Security Measures

This document describes technical and organizational measures implemented by Yandex to protect Controller Data in Yandex.Cloud Platform and is an integral part of Data Processing Addendum available at: https://yandex.com/legal/cloud_dpa.

Organization of information security

Information security management program

- Yandex maintains an information security management program that includes the adoption and enforcement of internal policies and procedures designed to minimize information security risks to Customer data.

Security responsibilities

- Yandex has a security team responsible for implementing and monitoring the security procedures.

Risk management

- Yandex has a risk management program that includes performing regular risk assessments and executing risk treatment plans.

Human resource security

Screening

- Yandex carries background verification checks on all candidates for employment.

Training

- Yandex requires all employees and contractors to apply information security in accordance with its established policies and procedures.
- Yandex provides awareness training for employees concerning the appropriate handling of cloud service customer data .

Termination or change of employment

- Yandex defines, communicates to its employees and contractors and enforces information security responsibilities and duties that remain valid after termination or change of employment.

Asset management

Asset inventory

- Yandex has an inventory of assets, which includes customer data and service derived data.

Acceptable use

- Yandex documents and implements rules for the acceptable use of information and of assets associated with information and information processing facilities.

Return of assets

- Yandex employees return all of the organizational assets in their possession upon termination of their employment.

Classification of information

- Yandex classifies information in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

Handling of assets

- Yandex develops and implements procedures for handling assets in accordance with the adopted information classification scheme.

Disposal of media

- Yandex securely disposes media when no longer required, using formal procedures.

Access control

Access control policy

- Yandex has a policy which ensures only authorized individuals have access to facilities, secure areas, and computing and networking resources.

Access to networks and systems

- Yandex employees are only be provided with access to the network and systems that they have been specifically authorized to use.
- Yandex management is required to approve individual's access to all facilities, secure areas and computing and network resources.
- Yandex restricts each user's access privileges to the minimum set required for the performance of their job and only for the duration of the need of that privilege.
- Yandex locates all management interfaces for hardware on segregated networks with limited access by authorized personnel.
- Yandex provides access to source code only to authorized persons according to security policy.

Review of user access rights

- Yandex annually reviews all users' access rights.

Removal or adjustment of access rights

- Yandex removes the access rights of all its employees to information and systems upon termination of their employment, or adjusted upon change.

Password quality

- Yandex ensures quality passwords in its password management systems including minimum password length, number of character classes and maximum life.

Segregation in virtual computing environments

- Yandex enforces segregation of network access between Customers and between the Yandex internal administration environment and the Yandex cloud computing environment.
- Yandex has automated systems for control of network data flows (router ACLs, dynamic firewall, host-based firewall).

Physical and environmental security

Physical security perimeter

- Yandex defines security perimeters and uses them to protect areas that contain either sensitive or critical information and information processing facilities.

Physical entry controls

- Yandex has appropriate entry controls to protect secure areas to ensure that only authorized personnel are allowed access.

Supporting utilities

- Yandex protects equipment from power failures and other disruptions caused by failures in supporting utilities.

Securing of equipment off-premises

- Yandex employees do not be take equipment, information or software off-site without prior authorization
- Yandex applies security to off-site assets taking into account the different risks of working outside the organization's premises.

Secure disposal or reuse of equipment

- Yandex ensures that any sensitive data on storage media has been removed or securely overwritten prior to disposal or re-use.

Data security & information lifecycle management

Transmission security

- Yandex encrypts all Customer information when transmitted over public networks using TLS

Secure disposal

- When vacating Customers' resources these resources are sanitized before allocating them to another Customer.

Incident management

Incident response and reporting

- Yandex has a formal security incident monitoring, reporting and response process to identify, report, and appropriately respond to known or suspected security incidents.
- Yandex has procedures for reporting security incidents that affect Customer data to the Customers without undue delay.

Information system development and maintenance

System Development Lifecycle

- Yandex has a documented System Development Lifecycle which governs the development and deployment of systems and applications.

Information security requirements

- Yandex includes information security related requirements in the requirements for new information systems or enhancements to existing information systems.

System change control procedures

- Yandex controls changes to systems within the development lifecycle by the use of formal change control procedures which include security architecture reviews.
- Yandex uses a peer-review process of all production code of its cloud platform and a security officer validates the critical functionality before release.

Secure system engineering

- Yandex applies principles for engineering secure systems to any information system implementation efforts.

Information security testing

- Yandex performs regular fuzz testing, penetration testing and vulnerability scanning to detect, mitigate and resolve security issues in cloud platform.

Cryptographic standards

- Yandex has a documented policy that sets minimum cryptographic standards which must be followed by all applications as well as networking and computing resources.

Secure development environment

- Yandex establishes and appropriately protects secure development environments for system development and integration efforts that cover the entire system development lifecycle.
- Yandex separates its development, test and production environments.
- Yandex has procedures to ensure production data is never replicated in non-production environments.

Vulnerability management

- Yandex performs regular vulnerability scans of pre-production, Internet-facing server systems and network devices before moving those systems/devices to production.
- Yandex remediates all discovered vulnerabilities prior to moving those systems to production.

Patch management

- Yandex has a policy for patch management documenting the maximum timeframes between the time a vendor supplies a critical security patch and the time it is applied in its systems.

Business continuity and disaster recovery

Redundancy

- Yandex employs redundancy mechanisms for all critical services.
- Yandex runs in several geographically distributed data-centers designed to work 24x7 and withstand various environment threats.
- Yandex uses data storage redundancy that permits to recover Customer data in case of equipment failure.

Tests

- Yandex regularly tests its business continuity and disaster recovery plans.

Information security review

Self-assessment

- Yandex regularly reviews its information systems for compliance with the organization's information security policies and standards.
- Yandex evaluates and reviews its approach to managing information security and implementation at planned intervals or when significant changes occur.