex

Attachment A. Yandex’s description of the boundaries of Yandex.Passport 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.Passport service allows users to use unified interface for authentication in Yandex services and controlling their information stored by Yandex (favorite addresses for delivery, banking card numbers for subscriptions etc.). Yandex.Passport also implements authentication with third parties, including supporting a standard OAuth mechanism.

Yandex.Passport is available for users on https://passport.yandex.com/ and https://passport.yandex.ru/. The list of addresses might be changed.

When registering an account, users explicitly accept Yandex's User Agreement and Privacy Policy.

Yandex.Passport Scope Boundary

Yandex.Passport provides these essential services using the following components included in the scope of this report:

- External:
  - Yandex.Passport website
- Internal:
  - Blackbox
  - Internal Yandex.Passport API
  - Yandex accounts database
  - Tech support interface

Yandex.Passport website

Yandex.Passport website is the main avenue of interaction between users and Yandex.Passport functions. Through the website users can learn about the data that Yandex.Passport stores, manage their data and third- party access to it, as well as authorization methods for their account.

The website is available in English, Russian, Turkish, Ukrainian, Kazakh and Uzbek languages.

Internal Yandex.Passport API

Internal Yandex.Passport API is provided for any Yandex service (including Yandex.Passport 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.Passport 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 MySQL (distributed by data centers) is the storage for current state 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 interface

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

Components of the System

Infrastructure

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

Yandex.Passport service is distributed across Yandex's data centers. Data centers and offices relevant to Yandex.Passport development and maintenance are 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, periodically reviewed and timely revoked. Yandex established unified requirements, control procedures and monitoring procedures for all data centers.

Yandex.Passport recovery plan is established, tested and annually reviewed.

Software

Yandex follows formal change management and access management processes.

The change management process is established for the Yandex.Passport development and maintenance. All changes including hotfixes are authorized, documented, tracked, tested, approved and deployed according to the established process. Development, testing and production environments are segregated at server and access levels. Users data is maintained only in production environment. Also as part of change management process Yandex.Passport implemented a Security Development Lifecycle.

Access to Yandex.Passport data is restricted only to authorized Yandex employees based on pre-approved requests and access roles, periodical access review and revocation processes are also established.

Other Yandex services can request and be granted access to preselected attributes of users' accounts. Access of other services to the Yandex.Passport API (including Blackbox) including information that can be provided is limited and need to be preliminary approved. Other services access review is periodically conducted.

People

Yandex Passport is supported by the following groups:

- Department of authorization systems development.
    - Front-end team, responsible for the development of the Yandex.Passport 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.Passport services, as well as hardware management.
- Quality assurance engineers, who perform automatic and manual testing of Yandex.Passport code and interfaces.
- Authorization service support. Support specialists, responsible for responding to user inquiries and resolving issues with authorization, including restoring access to accounts.
- Information security department. Security specialists who consult the development team on concepts and methods of protecting and processing authentication data and personal data of the users.
- Yandex.Passport is overseen by executives who manage Yandex infrastructure as a whole.

Responsibilities and access of these groups are explicitly outlined and isolated.

There are employees involved with Yandex.Passport without directly belonging to the Yandex.Passport team (information security, legal department, HR etc.). These employees consult and support Yandex.Passport in the same measure as any other Yandex service, and are not covered with control procedures implemented specifically for Yandex.Passport.

Data

Principal user data is stored in the accounts database, accessed by other Yandex.Passport 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.Passport users retain control and ownership of their own data. Various user authorization methods, including text message confirmation codes and two-factor authentication, are employed to reduce the risk of exposing user data to third parties.

A user's information is deleted from Yandex.Passport 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.

Decommissioned storage hardware, such as hard-disk drives, is disposed of and physically destroyed in accordance with industry-standard practices.

User entity responsibilities

To protect their own data, users are expected to follow general guidelines for managing authentication data and monitoring suspicious activity:

- 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 it as soon as unexplained activity is found.

Yandex.Passport has been developed based on the assumption that specific controls and procedures will be rendered by the users. Assumed complementary user entity controls and affected criteria are listed below.

Trust Service Criteria	User Entity Controls Assumed by Yandex
CC2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.	Yandex.Passport users are responsible for monitoring Yandex.Passport announcements or changes in Yandex's User Agreement and Privacy Policy (if any) and evaluating the impact on their ongoing procedures and users’ internal controls.

Trust Service Criteria	User Entity Controls Assumed by Yandex
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Yandex.Passport users are responsible for access control to manage accounts and authentication. Yandex.Passport users are responsible for password management and protecting their authentication data. Yandex.Passport users are responsible to install and maintain antivirus software on devices used for authentication with Yandex services. Yandex.Passport users are responsible to change password and check ways to automatically restore access it as soon as unexplained activity is found.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	Yandex.Passport users are responsible for promptly informing Yandex of any instances of unauthorized (not allowed by the user) access to Yandex.Passport service through the user's account and/or any breach (alleged breach) of confidentiality of the chosen means of access to his/her account.
C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	When requesting deletion of account, Yandex.Passport users are responsible for analysis what other services connected to Yandex.Passport they used, and deletion of their data from other services (if required).

The complementary user entity controls presented above are not intended to be a comprehensive list of all internal controls that should be employed by Yandex.Passport users.

Attachment B. Principal Service Commitments and System Requirements

Service Commitments

Commitments are declarations made by management to customers regarding the performance of Yandex.Passport. Commitments to customers are communicated via Yandex,Passport 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.Passport 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.Passport 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 Yandex.Passport service complies with SDL (Security Development Lifecycle) regulations. The implementation of the new functionality is coordinated with the Information Security Service.
- 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.