INFORMATION SECURITY AND DATA PROTECTION FRAMEWORK POLICY

IGDP_P1 VERSION 1.00

ALADDIN MIDDLE EAST LIMITED – TURKEY BRANCH OFFICE

INFORMATION SECURITY AND DATA PROTECTION FRAMEWORK POLICY

1. INTRODUCTION AND SCOPE

1.1. This document constitutes the Aladdin Middle East Limited – Turkey Branch Office Information Security and Data Protection Framework Policy (hereinafter referred as the "Framework Policy").

Data Controller : ALADDİN MİDDLE EAST LİMİTED ŞİRKETİ - TÜRKİYE ANKARA ŞUBESİ (Aladdin Middle East Limited – Turkey Branch Office)
Address : Karum İş Merkezi, İran Cad.No:21/394 Kavaklıdere - Ankara, Türkiye
Telephone : + 90 312 427 90 20
Mail : kvkk@ame.com.tr
Web Site : https://aladdinmiddleeast.com/
Field of Activity : Oil Exploration and Oil Drilling

Framework Policy gives an overview of the policies, codes of practice, notices and guidelines that apply to information governance and data protection at the Aladdin Middle East Limited – Turkey Branch Office (hereinafter referred as the "Company" or "AME Turkey"); it also sets out the Company's commitment to providing information governance training and increasing awareness in this area.

1.2. This Framework Policy pulls together all the requirements for information governance so that all Company information is processed legally, securely, efficiently and effectively. Information plays a key part in the AME Turkey's day to day operations and governance. The quality of the Company's services, planning, performance measurement, assurance and financial management relies upon accurate and available information. Robust information governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. Accordingly, this Framework Policy sets out the requirements, standards and best practice that apply to the handling of information and data protection and privacy.

1.3. Information governance is a key responsibility of each and every member of the Company staff. Every staff member has a part to play in implementing

and embedding our policies and codes of conduct into the Company's working practices. So, AME Turkey's staff must familiarize themselves with this Framework Policy and the policies it describes. This Framework Policy and the information governance it sets are also expected of any third parties handling Company information.

1.4. The purpose of this Framework Policy is to assist our Company in fulfilling its responsibilities listed below.

- comply with its legal, regulatory and contractual obligations;
- maintain robust corporate governance;
- deliver high quality services;
- protect company's financial resources;
- put in place appropriate business continuity arrangements;
- ensure and improve the continuity of the security of the data under AME Turkey's control.

1.5. The Company holds and processes huge volumes of standard and sensitive data that is necessary for service provision, ensuring the continuity of commercial relations and commitments and ensuring the job security of employees.

2. SCOPE

2.1. This Framework Policy covers all information held by the Company or on behalf of the Company whether in electronic or physical format including by way of example:

- electronic data stored on and processed by fixed and portable computers and storage devices;
- data transmitted on networks;
- information sent by fax or similar transfer methods;
- all paper records;
- microfiche, visual and photographic materials including slides and CCTV;
- spoken, including face-to-face, voicemail and recorded conversation.

2.2. The following parties are expected to comply with the Framework Policy:

- All member of Company staff;

- Any third parties handling, or having access to, Company information including for example consultants, service providers and contractors, visitors.

2.3. The Framework Policy consists of two parts – the first part describes the AME Turkey's overarching information governance and data protection strategy and the second part sets out the information governance roles and responsibilities, policies and training that shall be implemented.

2.4. For the purpose of this Framework Policy and of other instruments to be adopted pursuant to it, the following definitions shall apply:

(1) "Personal data" - defined in Article 4 of the General Data Protection Regulation and Article 3(1)(d) of the Law on Data Protection (Law No: 6698) as any information relating to an identified or identifiable natural person (referred to as a 'data subject'), where an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. The collection, use and retention of personal data must comply with strict conditions and such data requires special measures of protection as more particularly described in the Company's Data Protection Policy;

(2) Sensitive personal data (also known as special categories of data) is a subset of personal data - this is defined in Article 6 of the Law on Data Protection (Law No: 6698) as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. The processing of sensitive personal data is subject to additional requirements and requires additional protections also as described in more detail in the Company's Data Protection Policy;

(3) The data listed below, non-personal data (organizational data), shall be referred to as the organizational data of the Company:

(a) Sensitive organizational data which includes commercially sensitive planning / administrative or research data, data protected by confidentiality agreements, legally privileged information, etc. This data set should be protected by appropriate protection measures; and

(b) Non-sensitive organizational data which is data pertaining to Company not published by default, but which may be disclosed (subject to legal

advice) in response to requests made under the Freedom of Information Act (Law No 4982).

3. PURPOSE

3.1. The aim of Company's corporate strategy is to enable the AME Turkey to meet its information management, data privacy and security responsibilities so that customers, businesses, partners and suppliers have the confidence that information is handled and stored with due regard to its value and risk. All relevant parties must understand the importance of using information correctly, of sharing it lawfully and of protecting it from improper use.

3.2. The intention of this strategy is also to enable the AME Turkey to meet its legal and ethical obligations in terms of the following:

- lawful use and security of personal identifiable information;
- appropriate and lawful disclosure of information when required;
- regulatory frameworks for the management of information;
- professional codes of conduct for consent to the recording, sharing and uses of information;
- operating procedures and codes of practice adopted by the Company;
- information exchanged with third parties.

3.3. The strategy recognizes the high standards expected of the AME Turkey as well as the ongoing task of maintaining appropriate standards of security in the area of information governance and of embedding a security culture regarding personal data in all echelons of the Company.

3.4. The Strategic Objectives of the Company regarding Information Security and Privacy of Personal Data are as follows:

- Information governance inside the Company should be an enabler to the Company's overall strategy as well as to the underlying departmental strategies and business transformation programs and information assurance practices are to be embedded within the design and implementation of such strategies and programs;
- the infrastructure and processes for service delivery to provide the right information to the right people at the right time for the right purpose and promote the provision of high quality services by promoting the ethical, legal, effective and appropriate use of information;

- to provide innovative solutions to information governance issues with a view to transforming business processes;
- to promote information governance ensuring that it is embedded throughout our organization and to direct organizational wide cultural change so that information is regarded as a key asset;
- to integrate into staff competencies and job descriptions specific requirements regarding information governance;
- to encourage staff to work together in order to prevent duplication of effort and enable more efficient use of resources;
- to work to achieve required standards to comply with legislative, regulatory and contractual obligations and relevant policies;
- to identify and manage information assets used by the Company and introduce an information risk management system that balances risks with opportunities;
- to implement and operate proportionate controls that apply best practice standards to protect information assets and give confidence to all interested parties;
- to provide adequate training to all members of our workforce and key partners, increase awareness and embed a culture of care and responsibility in the handling of all information throughout the Company.

4. CORPORATE APPROACH

4.1. Information governance and data protection are integrated into all aspects of AME Turkey's operations. In delivering information governance services, four key elements will be taken into consideration:

- people
- process
- information
- technology

4.2. All information governance, improvement and assurance activities will take into consideration how these factors need to operate in combination to achieve our strategic objectives.

4.3. The delivery of our information governance strategic objectives will be implemented via a range of projects and a dedicated Information Security Management Program. The Program will define each information governance project, and these will be implemented and monitored in accordance with the

stated governance arrangements and the approach detailed within this Framework Policy.

4.4. We anticipate that the following benefits will be achieved with the implementation of this strategy:

- consistent and effective management of information across the Company;
- increased understanding of and compliance with relevant legislation;
- reduced frequency of information security incidents;
- reduced staff time and effort;
- improved data quality;
- clear responsibilities in relation to Information Governance and data protection;
- effective management of information risks;
- greater confidence that information risks are effectively managed;
- better management of oil exploration and research data, with protection of intellectual property.

4.5. The General Director is responsible for implementing this strategy. Under the chairmanship of the General Manager, the Personal Data Protection Committee is responsible for monitoring the Development Program and reporting the progress achieved throughout the year. The Information Security and Personal Data Protection strategy will be implemented through the agreed upon policies, development programs and projects. At the end of each year, the Personal Data Protection Committee will decide on the development programs envisaged for the following year, based on the agreed priorities and available resources. The General Manager will approve the development programs agreed by the Personal Data Protection Committee.

4.6. Relevant Concepts and Their Explanations

4.6.1 ISMS (BGYS): Information Security Management System

4.6.2 Inventory: All kinds of information assets important to the company

4.6.3 Senior Management: Senior Officers of the Company

4.6.4 Know-How: practical knowledge or skill; expertise.

4.6.5 Confidential Information: Information, like all other corporate and commercial assets, is an asset that represents a business value and must therefore be appropriately protected. Within the company, know-how, administrative processes, formulas, techniques and methods, customer records, marketing and sales

information, personnel information, commercial, industrial and technological information and secrets shall be considered as CONFIDENTIAL INFORMATION.

4.6.6 Confidentiality: It is the restriction of Access privileges to the content of information by granting access exclusively to those who are allowed to view the information / data. (Example: With the usage of encryption in e-mail transfers, even if e-mail is compromised, unauthorized persons can be prevented from reading e-mail's content - Registered e-mail address- REM)

4.6.7 Integrity: Data integrity refers to the accuracy and consistency (validity) of data over its lifecycle via detection of unauthorized or accidental changes, deletions or additions of information, and ensuring detectability of data breaches (E.g.: Storing data in the database with summary information - electronic signature - mobile signature)

4.6.8 Availability/Accessibility: The data availability is about the timeliness and reliability of access to and use of data. In other words, the systems are always available and the information in the systems is not lost and always accessible. (Example: Use of uninterruptible power supply and redundant power supply in chassis to prevent servers from being affected by power line fluctuations and power outages - UPS)

4.6.9 Information Asset: It refers to assets that the company owns, which are important in order to carry out its activities without interruption. Information assets within the scope of the processes subject to this policy are:

- All kinds of information and data maintained in paper, electronic, visual or audio media,
- All kinds of software and hardware used to access and change information,
- Networks that enable the transfer of information,
- Facilities and special areas,
- Departments, units, teams and employees,
- Solution partners,
- Services, goods or products provided by third parties.

4.7. In the organization chart found in appendix of this Framework Policy, the actors that will take part in information governance inside the Company and their duties are specified.

4.7.1 Responsibilities of Senior Management

- The Company Management undertakes that it will comply with the defined and implemented Information Security and Personal Data Protection System, allocate the necessary resources for the efficient operation of the system, and ensure that the system is understood by all employees. The General Manager is responsible for evaluating and minimizing information security risks and will ensure that the relevant policy and awareness is spread to everyone who needs to know across the Company. Information and data security risks will be addressed in a similar way to other risk factors related to financial, legal and corporate reputation. The Information Governance Steering Group (chaired by the General Manager) is responsible for monitoring and reporting progress on the improvement program throughout the year.

-For the implementation of the Information Security and Personal Data Protection Strategy, the Data Protection Liaison Officer is appointed by the General Manager. When necessary, this Policy document may be revised by the senior management and the assignment may be renewed.

- Department Chiefs and Division Managers shall help the staff at lower levels in terms of distributing responsibility and setting an example. It is necessary that vision of the senior level management is implemented at the lowest level of the company. For this reason, all managers must support their employees in compliance with safety instructions in writing or verbally, and in participating in security related work and preparations.

-Senior Management shall assign necessary budgetary resources needed for expenditures related with information security.

Data Protection Liaison Officer is responsible for signing of data sharing and processing agreements and additional protocols with the relevant stakeholders and establishing and maintaining the enterprise vision, strategy and programme that will be valid for the access and transfer of Company Data within the scope of its activities.

4.7.2. Data Protection Liaison Officer

Data Protection Liaison Officer is responsible for establishing and maintaining the enterprise vision, strategy and programme to protect information assets and systems. His/her activities that will be carried out within this framework is listed below:

- Planning the Information Security and Personal Data Privacy Framework, determining the acceptable risk level and the risk assessment methodology,

- Providing consultancy to Senior Management in terms of necessary resources for supportive and complementary activities in the establishment of Information Security and Personal Data Privacy framework, providing / improving user capabilities and raising awareness, training, providing communication, providing documentation requirements

- Execution and management of Information Security and Personal Data Privacy framework, ensuring the continuity of evaluations, improvements and risk assessments,

- Organization of internal audits, goals and management review meetings, and evaluation of Information Security and Personal Data Privacy frameworks and controls,

- Maintaining the current structure of Information Security and Personal Data Privacy framework and ensuring continuous improvements.

4.7.3 Heads of Department: Heads of Department are responsible for consideration of information governance implications across their department and when working with partners. Other responsibilities are listed below:

- Implementation of inventory setup and management of information assets regarding their department and carrying out risk analysis for their information assets,
- Informing the Data Protection Liaison Officer for risk assessment when there is a change in the information assets under their responsibility that will affect the level of information security risks.

-Ensuring that their subordinates comply with their Department policies and procedures.

- Instilling awareness among the work force regarding ISMS, ensuring communication, providing necessary documentation,

- Heads of Department are responsible for evaluating the working processes of their department and the issues related to information management concerning activities carried out jointly with stakeholders. Please review the Information Security Policy regarding the specific responsibilities to be undertaken regarding information security.

4.7.4. Information Asset Owners

Information asset owners are the assigned owners of Company's information assets as listed in the AME's Information Asset Register. They are responsible for assessing information security and data privacy risks annually using the "Code of

Practice Data Privacy Impact Assessment" or an approved alternative form of assessment determined per data provider for their assets and implementing appropriate measures accordingly.

4.7.5. All Company Staff and Authorised Third Parties

-Carrying out their work in compliance with our information security goals, policies and information governance framework and relevant documentation,

-All staff members are supposed to follow information security goals of their units and work in order to reach these goals.

- Being attentive to and reporting any information security vulnerabilities occurred or suspected in Company systems or services,

- Signing confidentiality agreements and imposing additional relevant information security requirements to service contracts (consultancy, etc.) concluded with third parties that are not under the responsibility of Purchasing.

- All Company staff as well as authorised third parties who use and have access to Company information must understand their personal responsibilities for information governance and comply with the law. All staff must comply with AME's policies, procedures and guidance and attend relevant education and training events in relation to information governance.

5. GENERAL PRINCIPLES OF INFRMATION SECURITY

5.1. Company staff and authorized 3rd parties must familiarize themselves with details of the information security requirements and rules outlined in this policy and relevant procedures and to carry out their work in accordance with these rules.

5.2. Aforementioned rules and policies will be taken into account for the use of all information and all information systems stored and processed in printed or electronic media, unless otherwise specified.

5.3. Information Security and Personal Data Privacy Framework shall be structured and operated on the basis of Law No 6698 on Personal Data Protection (i.e. KVKK), GDPR (EU General Data Protection Regulation), TS ISO / IEC 27001 standard of "Information Technology Security Techniques and Information Security Management Systems Requirements".

5.4. Implementation, operation and improvement works of the Information Security and Personal Data Privacy Framework shall be carried out with the contribution of the relevant parties. It is the responsibility of the Data Protection Liaison Officer to update the relevant documents when necessary.

5.5. The information systems and infrastructure provided by the company to employees or third parties and all kinds of information, documents and products produced using these systems are property of the Company, unless otherwise specified in legal provisions or contracts signed.

5.6. Confidentiality and non-disclosure agreements shall be signed with employees, employees of companies that provide consultancy services to the Company, service providers (security, catering, cleaning companies etc.), the and inters hired.

5.7. Information security checks shall be determined and implemented in order to be applied to hiring, reassignment and cease of employment.

5.8. Trainings that will increase the awareness of information security among staff and contribute to the functioning of the system shall be offered to current Company employees and new employees.

5.9. All actual or suspected information security breaches shall be reported. Post factum evaluations shall be carry out to determine discrepancies that may have caused security breaches and appropriate measures shall be taken to prevent recurrence of such events.

5.10. Inventory of all information assets shall be establishes in accordance with information governance necessities and asset owners shall be assigned for each information asset.

5.11. Personal and company data shall be classified and security necessities and usage rules shall be determined for each category.

5.12. Physical security controls and measures shall be implemented for information assets maintained in secure places.

5.13. Necessary controls and policies shall be developed and implemented against physical threats that information assets of the company may be exposed inside and outside the company.

5.14. Procedures and instructions regarding capacity management, relations with third parties, backup, system acceptance and other security processes shall be developed and implemented.

5.15. Audit record generation configurations for network devices, operating systems, servers and applications shall be set up in line with the security needs of the relevant systems. Audit records shall be protected against unauthorized Access via appropriate measures.

5.16. Access rights shall be assigned pursuant to Access needs of relevant asset owners. State of the art technology and techniques shall be used for Access control management.

5.17. Security requirements shall be determined regarding system procurement and development, and it shall be checked whether or not security requirements are met in system acceptance or tests.

5.18. Sustainability plans shall be prepared for critical infrastructure and necessary measures shall be taken in order to ensure maintenance of such structure

5.19. The necessary processes shall be designed in order to ensure compliance with laws, internal policies and procedures, technical security standards and continuous compliance shall be ensured through periodic surveillance and auditing activities.

6. POLICIES THAT WILL BE ADOPTED WITHIN THE FRAMEWORK

6.1. The Information Governance and Data Privacy Framework encompasses the following policies and codes of practice

Type of Document	Reference Numbers	Title
POLICY	IGDP_P1	Information Security and Data Protection Framework Policy
POLICY	IGDP_P2	Data Protection and Processing Policy
POLICY	IGDP_P3	Data Retention and Management Policy
POLICY	IGDP _P4	Data Protection Policy for Company Staff
POLICY	IGDP _P5	Information Security Policy
POLICY	IGDP _P6	Conditions of Use of IT Resources (Acceptable Use Policy)
POLICY	IGDP _P7	Access Control Policy
POLICY	IGDP _P8	CCTV Policy
POLICY	IGDP _P9	Internet & Electronic Communication Acceptable Use Policy
CODE OF PRACTICE	IGDP_CoP1	Code of Practice for Response Procedures for Data Subject Access Requests
CODE OF PRACTICE	IGDP_CoP2	Data Breach Response Plan

CODE OF PRACTICE	IGDP_CoP3	Code of Practice Data Privacy Impact Assessment
CODE OF PRACTICE	IGDP_CoP4	Code of Practice Inspection of Electronic Communications and Data
CODE OF PRACTICE	IGDP_CoP5	Code of Practice Electronic Messaging
CODE OF PRACTICE	IGDP_CoP6	Code of Practice CCTV Procedures
CODE OF PRACTICE	IGDP_CoP7	Code of Practice Usage of Passwords
CODE OF PRACTICE	IGDP_CoP8	Code of Practice Data Transfer Security
NOTICE	IGDP_N1	Privacy Notice for Prospective Employees
NOTICE	IGDP_N2	Cookie Policy
NOTICE	IGDP_N3	CCTV Privacy Notice
NOTICE	IGDP_N4	Data Subject Access Request Form
NOTICE	IGDP_N5	General Data Protection Notice
NOTICE	IGDP_N6	WebSite Privacy Notice
NOTICE	IGDP_N7	Contractor Privacy Notice
FORM	IGDP_F1	Subject Access Request Form

6.2. **Policy Development**

6.2.1. Information Governance Steering Group reviews and submit its recommendations of changes to all information governance policies to Senior Management. All policies are made available to staff via the internet and are communicated via regular updates to staff.

6.2.2. Existing policies are updated, and new policies introduced in line with requirements, with policies reviewed on an annual basis. These policies must be read in conjunction with staff employment contracts and/or regulations as appropriate.

6.2.3. Policies outline scope and intent and provide staff and relevant stakeholders with a robust information governance framework whilst setting out their responsibilities. AME Turkey is committed to ensuring that all staff and those working with it are familiar with the Company's objectives and what is expected in order for these to be achieved. Policies and procedures are one of the key means AME Turkey uses to communicate these expectations with staff and partners.

6.3. Training and development

6.3.1. Information governance training and development is essential for the development and improvement of staff knowledge and skills relating to information governance across all echelons of the Company.

6.3.2. Information governance and security training must extend beyond basic confidentiality and security awareness in order to develop and follow best practice. Staff must understand the value of information and their responsibility for it, which includes data quality, information security, records management, confidentiality, etc.

7. MONITORING COMPLIANCE WITH THIS FRAMEWORK POLICY

7.1. Information Governance Steering Group retain overall responsibility for monitoring compliance with this Framework and review of each policy.

7.2. Policies and procedures must be reviewed at least once a year. Apart from this, they must be reviewed after any changes that may affect the system structure or risk assessment, and if any change is required, it should be approved by the senior management and recorded as a new version. Each revision should be published so that all users can access it.

7.3. Management review meetings are organized by the Data Protection Liaison Officer and held with the participation of Senior Management and Department Chiefs. These meetings, where the suitability and effectiveness of the Information Security Management System are evaluated, are held at least once a year.

8. NON-COMPLAINCE WITH THIS POLICY AND SANCTIONS

In the event that that the Information Security and Personal Data Framework Policy and Standards are violated, the sanctions specified in the relevant articles of the contracts, which are also applicable for the Third Parties, are applied to the employees responsible for this violation according to the Company Discipline Directive and Procedure.