STATUTE OF THE SECURITY DEPARTMENT OF THE STATE OIL FUND OF THE REPUBLIC OF AZERBAIJAN

1. GENERAL PROVISIONS

1.1 The Security Department (the Department hereafter) is a structural unit of the State Oil Fund of the Republic of Azerbaijan (the Fund hereafter).

1.2 The Department is guided by the Constitution of the Republic of Azerbaijan, the laws of the Republic of Azerbaijan, the decrees and orders of the President of the Republic of Azerbaijan, the “Statute of the State Oil Fund of the Republic of Azerbaijan”, the decrees and orders of the Fund, as well as this Statute in its activities.

1.3 The Department operates in collaboration with other structural units of the Fund in fulfilling the functions identified by this Statute.

2. THE MAIN OBJECTIVES OF THE ACTIVITIES OF THE DEPARTMENT

The main objectives of the Department are the management of the Information Security of business activities and physical security of the building, territory and office areas.

3. THE FUNCTIONS OF THE DEPARTMENT

The Department has the following functions:

3.1 International standard based information security risk and incident management as well as the information technology and document management infrastructures monitoring are utilized to ensure sustainability of the Fund’s business processes.

3.2 Safety of business operations of the Fund is achieved through the prevention of threats to the Fund’s interests, protecting the territory, office area and people from illegal actions and organizing emergency protection measures.

4. THE RESPONSIBILITES OF THE DEPARTMENT

Information security project management and analytics:

4.1 Determination of information security risks, their probabilities and damage to business processes, risk management (acceptance, transfer, reduction and prevention) and prioritization, defining the framework for incident management and incident response schemes (detection-monitoring, inform, block, track, fallback, evaluation, evidence collection, remediation, emergency), clarification of the implementation models;

4.2 Organize development of projects and documentation for implementation and maintenance (continuous improvement) of Information Security Management System (hereinafter – ISMS), including information protection methods (procedures and regulations describing processes adequacy against possible threats);

4.3 Classify information protection roles and responsibilities, develop privilege separation matrix and related coordination projects;

4.4 Threat modelling analysis of the incidents happen (threat source – the objective – the target - disrupted requirement – vulnerability used – realization scheme - damage) and residual risk assessment;

4.5 Evaluation of the damage of the information security incidents to business continuity;

4.6 Identify information security incident trends, summarize collected experience on the regular basis and provide corrective recommendations.

<u>Information security risk management:</u>

4.7 Identification and assessment of information security threats, threat schemes, possible internal and external threat sources and other factors, perform a risk assessment;

4.8 Arrange activities towards creation, protection and usage of the risk register;

4.9 Participate in determination of the need for protection methods and appropriate security tools (for software, hardware and information assets), provide feedbacks on mentioned tools' specifications;

4.10 Examine the projects related to protection scope for compliance with information security requirements;

4.11 Define and control the implementation of guidelines for configuration parameters of the audit logs for security tools and registration rules;

4.12 Test current and renewed infrastructure’s configuration for vulnerabilities and compliance with security requirements;

4.13 Provide corrective recommendations for security methods and tools with regard to current and renewed infrastructure.

Information security incident management:

4.14 Determine the importance level and classification of possible incidents;

4.15 Submit proposals for the projects related to incident management, complement incident management system with necessary tools and components, define incident response procedures;

4.16 Practically organise formation and activities of information security incident response teams;

4.17 Monitor information security posture of subjects, protection methods and information security tools, evaluate information Security events (whether there is an incident), select and initiate an appropriate incident response procedure;

4.18 Collect the usage statistics of threat schemes and related components, as well as the usage of Security tools;

4.19 Provide corrective proposals to information Security risk management in incident related objects and processes.

Information Security Awareness

4.20 Track and classify information security trends, regulatory requirements and best practices;

4.21 Classify target groups of information security (objects participating in information process, processes and subjects);

4.22 Development and maintenance of the knowledge base of information security incidents;

4.23 Collect statistics and provide recommendations for information security events (including incidents) caused by human factors;

4.24 Inform interested parties about information security events happened in the Fund;

4.25 Prepare information security competency requirements for management, specialists and other personnel participating in ISMS;

4.26 Create training programs for the management, specialists and other personnel categories.

The organizational and analytical activities regarding physical security

4.27 Monitor activities of the structural departments of the Fund to comply with the security requirements;

4.28 Participate in the elaboration of the documents regulating the activity of the fund (rules, instructions, etc.) and to ensure the reflection of the guidelines related to security issues in these documents;

4.29 Proposal submissions for the design of systems, facilities and equipment for physical security, and control over their installation;

4.30 The accounting of the Fund's financial resources allocated for the physical security and the control of their use;

4.31 Maintain official relations with the representatives of local law-enforcement agencies and Security services of neighboring enterprises to maintain public law and order in the vicinity of the SOFAZ and also to study the criminal situation around;

4.32 Collect and analyze the cases of violation of safety rules and other legal and technical requirements related to the overall operation of the Fund and information on actions directed against the interests of the Fund, to forecast possible consequences for the physical security of the Fund;

4.33 Periodically assess the effectiveness and validity of the measures taken to ensure the physical security of the Fund;

4.34 Inform the Fund's Executive director about the risks to the physical security of the Fund, if necessary, inform the relevant government authorities with his permission;

4.35 Preliminary investigations of incidents related to the physical security of the Fund;

4.36 Take measures to improve the professional training of employees working in the field of security, to upgrade their skills and ensure proper moral and psychological training.

Protection of Fund's administrative building, the territory and property of the administrative building, ensuring the physical safety of employees and other persons in the building

4.37 Organize the protection of the perimeter of Fund's building and his territory with police forces, identifying the necessary measures and procedures to eliminate possible negative consequences of threats in extreme, ensure the training of personnel in this regard, and also the coordination of their activities with the police officers;

4.38 Take measures to eliminate the conditions, which might lead to the violation of Fund's security requirements;

4.39 Take measures to ensure the security of Fund in the event of breaches, inform the management according to the accepted rules;

4.40 Ensure the arrival of additional police forces in the event of criminal infringement in the Fund's administrative building or adjacent territories by means of security alarm systems and alarm buttons.

Ensuring the security of Fund's special regime zones

4.41 Determine the borders, categories and the risks of the Fund's special regime zones, ensure their adequate protection;

4.42 Ensure the security of the Fund's treasury operations in the Vault area;

Organizing of the check in regime in the Fund's building

4.43 Define the check-in regime and the Fund's internal security regime;

4.44 Organize the provision of service and temporary cards and their registration for an authorized entrance to the building of people and cars, ensure the control of compliance with these rules;

4.45 Ensure the control and registration of the delivered to the Fund goods and materials and the permitted withdrawal of goods and materials from Fund's building;

Ensure of fire regime and organizing of evacuation in emergency cases

4.46 Define the fire regime in the Fund's administrative building and their territory;

4.47 Ensure the control of compliance of the Fund employees and other persons in the building with aforementioned fire regime;

4.48 Carry out actions to eliminate the conditions that may cause the violation of fire security rules of the Fund;

4.49 Take measures to ensure safe and unhindered evacuation in case of emergency;

4.50 If necessary in case of emergency organizing the evacuation of property from the administrative building of the Fund;

Civil defense

4.51 The implementation of organizational measures to ensure the civil defense;

4.52 Ensure the trainings for the Fund's staff about the obligations and measures that should be taken in emergency situations, as well as during techno-genic accidents, using of weapons of mass destruction, natural disasters and epidemics;

4.53 Exercise control on fulfilling the requirements of civil defense in the Fund's building.

Maintenance of physical security systems

4.54 Using the capabilities of physical security systems to ensure the security of the Fund;

4.55 Analyze the data coming from physical security systems and use it in the investigation of the causes and consequences of incidents;

4.56 Ensure the proper exploitation and continuous work of safety equipment and facilities, including communications, security and defense means, control the timely and necessary maintenance;

4.57 Develop measures to eliminate weaknesses in the security of the Fund in order to prevent the information leakage from the Fund by ways and means not envisaged in the procedures approved by relevant documents.

5. ORGANIZATION OF THE OPERATIONAL PROCESS OF THE DEPARTMENT

5.1. The organizational structure and the number of employees of the Department are determined by the Executive Director of the Fund.

5.2. The operations of the Department are overseen by the Director of the Department. The Director of the Department is appointed and dismissed from his position by the Executive Director of the Fund. The Director of the Department bears personal responsibility for the accomplishment of the responsibilities assigned to the Department.

5.3. The Director of the Department:

5.3.1. Organizes and controls activities of the department.

5.3.2. Allocates work the employees under his/her supervision, coordinates their activities and monitors the execution of duties and oversees employee discipline in the workplace.

5.3.3. Informs the management of the Fund on important issues about the activities of the Department.

5.3.4. Provides the management of the Fund with proposals regarding the enforcement of appropriate incentives and disciplinary measures for the employees of the Department.

5.3.5. Ensures the review of incoming letters, requests, complaints and proposals in accordance with the legislation.

5.3.6. Ensures the execution of the clerical work of the Department.

5.3.7. Represents the Department.

5.3.8. In the case of absence of the Department Director, his/her duties are delegated to the Deputy Director of the Department.

5.4. The Department consists of the following divisions: Information Security Division and General Security Division (the Division hereafter). The activities of the Division are overseen by the Head of Division. The Head of Division is appointed and dismissed from his position by the Executive Director of the Fund. The Head of Division bears personal responsibility for the accomplishment of the responsibilities assigned to the Division. In the case of absence of the Head of Division, his/her duties are delegated to one of the employees within the Division.

5.5. The responsibilities of the Department are indicated in the "Responsibilities of the Department" section and covered in articles 4.1-4.14.

The responsibilities of Information Security Division are covered in articles 4.1. – 4.29.

The responsibilities of the General Security Division are covered in articles 4.30. – 4.57.

5.6. The Head of Division:

5.6.1. Organizes and controls activities of the Division.

5.6.2. Allocates responsibilities among the employees under his supervision, coordinates their activities and monitors the execution of duties and oversees employee discipline.

5.6.3. Regularly updates management of the Fund on important issues related to the activities of the Division.

5.6.4. Provides the Director of the Department with proposals regarding the implementation of incentives and disciplinary measures for the employees of the Division.

5.6.5. Ensures the execution of the clerical work of the Division.

5.6.6. Represents the Division.

6. THE MAIN OPERATION METHODS OF THE DEPARTMENT

The functions of the Department defined by the current statute realized by the methods listed below:

6.1. Preventive – minimize or prevent probability of threats and vulnerabilities.

6.2. Privilege separation – definition of responsibilities and goals of information security.

6.3. Registration – ensure promptly registration and logging of security events

6.4. Detection – timely detection of incidents and affected subjects

6.5. Response and contain – response to incidents and impact containment

6.6. Recovery – recovery of security posture

6.7. Analyze – analysis of information security incidents and evaluation of protection.