iskraemeco
BY ELSEWEDY ELECTRIC

Iskraemeco Cloud Security Policy

www.iskraemeco.com

Roles and responsibilities in cloud services

Cloud Service Provider: Iskraemeco, d.d. ("Iskraemeco") is responsible for providing cloud services to its customers. Iskraemeco is a personal data processor, therefore it is responsible for processing personal data of its cloud service customers and their users. Iskraemeco abides by standards and legislation for protecting personal data and other data as well as accepted organisational regulations, when providing cloud services.

Cloud Service Customer: Cloud service customer ("Customer"), entering a contract with Iskraemeco must comply with the provisions of this security policy, all contracts and general terms and conditions. The customer is the personal data controller for their users of Iskraemeco cloud services and therefore responsible for:

- Abiding by technical instructions for the use of cloud services and this security policy.
- Controlling personal data and other data of their users and respecting the relevant legislation.
- Specifying instructions for processing of personal data and other data.
- Correcting data on time and ensuring accuracy of data in cloud services.

Cloud Service User: Users of Iskraemeco cloud services are employees of customers (e.g. administrator of the customer's cloud environment), employees of Iskraemeco in case the customer has a contractual agreement for a fully managed cloud service, or customer's clients whose data is being processed by the cloud service.

Data Processor: Iskraemeco is the data processor of data in its cloud services. This includes the data about user's activity, received personal and other data about the users of cloud services. As a data processor, Iskraemeco is responsible for compliance with the relevant legislation and contractual requirements defined by cloud service customers, which may include:

- Ensuring security of personal data processing,
- Keeping records of data processing activities,
- Cooperation with the supervisory authorities and law enforcement officials,
- Informing personal data controllers about data breaches and other security incidents pertaining to them,
- Obtaining an approval from the personal data controller for engaging sub-contractors for data processing,
- Abiding by the relevant legislation regarding personal data protection.

Third Party Suppliers: Third party suppliers are contractors who ensure capabilities to Iskraemeco for providing services and under set conditions. Third party suppliers must fulfil security requirements defined in contracts and the relevant legislation for personal data protection, when providing their services. Third party supplier may have access to personal and other data for the purpose and in scope required for providing services.

Security, Legal and Compliance Team: ensures a contact point for providing information regarding personal data protection, intellectual property protection and reporting security incidents in cloud services, which may include:

- Notifications about personal data and other data breaches,
- Compliance with legislation and standards and
- Security risk assessments.

The information security sector, headed by the Security officer, is responsible for managing the information security in Iskraemeco. The sector is responsible for managing security procedures and policies as well as monitoring the execution of security controls from standards and the relevant legislation. All systems undergo a periodic security check, security risk assessments and monitoring and elimination of vulnerabilities.

Customers must abide by security policy guidelines and the product documentation to ensure a high level of information security. This security policy defines requirements regarding the implementation of appropriate security controls and data protection in Iskraemeco cloud services. The policy complements internal organizational regulations, general terms and conditions and contractual agreements relevant to Iskraemeco services.

Compliance

The right protection of information and information system is vital importance for Iskraemeco's business. With the changes in legislation, changes in organisation of the company and services, occurrence of new threats, incidents and the changes of technical infrastructure that influence on the protection of information and information security system, the information security management system will constantly be adjusted with the enrolment and supplementation of pre-existing procedures and security measures. Iskraemeco is yearly inspected for fulfilment in the balance of the enforced information security management system, so it is obliged to consider all of the demands of the standards ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 and the valid legislation.
Every noncompliance of the Iskraemeco policy regulation, security policies or procedures and instructions is counted as a violation of the contract about employment (for employees) or the contract about cooperation (for contractual partners) and can be sanctioned.

All internal organizational regulations, security policies and instructions are retained in Iskraemeco for at least five years after expiration or replacement by a new document.

Compliance with applicable regulation requirements

Iskraemeco and its whole activity needs to be in accordance with the accepted legal and regulatory acts, with ratified international contracts and with the primary and secondary EU legislation. The management binds itself and ensures that the company works in accordance with the whole accepted legislation and other relevant regulations.

The management is responsible, if needed together with the legal service, for following the changes of the legislation and other regulations. In case of any new requirements, Iskraemeco will align any changes in the information security management system with this document.

Legal department is responsible for compliance with regulatory.

Communication with customers

Iskraemeco will inform customers about important information regarding operation of cloud services, which may include:

- Notifications about important changes and maintenance in cloud services and/or by third party suppliers and,
- Notifying about detected security incidents, risks and vulnerabilities pertaining to customer's cloud environment and/or endangering personal and other data security.

Processing of personal and other data

Iskraemeco may obtain personal and other data from directly from the customer or indirectly from cloud service usage. Types of personal and other data collected by Iskraemeco include information about the user's session, connection and settings. This kind of information is kept in system logs, that are sufficiently secured as described in paragraph Data storage security.

Iskraemeco processes personal and other data exclusively in accordance with the purpose, instructions and requirements of the customer and a legitimate interest, which may include:

- Analysis of customer's service usage for improving the user experience, quality and security of cloud services based on the usage and
- Marketing activity and advertisement.

Storing personal and other data

Country of storage: Personal and other data is stored and processed in countries, where data centres of the third-party supplier are located (Microsoft Azure) and in countries where Iskraemeco premises are located. Iskraemeco does not transfer personal data to third countries. In cases when a transfer to a third country is needed, it can be granted in accordance with adequate measures for information security valid in Iskraemeco and requirements in contracts with customer. The list of data centres Microsoft Azure is available at *Global Infrastructure | Microsoft Azure*.

Retention period: Iskraemeco processes personal and other data for the period of valid contractual agreements with customers and until the fulfilment of contractual obligations. In order to comply with the relevant legislation and other regulative, Iskraemeco must retain personal and other data for a specified period.

Cessation of data storage (deletion/removal of data): Cancelation of the contract with a customer means Iskraemeco will cease to process personal and other data for the purposes provided in this policy. At the end of the retention period, Iskraemeco performs a removal of personal and other data in accordance with secure practises for data deletion and contractual measures.

Iskraemeco deletes all temporary files (e.g. system logs, documents) that include personal and other data, as soon as the reason for their storage ceases to exist.

Data storage security

Information security: Iskraemeco ensures security of personal and other data with security measures in the fields of technical security, physical security, communications security, operations security and human resources security. Iskraemeco uses proven security practices for monitoring systems. Development and operation of services takes place in a secure environment compliant with security controls from standards ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018, which may include:

- Protection of transactions of application services,
- Ensuring data encryption at rest and data encryption in transit,
- Change management,
- Principle of secure system engineering,
- Secure storage and restricted access to software source code,
- Backups of critical information sources (e.g. databases, virtual machines),

- Monitoring of cloud services and cloud infrastructure from the information security perspective,
- Controlling and managing technical vulnerabilities,
- Segregation of environments and data of different customers with a logical segregation of networks and
- Protection against malicious activities.

More details about the implemented security controls are documented in the technical documentation, internal security regulations and instructions, that cover a certain area of the cloud infrastructure.

Third party supplier (Microsoft) providing data centre capabilities to Iskraemeco, has implemented security measures described on its website at *Azure security documentation | Microsoft Learn*. The third party supplier providing data centre capabilities to Iskraemeco ensures compliance with different security standards listed on its website at *Azure compliance documentation | Microsoft Learn*.

Disclosure of personal and other data

Iskraemeco can disclose personal and other data to law enforcement or other state authorities, based on legal requirements and in accordance with procedures established by law. All requests for disclosure must be justified and have a legal basis. Customers can request Iskraemeco to disclose the data in accordance with contractual obligations and regulations of this policy.

Iskraemeco may disclose personal data to third persons only with prior consent of the customer and provided that it is recorded to whom, which data and when it was disclosed. Third persons may be third party suppliers, who need personal or other data for providing services to Iskraemeco. Third persons handle personal and other data in accordance with the relevant legislation and the contract with Iskraemeco for data processing. Iskraemeco checks if third persons meet the requirements for processing and security of personal and other data.

Customer rights (complaints)

Iskraemeco allows customers to exercise their right to:

- Access to personal and other data being processed by Iskraemeco,
- Rectification of inaccurate data being processed by Iskraemeco,
- Erasure and restriction of processing of personal and other data,
- Object to the processing of personal and other data under legitimate interest,
- Portability of their personal and other data, that was passed to Iskraemeco.

Customer can fill a complaint in case of suspected rights violation during personal and other data processing by Iskraemeco. Customer can exercise their right to appeal, by sending a written complaint by email to dpo@iskraemeco.com or by mail to Iskraemeco, d.d., Savska Loka 4, 4000 Kranj. Iskraemeco will handle complaints with measures and information within legally requested timeframes and in accordance with obligations in contracts with the customer.

Security incidents

Iskraemeco treats security events and incidents in cloud services as a priority. Customers are notified about important security events and incidents that affect their cloud environment or deployment within the time period defined in their contract or based on regulatory requirements. Notifying customers is described in the document »Iskraemeco Case Management System and Material Returns Management Process«, which covers the case management process. Iskraemeco notifies about any event which is not part of the standard operation of a service and which causes or may cause, an interruption to, or a reduction in, the quality of the service.

Customers can report detected security events and incidents and are expected to do so as soon as possible. Security events and incidents can be reported through the Case management system in line with the process mentioned above.

In case of a data breach incident or an incident involving personal information, Iskraemeco follows the established process for security event and incident management in line with security policies, notifies the customer with impacted users and if needed the competent authorities in accordance with legal obligations.

Iskraemeco will provide access to system logs and other evidence information of the customer's cloud environment on customer request and in accordance with contracted obligations. Access is granted in a secure way to prevent any negative impact on digital evidence.

Personal data breaches: Iskraemeco treats personal data breaches as security incidents. Customer is obligated to report any breaches in cloud services to Iskraemeco for investigation. Personal data breaches in cloud services in Iskraemeco are treated in accordance with the incident management process and legal obligations.

Clock synchronization

There must be a synchronization of clocks between the customer and Iskraemeco to ensure accurate time determination of events. Clock synchronization is important for accuracy of system logs, which may be used as evidence in investigations. Iskraemeco synchronizes its server infrastructure with the UTC standard through the central source on Arnes. Clock synchronization is automatic with the network time protocol, meaning all clocks on servers and workstations are in sync.

This security policy is formed to follow guidance from standards ISO 27001, ISO 27017, ISO 27018 and valid legal obligations. The policy is updated regularly and is publicly accessible on Iskraemeco's webites.