# SCOPE

## General

JSC NC “KazMunayGas” (hereinafter KMG) was established pursuant to Decree No. 811 of the President of the Republic of Kazakhstan dated 20 February 2002 On Activities to Further Pursue State Interests in the National Oil and Gas Sector, and RoK Government Resolution No. 248 dated 25 February 2002 On Activities to Enforce Decree No. 811 of the RoK President dated 20 February 2002.

The core activities of KMG are set out in KMG’s Charter approved by the decision of the entity that owns all the voting shares of KMG — Samruk-Kazyna JSC.

KMG has developed and implemented an information security management system (hereinafter the ISMS), which proves KMG’s ability to select adequate and commensurable information security controls that ensure the security of information resources when using them in KMG’s operations. The adoption of the ISMS is a strategic decision for KMG.

The ISMS is based on the requirements of ISO/IEC 27001:2013 Information Technology. Security Techniques. Information Security Management Systems. Requirements.

The ISMS preserves the confidentiality, integrity and availability of information and assures the interested parties that the risks are adequately managed.

The ISMS is part of the overall management structure, while information security is incorporated into the entire cycle of information system development as well as in relations with suppliers.

The Information Security Management System Manual (hereinafter the Manual) describes the implementation of ISO/IEC 27001:2013, roles and responsibilities of KMG’s employees and business units involved in the information security process. Conflicting roles and responsibilities shall be separated for the purposes of high-quality organisation of the ISMS.

## Scope of the ISMS

The territorial scope of the ISMS includes KMG’s HQ located at: 8 Kunayev Street, Nur-Sultan.

The ISMS applies to all business units of KMG.

The scope of the ISMS includes the following types of resources and technology:

1) primary information security resources:

 - information (information assets);

 - processes;

2) secondary resources:

 - hardware;

 - software;

 - services or business applications;

- network and (or) network equipment;

 - human resources;

 - resources related to KMG’s location (premises, physical security areas and security systems, telecommunications and equipment maintenance services, life support systems).

The ISMS applies to the following processes:

Consolidation of Business Plans, Financial Statements and Management Reports;

Management of Geological and Geophysical Information Systems.

The scope of the ISMS is defined in accordance with the current version of the Information Security Policy of JSC NC “KazMunayGas” (approved by the Resolution of the Management Board of JSC NC “KazMunayGas” dated 10.11.2015, minutes No. 55, item 12) and may be revised if necessary. The scope of the ISMS may be expanded during testing with the consent of the supervising managers.

# Regulatory References

The following international standards were used to develop the ISMS:

[ISO/IEC 27001:2013](http://ru.wikipedia.org/wiki/ISO/IEC_27001) Information Technology. Security Techniques. Information Security Management Systems. Requirements;

[ISO/IEC 27002:2013](http://ru.wikipedia.org/wiki/ISO/IEC_27002) Information Technology. Security Techniques. Code of Practice for Information Security Controls;

[ISO/IEC 27003:2017](http://ru.wikipedia.org/w/index.php?title=ISO/IEC_27003&action=edit&redlink=1) Information Technology. Security Techniques. Information Security Management Systems. Guidance;

[ISO/IEC 27004:2016](http://ru.wikipedia.org/w/index.php?title=ISO/IEC_27004&action=edit&redlink=1) Information Technology. Security Techniques. Information Security Management. Monitoring, Measurement, Analysis and Evaluation;

[ISO/IEC 27005:2018](http://ru.wikipedia.org/w/index.php?title=ISO/IEC_27005&action=edit&redlink=1) Information Technology. Security Techniques. Information Security Risk Management.

# DEFINITIONS AND ABBREVIATIONS

The following definitions and abbreviations are used in this Manual:

|  |  |
| --- | --- |
| **Availability of Information** | - the state of information when the subjects that have the right of access (the right to use, read, change, copy, destroy information) can exercise it freely |
| **Confidentiality of Information** | - the state of information when it is accessed only by the subjects that have the right to do so |
| **Integrity of Information (Resources)**  | - the state of information when it is changed only intentionally by the subjects that have the right to do so |
| **Information Security (IS)** | - the state of protection of KMG’s information space, as well as the rights and interests of KMG and each of its employees in the information sphere, from real and potential threats, which ensures the confidentiality, integrity and availability of information assets |
| **Information** **Asset** | - information and information carriers that are of value to KMG, the risk of loss of confidentiality/integrity/availability of which may result in material or other losses |
| **IS Incident** | - a single event or a number of undesirable or unexpected events in information security that put business processes at great risk or threaten information security |
| **Information Security Management System (ISMS)** | - part of the overall management system based on the risk assessment of information security, which is intended for the design, implementation, operation, monitoring, analysis, maintenance and improvement of information security |
| **ISMS Management Representative** | - an employee of KMG appointed by the order of the Chairman of KMG’s Management Board from among the management, heads of functional units or from among the heads of business units directly subordinate to the Chairman of the Management Board and responsible for information security |
| **ISMS** **Manager** | - an employee of the CSD responsible for the day-to-day management of the ISMS  |
| **Scope of the ISMS****Declaration on the Applicability of ISMS Controls of JSC NC “KazMunayGas”** | - processes, business units and resources within certain territorial boundaries that are subject to KMG’s ISMS- a document describing KMG ISMS controls. It is based on Appendix A of ISO/IEC 27001:2013 |
| **ISMS Users** | - employees of all business units of KMG (for the purposes of this Manual) |
| **IS Risk** | - a potential risk of damage to KMG from an IS threat (IS incident) due to the presence of vulnerability |
| **ISMS Working Group** | - a permanent body established at KMG for ISMS management and maintenance |
| **IS Threat** | - a potential cause of an IS incident that could cause damage to KMG |
| **Vulnerability**  | - a flaw or a weakness in the information system or a process that may be an enabler for an IS threat |
| **Information Systems** | - a set of methods, processes and software and hardware combined in a process chain for the collection, storage, processing and dissemination of information  |
| **Information Technology (IT)** | - a system of means, methods, techniques and models for implementing information processes using electronic and digital technology and information systems |
| **IT Unit** | - business units of KMG in charge of information technology |
| **KMG**  | - Joint-Stock Company “National Company “KazMunayGas” |
| **CSD** | - the Corporate Security Department |

# Information Security Management System

## General Requirements

KMG has developed, implemented, operates, constantly monitors, reviews, maintains and improves the ISMS. The main elements of the ISMS are described in the ISMS documentation.

The goal of implementing the ISMS at KMG is to: ensure the confidentiality, integrity and availability of information and the continuity of business processes.

The key objectives of the ISMS are:

- understanding of ISMS requirements by all KMG employees and third-party representatives who have access to KMG’s information resources;

- implementation and operation of ISMS risk management controls;

- ISMS performance monitoring and review;

- continuous improvement of the ISMS based on objective measurements.

To protect the information and means of its processing from breach of confidentiality, integrity and availability, the CSD and IT Unit shall use organisational, physical, technical, software and hardware facilities of the ISMS.

ISMS support measures meet the requirements of the legislation of the Republic of Kazakhstan, the requirements of contracts signed by KMG, as well as the requirements for KMG information security.

A process approach shall be applied to ISMS management procedures, which implies consistent implementation of the following steps:

- determining KMG’s requirements for the ISMS, and the policy and objectives of the ISMS;

- implementing information risk management (ensuring compliance with ISMS requirements) as part of the overall process of managing all KMG risks;

- monitoring and checking the implementation of ISMS processes;

- revising the requirements for the ISMS (in accordance with the changes in KMG’s business requirements) and improving ISMS management procedures.

The PDCA model (Plan — Do — Check — Act) is mainly applicable to the structure of ISMS processes. This model consists of four consecutive steps to be performed for each process:

- planning;

- implementation;

- performance review;

- improvement.

For the effective performance of management system processes, the PDCA model shall be applied cyclically, i.e. all steps shall be regularly repeated. If necessary, other models (or their elements) can be applied to management procedures.

## Establishment and Management of the ISMS

### Establishment of the ISMS

KMG has taken the following steps to establish the ISMS:

1) the scope of the ISMS has been defined;

2) the Information Security Policy of JSC NC “KazMunayGas” has been developed and approved by KMG’s Management Board;

3) the risk assessment approach at KMG has been defined, the risk assessment procedure, risk acceptance criteria have been described and acceptable risk levels have been determined in accordance with the Information Security Risk Management Rules of JSC NC “KazMunayGas” **(KMG-PR-1752.3-22)**;

4) KMG’s risks have been identified. The Resource Inventory Report **(KMG-F-1755.3-22/PR-1752.3-22)** and the Catalogue of Information Security Threats **(KMG-F-1756.3-22/PR-1752.3-22)** specify the valuable resources of KMG, the owners of resources and potential threats to these resources;

5) risks have been analysed and rated for significance, the adverse impact of the loss of confidentiality, integrity or availability of resources, the probability of resource and control security breach and risks have been assessed;

6) opportunities for risk treatment have been identified and evaluated;

7) targets and controls for risk treatment have been selected;

8) expected residual risk has been approved by the management;

9) the management has authorised to implement and operate the ISMS;

10) plans have been developed to define specific actions, deadlines, action owners, as well as the necessary resources, to achieve information security objectives;

11) the Declaration on the Applicability of ISMS Controls of JSC NC “KazMunayGas” has been developed.

### Operation of the ISMS

KMG has formulated and implemented an IS risk management action plan for risk prevention or mitigation and for the ISMS to continuously be capable of achieving the targets.

KMG has developed and implements controls to achieve control objectives that comply with the Information Security Policy as well as with the risk assessment results. The controls are described in the ISMS documents.

### Continuous Monitoring and Review of the ISMS

Continuous monitoring and review of the ISMS shall be conducted to identify and prevent security incidents and to determine the effectiveness of measures taken to eliminate them. All actions and events that could adversely affect the performance of the ISMS shall be recorded. In this case, information security and information technology functions shall be separated.

IS incidents shall be managed in accordance with the ISMS Incident Management Procedure of JSC NC “KazMunayGas” **(KMG-RI-1946.2-22)**.This is based on a consistent and effective approach to managing information security incidents, including reporting on security events and vulnerabilities.

The ISMS Manager shall prepare an ISMS performance review plan and have it approved by the ISMS representative of KMG’s management. ISMS performance review shall be performed in accordance with the Procedure for Performance Evaluation of Selected Controls and Information Security Management System of JSC NC “KazMunayGas” **(KMG-RI-1951.2-22)** and the Regulations on the Management System Council of JSC NC “KazMunayGas” **(KMG-PL-1093.7-59)**.Based on the evaluation results, the ISMS Manager shall prepare an ISMS performance evaluation report and have it approved by the ISMS management representative.

The purpose of the information security review is to confirm that information security is provided and managed in accordance with the Information Security Policy and ISMS documents.

Legal compliance review shall be performed in accordance with the Procedure for Information Security Management System Review for Compliance with Legislative and Contractual Requirements of JSC NC “KazMunayGas” **(KMG-RI-2024.2-22)**.

###  Maintenance and Improvement of the ISMS

The ISMS Manager shall:

1) regularly coordinate the maintenance and improvement of the ISMS by implementing all identified improvements in the ISMS, applying the information security experience of other organisations;

2) make all interested parties aware of all actions aimed at improving information security, the contribution of KMG’s employees to the performance of the ISMS, and of the possible consequences of failure to comply with the requirements of the ISMS.

## Documentation Requirements

KMG’s ISMS documentation shall be maintained to the extent necessary for the effective operation of the ISMS, including records of management decisions, and also enable reproducibility of results, demonstrating the relationship between the results of the risk assessment and treatment from the selected controls.

KMG’s ISMS documentation includes:

- documented statement of the information security policy and objectives;

- description of the scope of the ISMS;

- ISMS support procedures and controls according to the list of ISMS documentation;

- description of the risk assessment procedure;

- risk assessment report;

- risk treatment plan.

ISMS documentation shall be managed in accordance with the IMS Document Management Rules **(KMG-PR-1.13-59)**.

# Management Responsibility

## Management Commitment

KMG’s management is committed to the establishment, implementation, operation, constant monitoring, review, maintenance and improvement of the ISMS in accordance with the requirements of ISO/IEC 27001:2013, as well as to the integration of the requirements of this standard with the existing management system of KMG. This commitment is expressed in the following actions:

- approval of the Information Security Policy, which is reviewed for adequacy and relevance at planned intervals or in case of significant changes in KMG’s management system;

- making a decision on the risk acceptance criteria and acceptable risk levels;

- approval of business continuity plans, risk treatment plans, etc.;

- approval of the ISMS role structure;

- encouraging and supporting KMG’s employees who contribute to ISMS performance;

- consideration of information security in project management;

- providing a sufficient number of resources for the establishment, implementation, operation, constant monitoring, review, maintenance and improvement of the ISMS;

- conducting internal audits of the ISMS, ensuring the achievement of ISMS targets;

- ISMS management review;

- constant communication with authorities and organisations on information security issues, learning best practices;

- systematically raising awareness of all employees of KMG and interacting organisations about the importance of compliance with the information security objectives and Information Security Policy of JSC NC “KazMunayGas”, KMG’s responsibility under the laws of the Republic of Kazakhstan and KMG’s need for continuous improvement of the ISMS.

## Resource Management

Realising the importance of information resources for all business processes, KMG’s management declares that maintaining the ISMS is the responsibility of KMG’s employees along with their official duties.

The Chairman of KMG’s Management Board shall be responsible for the correct application of all implemented controls of the ISMS, which include initiating KMG information security measures, providing the necessary resources for the operation of the ISMS to support business requirements with information security procedures, monitoring the implementation of ISMS activities, demonstrating leadership and commitment to the ISMS.

The ISMS shall be headed by the Chairman of KMG’s Management Board, who manages it through an ISMS management representative. The ISMS management representative shall be appointed by the order of the Chairman of KMG’s Management Board from among the management or heads of business units directly subordinate to the Chairman of the Management Board and responsible for information security.

Regardless of his/her main job responsibilities, the ISMS management representative shall be responsible for:

- defining specific goals and current tasks for solving information security issues;

- day-to-day management, implementation of a unified policy and effective operation of the information security management system;

- coordinating ISMS-related interfaces with external organisations;

- considering together with the management representative for the integrated management system and deciding on problematic issues of the ISMS within his/her competence;

- making sure information security and risk management standards, policies and rules are applied by KMG;

- advising KMG’s management on information security;

- periodic assessment of information security risks and compliance with policies, procedures and rules;

- coordinating the information security training of KMG managers and employees, making KMG’s employees aware of ISMS requirements;

- monitoring and analysing the results of information security incident drills;

- ensuring the approval of developed policies, tasks, procedures and indicators for information security assessment;

- studying and analysing information security incidents, response to information security incidents and developing measures to improve network and information security;

- initiating the disciplinary action against KMG’s employees for violating the requirements of ISMS documentation;

- monitoring the implementation of information security documents approved by KMG’s management;

- managing the permanent working group on ISMS management and maintenance of JSC NC “KazMunayGas” (hereinafter the ISMS Working Group), and engaging business units in information security activities in coordination with the supervising manager;

- preparing reports with analyses of information security incidents, developing measures to mitigate and prevent such incidents.

The ISMS management representative shall duly interact with all business units of KMG, subsidiaries and dependent entities of KMG, and other organisations and government authorities in accordance with his/her powers.

In case of temporary absence (illness, business trip, vacation, etc.) of the ISMS management representative, his/her functions shall be performed by a person appointed by the order of the Chairman of KMG’s Management Board.

Day-to-day management of the ISMS shall be carried out by the ISMS manager assisted by process owners.

The ISMS manager shall be responsible for:

- development of ISMS documents;

- development, implementation, management and improvement of the ISMS;

- initiating ISMS internal audits;

- advising the ISMS management representative on information security;

- periodically assessing information security risks and developing risk mitigation plans;

- documenting information security incidents and immediately reporting them to the ISMS management representative.

All issues of ISMS development, updating and operation shall be resolved by the ISMS Working Group as advised by the ISMS management representative and Working Group members.

The ISMS Working Group shall be responsible for:

- expert consultations of the ISMS management representative and ISMS manager on specific information security issues;

- performing specialised performance evaluations of the ISMS as instructed by the ISMS management representative or ISMS manager;

- updating ISMS documents as applicable;

- suggesting improvements in the field of information security.

The CSD shall be responsible for monitoring the security of software and hardware that protect KMG’s information, compliance with security requirements for the protection of electronic document management, targeted use of Internet resources, monitoring of information security incidents.

The IT Unit shall be responsible for monitoring and maintaining the proper and smooth operation of KMG’s information and telecommunications infrastructure.

The heads of business units within the scope of the ISMS shall be responsible for:

- successful implementation, maintenance and improvement of the ISMS within the scope of their processes;

- determining the need for advanced information security training of employees of their business units, informing third parties on information security issues;

- making sure employees of their business units and third parties follow the requirements of ISMS documents in accordance with their contracts;

- making their employees aware of the information disclosure procedure;

- immediately reporting to the ISMS manager on incidents identified by employees or weaknesses found in information security;

- encouraging and supporting, together with the CSD, their employees who contribute to ISMS performance in accordance with KMG’s internal documents.

KMG’s employees within the scope of ISMS shall be responsible for:

- compliance with ISMS documents;

- compliance with the requirements for information security at the workplace (the clear screen and clear desk policy) and when using mobile devices;

- immediately reporting to the head of business unit on identified incidents or weaknesses found in information security.

Disciplinary action may be taken against KMG’s employees who have violated information security requirements.

The procedure for training, awareness raising and competence of information security personnel is described in the following documents:

Rules of Competitive Selection for Administrative Job Openings of JSC NC “KazMunayGas” **(KMG-PR-838.7-47)**;

Internal Labour Regulations of JSC NC “KazMunayGas” **(KMG-PR-
1167.3-6)**;

Personnel Training and Development Rules of JSC NC “KazMunayGas” **(KMG-PR-434.8-6)**;

Personnel Employment, Transfer and Relocation Procedure of JSC NC “KazMunayGas” **(KMG-RI-898.6-6)**.

# Internal ISMS Audits

KMG shall regularly (at least once a year) conduct an internal ISMS audit.

The internal ISMS audit shall be initiated by the ISMS manager. All operations necessary for the internal ISMS audit shall be planned to ensure the confidentiality, integrity and availability of KMG’s information resources, as well as business continuity.

Internal ISMS audits shall be conducted in accordance with the Process Audit Rules of JSC NC “KazMunayGas” **(KMG-PR-147.8-59)**.

# Management Review of the ISMS

**7.1 General**

The Chairman of the Management Board shall at least once a year review the performance of the ISMS to ensure its suitability, adequacy and effectiveness as well as compliance with ISO 27001:2013 and KMG’s internal requirements.

This review shall include an assessment of the opportunities for improvement and need for changes to the ISMS, including the information security policy and information security objectives. The technical compliance review of IS shall be regularly performed by the responsible employees of the IT Unit.

The Chairman of the Management Board together with the ISMS management representative shall determine the date of a meeting of the Security Management System Council of JSC NC “KazMunayGas” for ISMS review.

If necessary, unscheduled ISMS review meetings may be held as advised by one of the IMS and ISMS Council members.

The review shall evaluate the current status and compliance of the ISMS, on the basis of which the Chairman of the Management Board shall make decisions on further improvement of the system.

All security-related members of the IMS and ISMS Council, as well as other concerned employees, shall take part in the ISMS review meeting.

The agenda of the meeting shall be prepared by the ISMS manager in agreement with the ISMS management representative, reviewed by the Chairman of the Management Board and communicated to all participants of the meeting within two business days before it is held in accordance with the Regulations on the Management System Council of JSC NC “KazMunayGas” **(KMG-PL-1093.7-59)**.

**7.2 Review Input**

For ISMS management review, the ISMS management representative will initiate preparation of a report on ISMS performance and the state of IS at KMG.

The heads of business units shall provide inputs for the report to the ISMS manager within a certain time frame.

The report shall include the following:

- follow-up actions from the previous management review;

- vulnerabilities or threats not adequately addressed in previous risk assessments;

- results of ISMS audits and reviews;

- correction of nonconformities identified during audits and inspections, status of corrective actions;

- techniques, products or procedures, as well as any changes, which could be used by KMG to improve the ISMS performance and effectiveness;

- results from effectiveness measurements and recommendations for improving the ISMS.

**7.3. Review Output**

KMG management review outputs shall include decisions related to the improvement of the system, processes and procedures necessary for the best effectiveness of the ISMS. The review shall identify the need to change the ISMS policy and objectives and the need for resources necessary for further improvement of the ISMS.

Decisions made as a result of the management review shall be aimed at:

- improving the effectiveness of the ISMS;

- updating the risk assessment and risk treatment plan;

- modifying procedures and controls that affect information security, as necessary, to respond to internal or external events that could negatively impact the ISMS. These include: business requirements, security requirements, business processes effecting the existing business requirements, regulatory or legislative requirements, contractual obligations, risk levels and/or risk acceptance criteria;

- resource needs;

- improvement to how the effectiveness of controls is being measured.

Decisions taken based on KMG management review shall be documented in the minutes of a meeting of the Management System Council of JSC NC “KazMunayGas” with the indication of action owners and deadlines.

# Improvement of the ISMS

KMG’s management shall ensure the necessary competence of persons on whom the effectiveness of information security depends through appropriate training. ISMS corrective action and improvement plan shall be approved based on the decisions taken following KMG management review. The continual improvement of the ISMS shall be achieved through the consistent implementation of corrective and preventive actions in accordance with the Process Audit Rules of JSC NC “KazMunayGas” **(KMG-PR-147.8-59)**.

1. **Information Security Controls**

The control objectives and controls are set out in the Declaration on the Applicability of ISMS Controls of JSC NC “KazMunayGas”.

1. **Final Provisions**

This Manual and all amendments thereto shall be approved by KMG’s Management Board.