|  |  |  |
| --- | --- | --- |
| эмблема | **JSC "National Company "KazMunayGas"** | |
| Document title: | **Corporate Regulations for Physical Security and Counter-Terrorism Protection of Joint-Stock Company "National Company "KazMunayGas"** | |
| Document type: **Regulations** | **KMG-RG-3818.1-22** | **page 1** **of 79** |
| Developed by: V. Kulikov  2 December 2020 | Checked by: T. Aliaskarov  2 December 2020 | Approved by JSC NC KMG Management Board Resolution  dated 15 December 2020  Minutes No. 53 |

1. **Goal of the Regulations and General Provisions**
   1. The Corporate Regulations for Physical Security and Counter-Terrorism Protection of JSC NC “KazMunayGas” (the Regulations) are a basic document that defines primary goals, objectives, general philosophy and areas of Physical Security and Counter-Terrorism Protection activities of the KMG Group.
   2. The Regulations reflect the single vision, standardised guidelines and approaches to management and operation of the Physical Security and Counter-Terrorism Protection System of the Company to protect Security Objects.
   3. The goal of the Regulations is to create conditions for sustainable development of the Company through implementation of measures of the Physical Security and Counter-Terrorism Protection System to avoid, prevent and/or minimise potential Damage for Security Objects from Unauthorised Actions, including Unlawful Attacks and Acts of Terrorism.
   4. Goals of the Regulations are achieved through implementation of measures of the Physical Security and Counter-Terrorism Protection System combined with measures of the other areas of the Corporate Security System: economic, internal, information.
   5. Objectives of the Regulations:
2. establish single standards, approaches and standard procedures (regulatory control) for management and provision of Physical Security and Counter-Terrorism Protection of the Company;
3. identify Real and Potential external and internal Threats to sustainable development of the Company, timely report them;
4. develop effective mechanisms to counteract Potential and Real Security Threats to legal rights and interests of the Company;
5. develop and implement comprehensive and consistent measures to prevent and avoid Unauthorised Actions, including Unlawful Attacks and Acts of Terrorism against Security Objects, and to eliminate their causes, conditions and consequences.
6. improve the level of training and professional competence of employees of the Company’s Corporate Security Units, employees of security companies and other companies involved by the Company to ensure Security under the corresponding contracts.
   1. These Regulations consider requirements of Samruk-Kazyna Corporate Security Standard approved by Resolution of Samruk-Kazyna Management Board dated 26 December 2018, Minutes No. 42/18.
7. **Scope**
   1. Requirements and philosophy of the Regulations apply to KMG and SDE, are secured and maintained by implementation of legal, organisational and technical measures.
   2. SDE may, as required, develop and duly approve their own internal documents to specify approaches to implementation hereof given the specifics and features of their activities.
   3. Orders, guidelines, instructions and other internal documents governing Physical Security and Counter-Terrorism Protection of the Company, and contracts for the corresponding services, shall not contradict requirements hereof.
8. **Definitions and abbreviations**
   1. Definitions and abbreviations featured herein have the following meanings:

|  |  |  |
| --- | --- | --- |
| **Accident** | - | Destruction of buildings, facilities and/or technical devices, uncontrolled explosion and/or release of hazardous substances. |
| **Act of Terrorism** | - | Committed or threatened explosion, arson or other actions threatening to kill people, inflict considerable property Damage or other publicly dangerous consequences, if such actions are carried out to disturb public safety, intimidate population or influence decisions of state bodies of the Republic of Kazakhstan, by foreign states or international organisations, and endangering human life with the same purposes, endangering life of a state or public figure to terminate his/her public or other political activities, or to revenge any such activities. |
| **Counter-Terrorism Protection** | - | A group of legal, organisational measures and technical devices to ensure Counter-Terrorism Protection of the Facility. |
| **Counter-Terrorism Security** | - | A condition of the Facility described as availability of conditions that prevent an Act of Terrorism, and minimise or eliminate consequences of such Act. |
| **Lessee** | - | A company occupying premises in buildings of KMG and SDE under a lease or on other legal grounds. |
| **Security** | - | A condition of a Company’s Security Object when there is no unacceptable Risk associated with any harm from materialisation of any Threat or its consequences. |
| **Site Security Arrangements** | - | Arrangements established by the owner, which do not contradict the law of the Republic of Kazakhstan and have been communicated to employees, Lessees, Contractors/Subcontractors, Visitors and other persons, ensured by a group of activities and guidelines fulfilled as required by the internal code of conduct, fire safety requirements and other documents establishing behaviour of Employees and Visitors, and provision of Security. |
| **Internal Security** | - | A condition of security of Company resources against Real and Potential Threats associated with failure to fulfil or improper fulfilment by the Company Employees of their employment duties. |
| **First Response Team** | - | A team intended for immediate response after actuation of alarm at the infrastructure of Guarded Facilities and in case of complications of the situation until integrated forces, including law enforcement, arrive. |
| **Industrial Safety Declaration for a Hazardous Production Facility** | - | A document reflecting nature and magnitude of the danger posed by a hazardous production facility, activities to ensure industrial safety and protect population against harmful effects of hazardous occupational factors during commissioning, operation and decommissioning of a hazardous production facility. |
| **Duty Unit** | - | Round-the-clock dispatching service that controls forces and means of a Private Security Company, monitors provision of Security Activities by Security Units. |
| **Security Subsidiary** | - | KMG-Security Limited Liability Partnership; |
| **Personal Data Protection** | - | A group of measures, including legal, organisational and technical measures, taken for the purposes established by the personal data law; |
| **Exclusion Zones** | - | Areas of terrain directly adjacent to the engineering fencing of a Facility, free of constructions, trees, shrubs, etc. |
| **Protected Zone** | - | A Facility site accommodating buildings, premises with systems, equipment, devices and materials that may, together or individually, become a target of an Unauthorised Action, surrounded by permanently Guarded and monitored physical barriers, with restricted and controlled access. |
| **Emergency Zone** | - | A territory where an emergency has occurred. |
| **Information Security** | - | A state of information security of KMG’s and SDE’s information space, rights and interests of KMG and SDE and each Employee against real and potential threats when sustainable development, integrity and availability of KMG’s and SDE’s information resources are provided for authorised users. |
| **Security Equipment Systems**  **(SES)** | - | Devices, systems and special structures used to ensure security of the Guarded Facilities against unauthorised trespassing, theft of tangible assets or other valuables, Unauthorised Actions, Unlawful Attacks, Acts of Terrorism. |
| **Engineering Fortification** | - | Structural elements, utilities and/or their combinations counteracting unauthorised trespassing at a Facility or its part. |
| **Categorisation of the Guarded Facility** | - | Systemic division of Guarded Facilities according to Security Threats to ensure the best protection management. |
| **K9 Unit** | - | A dedicated area designed to use a working dog to guard the Facility. |
| **Emergency Classification** | - | Division of Emergencies by classes depending on how dangerous they are for human life and health, disturbance of living conditions, the magnitude of Damage/harm. |
| **The Company** | - | Joint name of KMG and SDE. |
| **Gate House**  **(GH)** | - | A dedicated location designed to control, give passage, examine people and vehicles. |
| **Trace Control Strip** | - | A strip of land with the surface that, in its natural condition or after special treatment, retains and saves visible prints of Offenders. |
| **Critical Zone/Element of the Facility** | - | A room, area or structural element that may lead to disruption of normal operation of, damage to or accident at the Facility if destroyed as a result of an Unlawful Attack, including an Act of Terrorism. |
| **Linear Part of a Trunk Pipeline** | - | Underground, underwater, on-ground, above-ground pipelines that directly transport products. |
| **Trunk Pipeline** | - | A single production and process package comprising a linear part and facilities for safe transportation of products that complies with technical regulations and national standards. |
| **Reinforcements of Engineering Fortification and Safety Systems** | - | A group of activities to improve strength of structural elements of buildings, rooms, and to use unauthorised intrusion detection, fire detection and extinguishing equipment in an effective manner. |
| **Mobile Team** | - | A team that patrols protected zones of trunk pipelines to inspect them periodically, take measures to Secure them and prevent attempts of Unauthorised Actions, including Unlawful Attacks and Acts of Terrorism against them. |
| **Offender** | - | A person who has violated the rules of behaviour at the Guarded Facility established by the law or the owner. |
| **Security Squad** | - | A part of the Site Security Unit (a team, shift, First Response Team, etc.) appointed for physical Security Guarding of the Facility. |
| Unauthorised Actions  (UAA) | - | Direct actions committed by an Offender against the Facility that violate the law, legal regulations and Site Access Control and Site Security Arrangements, including Unlawful Attacks and Acts of Terrorism. |
| **Inspection Post** | - | A post where a Security Guard guards one or more Facilities by walking around them, with the post being over 100 m but not more than 300 meters long. |
| **Facility** | - | A company/institution with an organised team of Personnel, and/or a building, facility, a group of buildings and facilities or their part. |
| **Facilities Vulnerable to Terrorist Attack**  **(FVTA)** | - | Particularly important state-owned, strategic facilities and facilities of strategically important economy sectors, hazardous production facilities, places of mass gathering of people, the [list of](jl:31440340.0 ) and the corresponding requirements for which are established by the Government of the Republic of Kazakhstan. |
| **Personal Data Processing** | - | Actions to accumulate, store, modify, supplement, use, distribute depersonalise, block and destroy Personal Data. |
| **Security Objects** | - | Objects that need to be secured, including personnel, tangible assets (immovable and movable property), financial assets (cash money, deposits, investments in securities, liabilities of other companies, etc.), non-property assets (intellectual property, information, business reputation, etc.). |
| **Critical Infrastructure** | - | Healthcare, telecommunication, communication, gas supply, power supply, heat supply, water supply and water discharge organisations with buildings, facilities, process units and sets that will disrupt operation of social and engineering infrastructure of settlements and lands if their operation is shut down/suspended. |
| **Hazardous Production Facility** | - | Factories, production units and other objects of such factories demonstrating signs established by the Civil Defence Law and identified as such by the hazardous production facility identification guidelines approved by an authorised industrial safety body. |
| **Guarded Facility** | - | A standalone guarded secured room/land containing tangible assets or other valuables, or several rooms distributed across one or several buildings in the same area. |
| **Trunk Pipeline Protected Zone** | - | A territory (onshore and/or offshore) with special Security and usage arrangements, which is adjacent to Trunk Pipeline Facilities and intended to ensure public safety and create the necessary conditions for safe and uninterrupted operation of Pipeline Facilities, where activities that are incompatible with its purpose are restricted or prohibited. |
| **Facility Security Guarding** | - | A prescribed combination of organisational activities, engineering equipment and actions of people to prevent Unlawful Attacks on the Guarded Facility, eliminate or minimise threat to life and health of people, and to protect Security and Safety Equipment Systems against deliberate incapacitation. |
| **Guarded Zone/Area** | - | Zones/areas allocated within the Facility, parts of a building (construction or facility), rooms and their structural elements to be guarded, since, if damaged/destroyed, they may lead to disruption of normal operation of the Facility. |
| **Security Guard** | - | An employee of a private security company, at least 19 years of age, who has been duly trained and passed advanced training, and who directly guards Facilities. |
| **Site Security Unit** | - | A unit that guards Facilities, implements Access Control activities and Site Security Arrangements, under a contract with a private security company. |
| **Security Alarm** | - | Acquisition, processing, transmitting and displaying information about trespassing at the Guarded Facilities in the predetermined format using information equipment. |
| **Security Guarding** | - | Activities by legal entities to protect life, health and property of private individuals and property of legal entities against unlawful attacks (security guarding services). |
| **Counter-Terrorism Security Certificate** | - | A reference document that contains general and engineering details of the facility, reflects status of counter-terrorism security, and is intended to schedule activities to prevent, avoid, minimise and/or eliminate consequences of Acts of Terrorism at a Facility Vulnerable to Terrorist Attack. |
| **Site Perimeter**  (for the purposes hereof) | - | Border of a secured area/zone of the Facility fitted with fencing civil structures (barriers) and gate houses. |
| **Personal Data** | - | Details of a Personal Data Subject that has been or is defined based on such details, recorded on an electronic, paper and/or other physical medium. |
| **Potential Threats** | - | Potential Damage to security interests. |
| **Potentially Hazardous Areas of the Facility**  **(PHA)** | - | Territorially allocated zones/areas, structural and technological elements of the Facility that use, store or operate explosive, fire hazardous, chemical substances, weapons and armour, toxic substances and products, elements of process chains, systems, equipment or devices, Critical Zones of the Facility where an Act of Terrorism may facilitate an accident, threaten to create an Emergency with dangerous social and economic consequences, theft of hazardous substances and materials for further use in an Act of Terrorism. |
| **Right of Way** | - | A piece of land along the inner side of the perimeter fencing intended to create a trace control strip and arrange Security Alarm Equipment, prohibited for unauthorised persons. |
| **Unlawful Attack** | - | A legally prohibited action against a Security Object carried out by a private individual. |
| **Access Control** | - | A group of activities to arrange entrance/exit of people and vehicles to/from the Guarded Facilities, carrying in/out documents and property, and to manage passage and presence of private individuals and vehicles at the Guarded Facilities under special permissions. |
| **SDE Corporate Security Units** | - | Business units or officials implementing tasks and functions to ensure corporate security in SDE. |
| **Contractor/ Subcontractor** | - | A company involved by KMG and SDE to carry out work or provide services under a contract, inter alia, under a subcontract. |
| **Employee** | - | A private individual employed by KMG and SDE and working under an employment contract. |
| **Personal Data Sharing** | - | Actions resulting in transmission of personal data, inter alia, via mass media or by granting Access to personal data or otherwise. |
| **Regulations** | - | An internal document governing activities of KMG and its business units in a certain area. |
| **Management**  (for the purposes hereof) | - | Chairman and members of KMG and SDE Management Board. |
| **Heads of Business Units** | - | Directors of departments, heads of units, standalone subdivisions and departments. |
| **Real Threats** | - | Intentions and capability to inflict Damage to security interests. |
| **Risk** | - | A potential hazard of Damage after materialisation of a threat due to Security Object being vulnerable. |
| **High Security Facility** | - | A Guarded Facility with additional security measures established to maintain its operation. |
| **Safety System** | - | A group of legal, organisational, engineering and other safety measures to ensure Security. |
| **Physical Security and Counter-Terrorism Protection System** | - | A group of legal, organisational, economic, technical and other measures to ensure Physical Security and Counter-Terrorism Protection of Security Objects; |
| **Security Equipment**  **(SE)** | - | Security and warning alarm systems; access control systems; video surveillance and closed-circuit television systems; video analysis equipment; seismic and video detectors; detectors of radioactive, chemical and other harmful substances, detectors of weapons, explosive substances and devices. |
| **Access Control System**  **(ACS)** | - | A group of technically compatible hardware and/or software intended to control access, differentiate rights for access, acquisition and storage of information. |
| **Security Check Systems and Equipment** | - | A group of equipment designed to detect prohibited objects and substances being carried in without authorisation. |
| **Video**  **Surveillance System**  **(VSS)** | - | A group of technically compatible optical and electronic devices, hardware and software designed for visual monitoring over site situation, to acquire, store, transmit, process and display video about site situation. |
| **Security Alarm System** | - | A group of jointly acting equipment designed to detect unauthorised trespassing at a guarded zone/area, violated integrity of a guarded zone/area, to acquire, process, transmit and display information in the pre-determined format about violated integrity of a guarded zone/area. |
| **Public Address System** | - | A group of technical devices designed for prompt warning (visual and/or sound) of people at the facility and/or rescue services about an act of terrorism, the resulting emergency and first response measures in the situation. |
| **Communication System** | - | A group of technical devices designed to transmit/share information, provide dispatching control of forces of the security guarding subject, ensure interaction with the Facility Management (in charge of counter-terrorism protection), law enforcement and special state authorities. |
| **Lighting System** | - | A group of lighting equipment to provide the necessary illumination during night time for the video surveillance system and visibility of offender(s). |
| **Access Control Equipment** | - | Equipment and devices preventing unauthorised access to the Facility. |
| **Stationary Post** | - | A post to guard a standalone Facility or several Facilities in an outdoor site or within a fenced area, if total walk-around distance by a Security Guard is not more than 100 meters. |
| **Personal Protective Equipment** | - | Equipment, including special garments, designed to protect an Employee against exposure to hazardous and/or harmful occupational factors. |
| **Technical Fortification of the Facility/Premises** | - | A group of engineering protections of structural elements, buildings, rooms, their perimeters, Security Equipment (security and warning alarm, access control, video surveillance and closed-circuit television system; detectors of radioactive, chemical and other harmful, substances; detectors of weapons, explosive substances and devices), and fire alarm systems, automatic fire detection and extinguishing systems. |
| **Facility Security Threat** | - | A threat presented by unlawful actions of a person (a group of people) that may result in adverse consequences for the Facility. |
| **Security Threat** | - | A group of conditions, processes and factors preventing Company interests from being implemented or endangering them. |
| Facility Vulnerabilities | - | Critical zones/elements of the Facility, including elements of its Physical Protection System, which may become a target of planned and successful Unauthorised Actions by an Offender because of insufficient protection or stability. |
| **Physical Security** | - | A state of security of material and human resources, information stored on physical media in paper, electronic or another format, against real and potential threats, when their integrity is ensured. |
| **Physical Protection** | - | A set of organisational means, Security Equipment Systems and actions of Security Guarding Units to prevent unauthorised intrusions to the Guarded Facilities, Guarded Zones, and to timely detect and stop any Unauthorised Action, Unlawful Attack on integrity and safety of the Guarded Facilities, including actual and attempted Acts of Terrorism. |
| **Damage** | - | Loss or damage to property of a private individual or legal entity. |
| **Security Company**  **(Private)** | - | A commercial company engaged in the business of providing security services. |
| **Emergency Situation**  **(ES)** | - | A situation at a certain territory resulting from an accident, fire, harmful exposure to hazardous occupational factors, a dangerous natural phenomenon, catastrophe, disaster or another calamity that may result or have resulted in casualties among people, harm to health of people or environment, considerable material damage and disruption of living conditions of people. |
| **Man-Made Emergencies** | - | Emergencies caused by harmful exposure to hazardous occupational factors, traffic accidents and other accidents, fires/explosions, accidents with releases (threatened releases) of highly potent, toxic, radioactive and biologically hazardous substances, sudden collapse of buildings and facilities, failure of dams, accidents at critical power supply and communication systems, treatment facilities. |
| **Economic Security** | - | A state of security of KMG’s business processes against real and potential threats when their sustainable development and steady operation is ensured. |
| **SDE** | - | Subsidiaries and dependent entities including jointly controlled entities and joint ventures of KMG. |
| **CSD** | - | Corporate Security Department of KMG. |
| **KMG** | - | Joint-Stock Company "National Company "KazMunayGas". |
| **SDE CSU** | - | Corporate Security Units of SDEs. |
| **SCC** | - | Security Control Centre − A body that manages security forces of KMG administrative buildings, manages supervision control and interaction with service and fire departments, as well as with duty dispatcher units of SDEs, law enforcement, special and other state bodies. |

* 1. Other definitions and abbreviations featured herein are applicable in accordance with the law of the Republic of Kazakhstan.

1. **Responsibility**
   1. **Company Management** is responsible for appropriate provision of necessary and sufficient human, financial, material and technical resources for the Physical Security and Counter-Terrorism Protection System, and for management of the following activities at the subordinate Facilities in order to:
2. ensure appropriate Access Control and Site Security Arrangements, provide Facilities with state-of-the-art SES in accordance with the requirements for them;
3. develop Counter-Terrorism Protection Certificates based on a typical certificate for the subordinate Facilities;
4. hold preventive activities and drills to train Personnel in examination of premises, detection of potential locations of explosives;
5. schedule and master joint actions together with the concerned state bodies and companies to respond to man-made threats resulting from a committed Act of Terrorism;
6. manage protection of information networks of Facilities, Informational Security;
7. immediately report a committed Act of Terrorism to national security and internal affair bodies of the Republic of Kazakhstan and ensure evacuation of Personnel.
   1. KMG and SDEs provide the necessary funding to implement activities provided by 4.1.
   2. **CSD and SDE CSU** are responsible for:
8. exercising the single policy and coordination of Physical Security and Counter-Terrorism Protection activities of KMG and SDE business units;
9. making arrangements for and recording, systematising, evaluating and reviewing information about Real and Potential Physical Security and Counter-Terrorism Protection Threats to the Company, management of security incidents, making arrangements to identify and prevent them;
10. maintaining proper condition of Company’s Physical Security and Counter-Terrorism Protection Systems;
11. making arrangements for and monitoring status of business processes to ensure Physical Security and Counter-Terrorism Protection of the Company;
12. making arrangements for inspections of Company Facilities to identify effective measures to counteract different types of Unlawful Attacks, including Acts of Terrorism;
13. making arrangements to ensure Technical Fortification of the Guarded Facilities, introduce/add Security Equipment Systems and Special Security Equipment, Access Control Systems, Security Check Systems and Equipment, Access Control Equipment, Surveillance Systems at Facilities;
14. implementation of activities to improve Physical Security and Counter-Terrorism Protection of the Company;
15. making arrangements for and monitoring over implementation of security guarding activities at Company’s Secured Facilities and High Security Facilities;
16. issuing, recording and withdrawing gate passes and creating proper conditions to collect, process, protect and destroy personal data during issue of gate passes by responsible Employees of CSD and SDE CSU;
17. making arrangements for requirements of Access Control and Site Security Arrangements, identification of potential routes for unauthorised access to Guarded and High Security Facilities, taking measures to prevent them;
18. making arrangements for and holding scheduled and unscheduled (sudden) checks of performance of security companies under contracts, and companies maintaining SES, Security Alarm Systems, ACS, Video Surveillance Systems, other Security and Counter-Terrorism Protection Systems;
19. making arrangements for and participation in briefings, trainings and drills together with personnel of Guarded Facilities, Contractors and Lessees;
20. making arrangements for and implementing data exchange with law enforcement, special and other state bodies to identify Potential and Real Security Threats, minimise consequences of potential materialisation.

4.4. **Security Companies involved under security guarding service contracts** are responsible for:

* 1. proper performance and unconditional compliance with the laws governing security guarding, counter-terrorism, circulation of weapons, personal data and commercial secret protection, internal documents of KMG and SDEs governing corporate security;
  2. Physical Guarding of buildings, rooms, facilities, utilities, territories of the Guarded Facilities, prevention and suppression of offences and other UAA, including Acts of Terrorism;
  3. protection of personnel of the Guarded Facilities, persons who permanently or temporarily stay at the Guarded Facilities against criminal and other Unlawful Attacks;
  4. fulfilling obligations to ensure the corresponding Access Control and Site Security Arrangements, hold preventive activities and drills to train Security Guards in examination of rooms, identification of potential locations of explosives, proper application of Counter-Terrorism Protection equipment;
  5. keeping confidential and safeguarding information and documents obtained in the process of work, including Personal Data of Employees of KMG, SDEs, Lessees, Contractors and Visitors, which have become available to them in the process of their activities;
  6. identification of causes and conditions facilitating Damage to the Guarded Facility, and persons involved in infliction of such Damage;
  7. compensation for Damage inflicted as a result of improper services.

4.5. **Employees of the Company, Lessees and Contractors** are responsible for compliance with Access Control and Site Security Arrangements at the Guarded Facilities, and shall inform (orally or otherwise, inter alia, via telephone, SMS, etc.) responsible Employees of CSD and SDE CSU:

1. about suspicious persons or objects detected at the Guarded Facilities;
2. information about committed or attempted Unlawful Attacks on legal rights and interests of the Company;
3. ungrounded interests of third parties to confidential and other restricted information;
4. other offences that may affect Physical, Information, Economic, Internal Security of the Company.

4.6. Persons at fault for a breach hereof shall be liable under the law of the Republic of Kazakhstan and internal Company documents.

* 1. Failure to perform obligations by entities carrying out the Security Guarding activities, which have entered into a Security Guarding Services contract for Guarded Facilities of the Company, including FVTAs, entail liability as provided by the law of the Republic of Kazakhstan and contracts.

1. **Description of the Regulations**
   1. **Basic philosophy and approaches to management and provision of Physical Security and Counter-Terrorism Protection of the Company**
      1. Company's activities to ensure the system of Physical Security and Counter-Terrorism Protection are based on the following principles:
   2. lawful, comprehensive, timely, continuous and active implementation of the established objectives;
   3. economic feasibility and comparability of the potential Damage and costs for operation of the Physical Security and Counter-Terrorism Protection System;
   4. centralised management of the Physical Security and Counter-Terrorism Protection System based on clear interactions between the concerned units and subdivisions;
   5. active engagement of Employees in the processes of the Physical Security and Counter-Terrorism Protection System of the Company.
      1. The Physical Security and Counter-Terrorism Protection System is based on the following approaches:
2. safety and security of Personnel are the priorities of all Company's business processes;
3. measures of the Physical Security and Counter-Terrorism Protection System of the Company are intended to prevent Damage;
4. threats and Risks of Physical Security and Counter-Terrorism Protection are continuously analysed and assessed;
5. security plans of Facilities contain measures to respond to the emerging Threats in a timely manner;
6. all Company Facilities employ the same approach to operation of the Physical Security and Counter-Terrorism Protection System;
7. all Security measures, including level of training of Security Guarding forces, are regularly checked and evaluated by CSD and SDE CSU;
8. Physical Security and Counter-Terrorism Protection of the Company is ensured in compliance with the law and in coordination with state bodies.
   1. **Subjects and Objects of the Physical Security and Counter-Terrorism Protection System of the Company**
      1. Subjects of the Physical Security and Counter-Terrorism Protection System of the Company are:
9. Company Management;
10. CSD and SDE CSU;
11. other business units of KMG and SDEs, fully or within their competence (limited) responsible for one or more types of Security;
12. Security Companies providing Physical Security Guarding, including Counter-Terrorism Protection of Facilities, and companies maintaining SE, security alarm systems, ACS, VSS, other Security and Counter-Terrorism Protection systems of the Company under contracts.
    * 1. The main Subject that coordinates operation of the Physical Security and Counter-Terrorism Protection System of the Company is CSD.
      2. Objects of the Physical Security and Counter-Terrorism Protection System of the Company that may be damaged as a result of materialisation of Potential or Real Threats are:
         1. Management and Employees of the Company, Lessees and Contractors;
         2. financial assets (cash and non-cash money);
13. tangible (fixed) assets and commodities (buildings, facilities, warehouses, production Facilities, equipment, transportation and other);
14. information resources, systems, data arrays and databases, Personal Data to be protected, commercial and other legally protected secrets, insider information and other restricted information stored on physical media, in paper, electronic or other formats;
15. informatisation equipment and systems (automated systems and communication networks of different levels and applications, telephone, fax and radio communication links, information transmission equipment, information reproduction and displaying equipment, auxiliary equipment and systems);
16. Security Guarding and protection equipment and systems of tangible and information resources;
17. intangible assets (image, business reputation, intellectual property, etc.);
    1. **Security Threat modelling**
       1. Modelling of Security Threats shall include:
18. analysis of Facilities, identification of critical assets to be protected, and their supporting infrastructure;
19. categorisation of Facilities;
20. analysis of Potential Threats to Facilities, their sources and ways of materialisation, classification of Threat materialisation possibilities;
21. creating an Offenders model, including categories of Offenders who may affect the Facility; goals that may be sought by each category of Offenders, scenarios of potential actions of Offenders;
22. vulnerability analysis of Facilities, including comparison of Potential Threats and available protection measures, evaluation of consequences of a materialised Threat;
23. Threat materialisation Risk assessment, including probability and scale of adverse consequences.
    * 1. The modelling results in establishing a list of current Threat sources, list of current vulnerabilities, interconnections between Threats, sources of Threats and vulnerabilities, list of potential attacks against the Facility, potential consequences of a materialised Threat. Based on the above, according to Clause 5.6 hereof, recommendations are developed to take measures to prevent Threats and minimise consequences of their materialisation.
    1. **Main sources, types and kinds of Threats to Physical Security and Counter-Terrorism Protection of the Company**
       1. Company Security Threats are classified as external and internal by sources of origin, and according to the Facility they are directed against.
       2. The main sources of Threats to Physical Security and Counter-Terrorism Protection of Company Facilities are:
24. criminal groups and individuals;
25. terrorist and extremist groups and individuals;
26. current and ex-employees of the Company, Lessees and Contractors.
    * 1. The main types of Threats to Physical Security and Counter-Terrorism Protection of the Company are:
27. harm to life or health of Employees;
28. theft of valuables and information;
29. destruction of and damage to property;
30. discontinuity of business processes;
31. Acts of Terrorism.
    * 1. The main kinds of Threats to Physical Security and Counter-Terrorism Protection of the Company are:
32. actions without a lucrative motivation that result in Damage to the Company or create preconditions for Damage or other Threats (unintentional damage to pipelines and other Facilities, acts of vandalism, trespassing at protected zones of oil and gas Facilities, etc.);
33. lucrative Unlawful Attacks to steal oil, petroleum products and other commodities (theft from trunk oil pipelines, interfield pipelines, at oil production Facilities, theft of oil production equipment and other equipment, dismantling spare parts, theft of gas from gas distribution pipelines), assaults on Facilities containing commodities (warehouses, supporting bases, etc.), etc.;
34. Damage resulting from interruption or shutdown of a production process, inter alia, as a result of different unauthorised campaigns (strikes, protests, etc.);
35. Unlawful attacks to inflict harm to information resources (illegal misappropriation, use of and sharing information, breaking integrity and availability of information, preventing operation of information systems, etc.);
36. terrorism threats, typical of which are:

* damage/destruction of critical facilities or equipment;
* interfering with power supply, process control and/or protection systems (including remote interventions);
* spreading toxic, radioactive substances and products, and other hazardous substances and materials, inter alia, through an explosion;
* theft of hazardous substances and materials for further use in an Act of Terrorism;
* theft of confidential or other restricted information that may facilitate an Act of Terrorism, if used;
* hostage-taking.
  1. **Categorisation of Facilities**
     1. Facilities that may become targets of Security Threats or UAA, including Unlawful Attacks and Acts of Terrorism, have different potential vulnerability to potential physical or non-physical Damage and are classified (categorised) according to vulnerability and level of Risk.
     2. Categorisation is made to divide Facilities in a systemic manner according to Security Threats to improve their Physical Security and Counter-Terrorism Protection.
     3. Unless otherwise established by the law of the Republic of Kazakhstan, Company Facilities are Categorised if the Facility:

1. is categorised as a strategic, hazardous production Facility; a socially and economically critical system for population;
2. includes, among other things, outdoor units (packages of outdoor units and process equipment, structures and facilities), premises and/or buildings which have been assigned fire and explosive hazard categories;
3. is classified as a FVTA.
   * 1. For the purposes hereof, the following Company Facilities are subject to mandatory Categorisation along with FVTAs:

| **Groups of gas production, transportation,**  **processing, storage and supply facilities** | | |
| --- | --- | --- |
| **critical** | **explosive** | **infrastructure** |
| 1. Industrial sites of gas production facilities:   * gas pre-treatment units; * integrated gas treatment units; * booster compressor stations.   2. Industrial sites of gas transportation facilities:   * compressor stations with connections; * gas distribution stations; * gas metering stations. | 1. Gas refineries with at least 10 employees.  2. Gas holders over 1 000 cubic meters.  3. Storages of explosive substances and materials.  4. Underground gas storages. | 1. Gas filling points and filling stations.  2. Tanks over 1 000 cubic meters.  3. Storages of liquefied gas containers with tanks over 500 cubic meters.  4. Regasification stations with tanks over 500 cubic meters.  5. Standalone methanol units and methanol warehouses with tanks over 500 cubic meters. |

|  |  |  |
| --- | --- | --- |
| **Groups of oil production,**  **transportation, processing and petroleum products supply facilities** | | |
| **critical** | **explosive** | **infrastructure** |
| 1. Main and intermediate oil pumping stations. 2. Oil loading stations. 3. Oil loading ports and terminals. 4. Oil and gas gathering, treatment and transportation points. 5. Oil and gas treatment units. 6. Separation units. 7. Supporting bases of fields. 8. Booster pump stations. 9. Compressor stations. 10. Gas turbine power plants. 11. Well clusters. | 1. Tank farms. 2. Oil and petroleum product warehouses over 2000 cubic meters. 3. Oil refineries with at least 10 employees. 4. Storages of explosive substances and materials. | 1. Oil refineries. |

* + 1. A Facility is categorised as a single Facility, if all buildings, constructions, structures and outdoor units in its territory are owned by the same person under the right of ownership (or on other legal grounds).

If a Facility site comprises buildings, construction, structures and outdoor units owned by different entities under the right of ownership (or on other legal grounds), they are categorised for each owner (legal owner).

* + 1. Inputs for categorisation of Facilities are:

1. classification of a Facility as a critical infrastructure and life support Facility of the Company, and availability of Hazardous Production Facilities at the Facility;
2. general information about the Facility;

* location of the Facility;
* total number of staff employed by the Facility, including personnel of lessees and contractors (including for different time of day, seasons);
* maximum number of people working at the Facility during the same day or night shift;
* duty of the Facility;
* availability of other operations, settlements, residential buildings and other places of mass gathering of people around the Facility, their description and location in relation to the Facility;
* location of the Facility in relation to transportation links;
* information about hazardous substances and materials used at the Facility;

1. potential conditions for onset or development of an Emergency with dangerous social and economic consequences;
2. magnitude of potential social and economic consequences of accidents at the Facility, including as a result of an Unlawful Attack, involving Act of Terrorism among other things;
3. Critical zones at the Facility and their description;
4. PHA at the Facility and their description;
5. Vulnerabilities of the Facility;
6. hazard categories previously assigned to the Facility;
7. types of Threats and Offender models for the Facility;
8. condition of the Physical Security and Security Guarding System of the Facility, previous offences, attempted intrusions at the Facility by unauthorised persons, Unauthorised Actions to damage or destroy elements of the production process;
9. layouts and plot plans of the Facility, utilities, layouts and lists of individual buildings and facilities, their parts, emergency containment and response plans of the Facility, design documentation for the Facility, Industrial Safety Declaration of the Facility, documentation for processes used by the Facility.
   * 1. The inputs are used to develop a Facility Security Certificate, FVTA Counter-Terrorism Security Certificate, security guarding handover certificates for the Facility.
     2. Company Facilities are categorised according to the criteria established based on parameters of an emergency zone that may result from an Unlawful Attack on Facilities, potential number of casualties and magnitude of physical Damage.
     3. Criteria for categorisation of Facilities are established using values defined by Classification of Man-made and Natural Emergencies approved by an authorised body.
     4. **Highest Hazard/Risk category (category A)** includes a Facility, an Unlawful Attack on which would result in an Emergency occurring in three or more regions of the Republic of Kazakhstan or covering adjacent states, that would be or may be accompanied by one of the following consequences:
10. death of more than 200 people;
11. disruption of living conditions of more than 1500 people;
12. physical Damage to health of people, environment and economic facilities of more than 200,000 monthly calculation indices.
    * 1. **High Hazard/Risk category (category B)** includes a Facility, an Unlawful Attack on which would result in an Emergency occurring in at least three districts of the same region or in two regions of the Republic of Kazakhstan, that would be or may be accompanied by one of the following consequences:
13. death of over 50 but not more than 200 people;
14. disruption of living conditions of more than 500 but not more than 1500 people;
15. physical Damage to health of people, environment and economic facilities from 100,000 to 200,000 monthly calculation indices.
    * 1. **Medium Hazard/Risk category (category C)** includes a Facility, an Unlawful Attack on which would result in an Emergency beyond the site of a production or social Facility, and not beyond two districts of a region.
16. death of over 10 but not more than 50 people;
17. disruption of living conditions of more than 100 but not more than 500 people;
18. physical Damage to health of people, environment and economic facilities from 15,000 to 100,000 monthly calculation indices.
    * 1. **Low Hazard/Risk category (category D)** includes a Facility, an Unlawful Attack on which would result in an Emergency within the site of a Facility that would be or may be accompanied by one of the following consequences:
         1. death of over 5 but not more than 10 people;
         2. disruption of living conditions of more than 50 but not more than 100 people;
         3. physical Damage to health of people, environment and economic facilities from 5,000 to 15,000 monthly calculation indices.
      2. Conditions of onset and development of Emergencies caused by an Unlawful Attack, including an Act of Terrorism at the Facility, are considered in the pessimistic, worst-case scenario, where consequences of an accident/incident match or exceed the consequences designed for the Facility.
      3. FVTAs are categorised according to FVTA classification criteria approved by an authorised body.
      4. According to the main sources, types and kinds of Security Threats listed in section 7 hereof, Company Facilities are subdivided into three main categories:
    1. High-risk facilities – **category I**;
    2. Medium-risk facilities – **category II**;
    3. Low-risk facilities – **category III**;
       1. **High-risk facilities (Category I)** include trunk pipelines and associated facilities, field facilities, oil and gas refineries, oil depots, storages of explosive and highly potent, toxic substances, offshore operations support vessels.
       2. **Medium-risk facilities (Category II)** include procurement bases, vehicle filling stations, vehicle gas filling stations, vehicle gas filling compressor stations, gas filling stations, gas filling points, dispatcher points.
       3. **Low-risk facilities (Category III)** include office and administrative buildings, dormitories, rotation camps, communication facilities, water supply, power supply, economic, social and cultural facilities, other facilities not associated with storage of chemical explosives, toxic substances, and fuels and lubricants.
       4. Regardless of the Hazard/Risk level, each Facility may include High Security Facilities.
       5. Basic requirements for Engineering Fortification and SES, Access Control and Site Security Arrangements are established based on the Hazard/Risk Category of the Facility (A, B, C, D) and category of the Facility by main sources, types and kinds of Security Threats.
       6. Basic requirements for Physical Security and Counter-Terrorism Protection of Company FVTAs are established according to the counter-terrorism law of the Republic of Kazakhstan, specifics and features of activities.
       7. Requirements for security companies and other companies involved to provide Physical Security and Counter-Terrorism Protection of categorised Facilities, including FVTAs, are stipulated in service/work contracts entered into with such companies.

***Categorisation of Facilities***

* + 1. For Categorisation of a Facility, resolution of KMG and SDE management establishes a Facility Categorisation Commission (the Commission), which includes:

1. supervising managers of KMG and SDE, the Facility;
2. representatives/Employees of the Facility Security Unit in charge of SES and information security;
3. Facility Employees specialising in the main process equipment, industrial and fire safety, control and recording of hazardous substances and materials.
4. representatives/Employees of civil defence unit of the Facility;
5. representatives of the security company, other companies involved to provide Physical Security and Counter-Terrorism Protection of the Facility (as approved).
   * 1. The Commission is chaired by a supervising manager of KMG and SDE.
     2. Facility information is analysed based on Facility inputs, interviewing employees and Facility inspections.
     3. The Commission identifies:
6. potentially hazardous areas of the Facility;
7. critical zones and vulnerabilities of the Facility that, if protected, may prevent an Unlawful Attack on the Facility;
8. potential escape routes and hiding places of Offenders.
   * 1. Critical zones of the Facility are identified from among potentially hazardous areas (PHA) of the Facility. The Commission compares Critical Zones of the Facility and identifies zones, an Unlawful Attack on which may result in an Emergency.
     2. Identification of Critical Zones of the Facility includes:
9. listing PHA of the Facility;
10. identifying and listing Critical Zones of the Facility from among PHA of the Facility;
11. establishing the Threat of UAA and potential ways of implementation towards each Critical Zone of the Facility;
12. establishing a model of Offender for each Critical Zone of the Facility;
13. UAA vulnerability assessment for each Critical Zone of the Facility.
    * 1. Social and economic consequences of UAA are evaluated for each Critical Zone of the Facility and the Facility in general.
      2. Based on the work results, the Commission assigns Hazard Categories to the studied Facility according to degree of potential hazard followed by issue of a certificate.
      3. Potential hazard categories of Facilities are established as follows:
    * Arrange work to establish category of the Facility;

* Collect and analyse Facility inputs;
* Study production processes and identify Potentially Hazardous Areas of the Facility;
* Inspect the Facility and identify Critical Zones/elements;
* Evaluate social and economic consequences of an Unauthorised Attack / Act of Terrorism against its critical elements;
* Assign a category to the Facility.
  + 1. The following documents are issued for each categorised Facility:

1. Facility security certificate;
2. Guidelines (procedure, instructions) for interaction with national security, internal affairs, emergency bodies in case of an Emergency at the Facility;
3. Guidelines/instructions for Access Control and Site Security Arrangements;
4. Industrial Safety Declaration for a Hazardous Production Facility – if the Facility has been classified as a Hazardous Production Facility;
5. Counter-Terrorism Security Certificate (if classified as a FVTA). If the Facility has a Counter-Terrorism Security Certificate, no Facility Security Certificate is required.

***Identification of Potentially Hazardous Areas of the Facility***

* + 1. The Commission evaluates the degree of potential hazard of each PHA of the Facility to identify the most attractive areas for UAA, Unlawful Attack, including an Act of Terrorism.

A criterion of potential hazard is potential number of casualties as a result of materialisation of a Security Threat and Emergency with certain social and economic consequences.

* + 1. To identify all PHA, production cycle (operation regulations) of the Facility is analysed in full, and basic Threats and expected consequences of materialisation are identified for each PHA.
    2. The identified PHAs are included in the list with:

1. sequential number of PHA;
2. description of the process;
3. description of PHA marked at the facility layout;
4. number of employees at the PHA according to the organisational chart;
5. name and brief description of PHA, structures, equipment elements, etc.
6. nature and brief description of a potential accident, which may occur at a certain production area, and whether or not it can develop into a natural or man-made Emergency.

***Establishing Critical Zones/elements of the Facility***

* + 1. From among all the PHAs of the Facility, the Commission identifies Critical Zones, including zones attractive for terrorists, and vulnerabilities of the Facility. Several close Critical Zones may be seen by the Commission as a single Critical Zone.
    2. After comparison of the identified Critical Zones according to their mutual influence, the Commission identifies zones that may become a source of Emergency or Damage after UAA.
    3. The identified Critical Zones of the Facility are included in the list with:

1. sequential number of a Critical Zone;
2. name of the Critical Zone based on PHA name;
3. basic Threats (brief description of the most dangerous accident);
4. Offender type (the most probable Offender model);
5. estimated time needed for an Offender to commit UAA;
6. effect on situation in other Critical Zones of the Facility (Critical Zones (numbers), where an associated accident may occur).
   * 1. Critical Zones of the Facility may include:
7. zones, structural and process elements of the Facility, buildings, utilities, communications;
8. elements of systems, assemblies of equipment or devices of a potentially hazardous unit;
9. locations where hazardous substances and materials are used or stored;
10. other systems, elements and utilities of the Facility identified as requiring Physical Protection during vulnerability analysis.

***Identifying Threats to the Facility***

* + 1. To identify Threats to the Facility, the Commission identifies potential Offenders, predicts their capabilities, intentions and tactics.
    2. Threats to each Critical Zone (a group of zones/elements) are identified by studying all possible accident scenarios resulting from UAAs by Offenders, and identifying a basic Threat that may be carried out against this Critical Zone.
    3. Threats and their probable ways of execution are defined by the UAA nature and a model of an Offender who has committed or is attempting to commit UAA against the Facility, and his/her accomplices. For this, the Commission:

1. studies different types of Threats applicable to the Facility;
2. defines the most probable Threats to this Facility type;
3. evaluates probability of materialisation of the most probable Threats;
4. considers factors affecting the Threat materialisation probability;
5. checks legitimacy of the sources of information about Threats and how credible they are.

***Offender Model***

* + 1. An Offender Model (a combination of qualitative and quantitative characteristics of an Offender, his/her motivations and goals) is used to establish the required level of protection for the Facility and its Critical Zones, elaborate requirements for the Physical Security and Counter-Terrorism Protection System of the Facility and evaluate its effectiveness.
    2. The generalised Offender Model for different types of Company Facilities is established by the Commission according to the following **basic Offender Model options**:

1. an Individual Offender (IO), including an Internal Offender (1 person);
2. a Group Offender (GO) (2 or more people);
3. a Terrorist Group (TG) (5 or more people).
   * 1. An Offender Model is classified based on the following criteria:
   1. Offenders who may affect the Facility are subdivided into Internal Offenders (persons from among Facility employees and other people who have been allowed to the territory as established) and External Offenders (persons who are not employees/visitors of the Facility and have no right to access it).

An Internal Threat is established by evaluating the Facility Personnel according to the level of their access to Vulnerabilities and Security Systems of the Facility, nature of work, social and psychological factors;

* 1. goals that might be sought by each Offender type, motives behind their actions, possible number;
  2. vehicles, equipment, weapons, tools, accessories and other things they use;
  3. awareness about technological features, vulnerabilities, Physical Security and Counter-Terrorism Protection System of the Facility;
  4. technical qualifications and preparedness to commit UAA, including an Act of Terrorism at the Facility;
  5. potential tactics and scenarios of Offenders’ actions, characterising the sequence/algorithm and modus operandi of Group Offenders and Individual Offenders at each stage of UAA or Unlawful Attack, including Act of Terrorism, at the Facility, movement routes.
     1. The main Offender categories include:

1. Facility Employees forced to assist external offenders by being bribed, blackmailed or threatened with violence;
2. disgruntled Facility Personnel;
3. criminals;
4. terrorist and extremist groups.
   * 1. The basic motives of potential Offenders for UAA against the Facility include:
5. political/ideological;
6. economic (material gain);
7. personal (related to specific circumstances of a certain individual, may be caused by relationships among colleagues, social, and other reasons).
   * 1. The basic means used by External Offenders to intrude into Guarded Zones may include:
8. weapons – to break through Gate Houses and counteract Security Guarding Forces;
9. explosives and incendiaries – to overcome physical barriers and commit Act of Terrorism;
10. special equipment, devices, tools, other equipment and gear; vehicles (aircrafts, including unmanned air vehicles, cars, floating vessels, etc.);
11. financial resources – to bribe internal Offenders.
    * 1. An Offender Model is established by evaluating the potential tactics to intrude into Guarded Zones:
12. forced – using violence against people and/or damaging SES;
13. deceptive – attempting to make their actions look legal by using fake documents, gate passes, keys, personal ID, etc.;
14. concealed – trying to remain unnoticed;
15. combined – combinations of different tactics.
    * 1. For the purposes hereof, an Offender Model includes **six basic potential Offender types** and may be expanded based on features, location and operation of a specific Facility.

|  |  |  |
| --- | --- | --- |
| **Offender type** | **Main characteristics** | **Probable tactics** |
| **1. External Offender Type 1**  (a terrorist group (5 or more people), the goal is to commit an act of terrorism) | 1. generally aware about the Physical Security and Counter-Terrorism Protection System of the Facility based on visual exploration of the Facility, about location of the attack targets in the territory; 2. highly likely to have cold arms and fire arms (including automatic weapons), explosives and incendiaries, explosive devices, etc. 3. highly prepared to overcome physical barriers, defence lines and alarms; 4. ready to take an open armed conflict with Site Security Unit (SSU); 5. can divide into subgroups to address different tactical objectives; 6. may include persons who can sacrifice themselves to achieve their goals. | Forced entry with armed attacks and breaking through Security Guarding Systems (including using vehicles), using diversion tactics, taking hostages (as required).  The Offender may conspire with Facility Personnel, SSU to gather additional information. |
| 1. **External Offender Type 2**   (a Group Offender (2 or more people) from among persons who do not have an authorised access to the Facility), the goal is to commit an Act of Terrorism) | 1. moderately aware about composition and structure of the Physical Security and Counter-Terrorism Protection System of the Facility, about location of the attack targets in the territory; 2. highly likely to have cold arms and fire arms; 3. may have explosives; 4. may be using hand tools or special tools; 5. highly likely to use vehicles; 6. highly prepared to overcome physical barriers. | Concealed entry to the Facility, Guarded Zones and objects located there.  The Offender may conspire with a SSU employee to conceal his/her intrusion into the Facility. Certain Offenders may have both material gain and ideological reasons as their motives. |
| 1. **External Offender Type 3**   (Individual Offender from among persons who do not have an authorised access to the Facility), the goal is to commit an Act of Terrorism) | 1. hardly aware about structure and composition of the Physical Security and Counter-Terrorism Protection System of the Facility, about location of the attack targets in the territory, but may be using a scenario; 2. highly likely to have fire arms, explosive devices to commit an Act of Terrorism; 3. unlikely to use vehicles; 4. highly prepared to overcome physical barriers; 5. may be ready to sacrifice himself/herself to achieve the goals. | Concealed or deceptive entry to the Facility. |
| 1. **External Offender Type 4**   (Individual Offender from among persons who do not have an authorised access to the Facility), the goal is to steal material valuables | 1. hardly aware about the Physical Security and Counter-Terrorism Protection System of the Facility, about locations of material valuables at the Facility; 2. unlikely to have fire arms; 3. may only be using hand tools; 4. unlikely to use vehicles; 5. hardly prepared to overcome physical barriers. | Concealed entry to the Facility and stealing valuables.  The Offender does not have enough information about production processes of the Facility.  The motive is theft for material gain.  An attempted theft may damage critical equipment. |
| 1. **Internal Offender Type 1**   (an employee/specialist of the Facility who has authorised access to the territory)  The main goal is to steal for material gain, but an Act of Terrorism possibility cannot be excluded. | 1. highly aware about composition and structure of the Physical Security and Counter-Terrorism Protection System of the Facility and locations of Guard posts; 2. highly aware about locations of the targets of theft or sabotage at the Facility; 3. hardly likely to have firearms, explosives or explosive devices; 4. may be using hand tools or special tools; 5. unlikely to use vehicles; 6. prepared enough to overcome physical barriers. | Legally enters the Facility during working hours using his/her gate pass.  The Offender may be a source of information about a potentially hazardous Facility for an External Offender Type 1 or 2, conspire with External and Internal Offenders to participate in joint Acts of Terrorism. |
| 1. **Internal Offender Type 2**   (SSU employee) | 1. highly aware about composition and structure of the Physical Security and Counter-Terrorism Protection System of the Facility, locations of Guard Posts; 2. hardly aware about the production process; 3. highly aware about locations of the targets of Security Objects at the Facility; 4. has weapons and special devices (depending on the regular gear of security forces at a specific Facility); 5. may freely enter a Guarded Zone; 6. hardly prepared to overcome physical barriers. | Open access to the targets of theft during working hours using his/her official authority.  Offender: is aware about working hours of the Facility, locations of possible material and other valuables; may select the best moment for an Act of Terrorism; may conspire with External Offenders |

* + 1. An Offender Model is established by analysing goals and objectives of a Potential Offender and Facility Category. An Offender Model for a specific Facility includes as much information as possible about potential actions of Offenders according to the established Threats to the Facility, is updated during collection of inputs or revised according to the specific Facility features.

***Evaluating social and economic consequences*** ***of an Unlawful Attack on the Facility, including an Act of Terrorism***

* + 1. Social and economic consequences of an Unlawful Attack on the Facility, including an Act of Terrorism, are predicted (as applicable) based on Facility’s Industrial Safety Declaration.
    2. For a potentially Hazardous Production Facility, the basic social and economic consequences of an Unlawful Attack on the Facility, including an Act of Terrorism, are the potential number of casualties (people) and Economic Damage (thousand MCI). For a Facility that is not classified as potentially hazardous, the main indicator is the Economic Damage.
    3. The number of casualties at a Potentially Hazardous Production Facility means permanent losses (fatalities) and medical losses (injured people), including employees of the Facility, Site Security and population within the affected area.
    4. The Economic Damage, which may be incurred by a Security Subject (a group of subjects) as a result of an Unlawful Attack, including an Act of Terrorism, in this Regulations means the loss by a Security Subject of a part or all of its valuables, and the Damage includes own and third-party Economic Damage.
    5. The Own Economic damage is estimated by the sum of:

1. the magnitude of Damage (in absolute units) to plant and equipment of the Facility in general, including buildings/constructions and equipment;
2. lost profit from shortage of released products and cost of the lost finished products;
3. cost of the lost material resources and production reserves;
4. cost of compensations and payments for Personnel during outage of the Facility or its individual units or parts;
5. cost of the lost intangible assets, including scientific, technical and other documentation (as applicable);
6. losses associated with changes to the quality of products;
7. costs for response to an Emergency and its consequences at the Facility;
8. estimated cost of the Damage to environment;
9. cost of activities to eliminate Emergency consequences and restore the environment.
   * 1. The Own Economic Damage is established based on the following basic documents and inputs:
10. plot plan of the Facility, layouts of production sites, general process flow diagram;
11. production capacities of the Facility;
12. list and quantities of the main elements (plant and equipment) of the Facility, including potentially hazardous buildings, workshops, constructions, storages, tanks, etc.;
13. distances between them;
14. the initial book value of the entire Facility and each of its elements;
15. physical stability of Facility elements against a shock wave;
16. fire hazard of Facility elements (workshops, buildings, constructions, storages, tanks etc.) (production category);
17. thermal and physical properties of combustible materials in different elements of the Facility;
18. fields of affecting factors for different explosives;
19. fields of affecting factors of fires from combustion of different materials and oil and gas products;
20. figures of failure of main elements of the Facility (plant and equipment) at different degrees of damage;
21. efforts to restore elements of the Facility at different degrees of damage (if there is no data about efforts, use an industry average production per day of a single worker involved in construction, installation and repair of the main equipment);
22. time to restore the Facility according to scopes of construction and installation and other work;
23. number of personnel (responders) involved in recovery work;
24. efforts and time required to eliminate consequences of an Unlawful Attack, including an Act of Terrorism, Emergency, and to restore the environment;
25. costs to recover health, pay financial and other compensations for people affected as a result of an Unlawful Attack, including an Act of Terrorism, and Emergency.
    * 1. The Third-Party Economic Damage is estimated tentatively based on costs, losses and damage associated with forced (caused by an accident at the Facility) action/inaction of third-party companies involved in production and cooperation. The main components of the Third-Party Economic Damage for a Facility are:
26. Own Economic Damage incurred by downstream companies in the Supplier-Consumer chain;
27. Own social and welfare Economic Damage for town-forming companies of administrative units.
    1. **Evaluating adequacy of activities to ensure Physical Security and Counter-Terrorism Protection of the Facility**
       1. Adequacy of Facilities protection is reviewed and evaluated by the Commission to establish whether the Physical Security and Counter-Terrorism Protection System of the Facility is capable of counteracting the established Threats and Offender actions for this Facility type. Results of the evaluations are used to build or improve the Physical Security and Counter-Terrorism Protection System of the Facility.
       2. The main goal of the evaluation is to provide objective information about status of the Facility Security Guarding and Physical Protection of its Critical Zones for people who make decisions regarding Security of the Facility.
       3. Adequacy of activities to ensure Physical Security and Counter-Terrorism Protection of the Facility is evaluated in the following descending order:
28. make arrangements to evaluate the adequacy;
29. collect and analyse inputs about Physical Security and Security Guarding of the Facility;
30. establish the required level of protection for the Facility;
31. evaluate condition of Physical Protection and Security Guarding of the Facility;
32. build/improve the Physical Security and Counter-Terrorism Protection System of the Facility.
    * 1. Adequacy of activities to protect the Facility is evaluated based on:
33. identifying and establishing all Critical Zones of the Facility, Threats to them and the most probable ways of execution;
34. establishing the required level of protection for the Facility and its Critical Zones;
35. evaluation of the level of protection of the Facility and Critical Zones against the requirements.
    * 1. The adequacy of protection is established for each Critical Zone and for other zones of the Facility. The general security of the Facility is defined by security of its Critical Zones and other elements that define how important it is (high security arrangements, category, etc.).
      2. For evaluation, the Commission gathers information about Physical Protection and Security Guarding activities at the Facility based on:
36. categorisation of the Facility;
37. studying the available documents about Physical Protection and Security Guarding of the Facility;
38. interviews with Facility employees;
39. analysing condition of Facility Security Guarding and protection of its Critical Zones;
40. inspection of the Facility.
    * 1. The Commission studies the following basic documents:
41. plot plans/layouts of the Facility showing locations of storages of hazardous substances and materials, arrangement of process equipment, construction drawings of buildings, etc.;
42. Facility Security Guarding plan showing locations of Guard Posts, SES equipment;
43. potential hazard category of the Facility;
44. results of inspections of the Facility, Physical Security and Counter-Terrorism Protection System of the Facility, and Security Guarding;
45. documents governing Access Control and Site Security Arrangements, other documents in Security Guarding and protection of the Facility;
46. information about interactions with law enforcement and special bodies, civil defence units, other state authorities;
47. information about fire safety of the Facility.
    * 1. The adequacy of Facility protection is evaluated based on the results of Categorisation and includes:
48. the list of Critical Zones of the Facility identified during vulnerability assessment of the Facility’s Physical Security and Counter-Terrorism Protection System;
49. the established protection level requirements for Critical Zones;
50. results of Critical Zones protection evaluation;
51. evaluation of the Physical Security and Counter-Terrorism Protection System of the Facility at the beginning of work;
52. recommendations to build/improve the Physical Security and Counter-Terrorism Protection System of the Facility;
    * 1. Following the work, the Commission prepares conclusions about condition of the Physical Security and Counter-Terrorism Protection System of the Facility and recommendations on how to improve it, including activities to achieve the required level of protection of the Facility and its Critical Zones.

***Establishing the required level of protection for the Facility***

* + 1. The required protection level of the Facility is defined by:

1. maximised Damage from unauthorised actions against Critical Zones;
2. efficiency of Security Guarding and Physical Protection activities for Critical Zones.
   * 1. The efficiency of Security Guarding and Physical Protection activities for the Facility are defined according to potential hazard category, vulnerability assessment of Critical Zones, the established Threats and Offender Models, regulatory requirements for Physical Protection and Security Guarding of the Facility (strategic, hazardous production facilities, FVTA, etc.)
     2. Physical Protection and Security Guarding activities of the Facility govern actions of Personnel of Facility’s Physical Security and Counter-Terrorism Protection System, and Security Guarding activities using SES.
     3. Objectives of the Physical Security and Counter-Terrorism Protection System of the Facility include organisational and technical activities for Physical Protection and Security Guarding of the Facility in general.
     4. The goal of the Physical Security and Counter-Terrorism Protection System of the Facility is to prevent UAA against Critical Zones of the Facility so that an Offender is timely detected and his/her movement towards the place of UAA is stopped; capabilities and preparedness of SSU or other response forces.
     5. Depending on category of the Facility, Security Guarding at the Facility, features of the Facility and Critical Zones, Threats and Offender Models, measures taken to ensure process safety and other safety types, the goal of the Physical Security and Counter-Terrorism Protection System of the Facility is achieved by the following objectives:
3. prevent UAAs against Critical Zones of the Facility;
4. timely detect UAAs;
5. ensure quick response of SSU forces to UAAs following alarms, apprehend/slowing movement of an Offender;
6. prevent UAAs by neutralising Offenders outside of the scene by blocking the Critical Zone before it begins;
7. prevent UAAs by neutralising the Offender in the process of execution before unacceptable consequences for the Facility emerge.
   * 1. The scope and composition of Physical Protection activities for Critical Zones of the Facility, efficiency of implementation are differentiated according to the potential hazard and attractiveness of a Critical Element for Offenders, the established Offender models and acceptable ways to prevent UAAs.
     2. Critical Zones are assigned protection levels by implementing Physical Protection tasks in the most efficient manner, primarily for Critical Zones that are the most potentially hazardous and attractive for UAAs.
     3. The protection level requirements for Critical Zones of the Facility are established as follows:
8. establish the potential hazard and importance of each Critical Zone;
9. define an Offender Model for each Critical Zone;
10. specify the level of protection of each Critical Zone according to attractiveness and other features.
    * 1. The degree of potential hazard and importance of Critical Zones of the Facility are established according to:
11. social and economic consequences (expected number of casualties and material Damage as a result of UAA);
12. secrecy mode of a building, room the Critical Zone is located in;
13. explosive and fire hazard category and chemical hazard category of a building, room the critical zone is located in.
    * 1. The Commission establishes a Critical Zone category according to the highest indicator and may increase it by one required indicator if values of two indicators match.
      2. The protection level requirements are established by considering an Offender Model for highly potentially hazardous Facilities according to the results of Facility vulnerability assessment and classifying it as one of the basic options (terrorist group (TG), group offender (GO), individual offender (IO)).

Offender Model for Facilities categorised as medium potential hazard is IO or GO (when substantiated), and is not assigned to low category facilities, or IO is used as such.

* + 1. The protection level requirements for Critical Zones according to potential hazard and importance, and the assigned Offender Models are defined by:

|  |  |  |  |
| --- | --- | --- | --- |
| Potential  Hazard of a Critical Zone | Offender  Model | Attractiveness of a Critical Zone/element for UAA | Protection level required |
| High | TG | attractive | I |
| High | TG, GO | attractive | II |
| High | TG, GO, IO | attractive | III |
| Medium | GO, IO | not attractive | IV |
| Low | IO | not attractive | V |

* + 1. Critical zones are classified as attractive or unattractive for UAA based on Threat vulnerability assessment of the Facility, ways of Threat execution applicable to potential offender models according to:

1. accessibility of a Critical Zone for UAA related to Facility operation conditions, access of personnel and other people, location and other features of the Facility;
2. vulnerability of structures and systems that ensure safety of the Critical Zone, how hard it is to commit UAA, how much time is required to commit it after the Critical Zone is reached.
3. acceptability of the Risk of UAA due to consequences for the Offender;
4. economic, environmental, psychological and other consequences of UAA.
   * 1. The security of a Critical Zone is determined through UAA prevention procedures, the minimum number of protection boundaries to detect and/or apprehend Offenders, recommendations for access to the Critical Zone, Security Guarding including armed security, and SES.
     2. The following Physical Protection activities are implemented for critical zones with different protection levels according to the protection level requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Protection  level required | Prevention  **UAA** | Number of protective  boundaries | Requirements for  access to the Critical Zone | Armed security/surveillance at the Facility |
| I | before UAA | at least three | restricted and controlled access | Security guard |
| II | before or during UAA | three | the rule of two (three) persons | Security guard |
| III | before or during UAA | at least two | restricted and controlled access | Security guard and surveillance |
| IV | during UAA | two | restricted access | surveillance |
| V | interception | one | restricted where possible | periodic surveillance |

* + 1. To prevent UAA, the basic Physical Protection activities of the Facility include measures to prolong the time required for an Offender (intrusion time) to overcome physical barriers by increasing their number or reinforcing them, and which includes the time required for the main Guard Forces, law enforcement and special bodies to arrive.
    2. The Facility is considered protected if:

1. basic protection activities are provided for all Critical Zones according to the established protection levels;
2. UAAs in Critical Zones classified as Protection Levels I-IV are prevented by SSU:

* UAAs in critical elements classified as Protection Level I are prevented by blocking the Critical Zone before the UAA;
* UAAs in *critical elements classified as Protection Level II* are prevented by blocking the Critical Zone before the UAA, or by intercepting Offenders before/during the UAA;
* UAAs in critical elements classified as Protection Level III-V are prevented by intercepting Offenders before/during the UAA.

***Evaluating Facility protection***

* + 1. Protection of the Facility is evaluated based on:

1. requirements for Facility Security Guarding and protection of Critical Zones established by the Commission for the Facility, according to the type and category;
2. fulfilment of Physical Protection objectives for Critical Zones of the Facility;
3. efficiency and adequacy of the Physical Security and Counter-Terrorism Protection System of the Facility.
   * 1. Evaluation of the fulfilment of Facility Security Guarding and Critical Zone protection requirements includes:
4. checking fulfilment of the established organisational activities to ensure Physical Protection and Security Guarding of the Facility against Threats, including Acts of Terrorism;
5. checking preparedness of management and personnel involved in Physical Protection and Security Guarding of the Facility;
6. checking equipment, technical condition and efficiency of SES package.
   * 1. Checking the fulfilment of the established organisational activities to ensure Physical Protection and Security Guarding of the Facility against Threats, including Acts of Terrorism, includes:
7. checking for compliance with the requirements for prevention of Unauthorised Actions against Critical Zones of the Facility;
8. checking fulfilment of the requirements for Security Guarding according to type and category of the Facility;
9. checking availability, efficiency and quality of managerial documents of the Facility in Physical Protection and Security Guarding;
10. checking Access Control and Site Security Arrangements;
11. checking access of personnel to Critical Zones of the Facility and restricted information;
12. checking activities to protect information about organisational and technical measures of Physical Protection and Security Guarding of the Facility and other information that can be used to commit UAA;
13. checking efficiency and quality of other activities to arrange for Physical Protection and Security Guarding established in the Company.
    * 1. Preparedness of management and personnel involved in Physical Protection and Security Guarding of the Facility is evaluated based on:
14. checking knowledge of officials who manage the Physical Security and Counter-Terrorism Protection System (corporate security) of legal regulations in Physical Security, Counter-Terrorism Protection and Security Guarding of Facilities;
15. checking knowledge of Site Security Unit (SSU) employees of documentation related to their functional duties, establishing the level of their professional training;
16. checking practical skills of management employees of the Physical Security and Counter-Terrorism Protection System of the Facility, Site Security Unit for actions in different situations;
17. checking equipment of SSU (weapons, special devices, main and redundant communication devices, vehicles and other material assets), interactions between units, staffing and other matters.
    * 1. Condition and efficiency of the SES package is checked by evaluating:
18. fulfilment of the requirements for provision of SES at Secured Zones of the Facility;
19. technical condition and correct operation of SES;
20. fulfilment of operational documentation requirements for installation, mounting, maintenance and repair of SES;
21. reliability of boundaries and interference resistance of SES.
    * 1. Following the checks, the Commission’s adequacy evaluation report includes the identified deviations from requirements of regulations and internal documents, other flaws in Physical Protection and Security Guarding of the Facility, measures and deadlines to eliminate them.
      2. The Commission evaluates condition of the Physical Security and Counter-Terrorism Protection System of the Facility, develops additional organisational and technical activities as necessary to improve it for each Critical Zone of the Facility, including protection boundaries, access control arrangements, Security Guarding and surveillance measures that are then included in the Security Certificate and/or Facility’s ATP Certificate.
      3. Facility protection level is evaluated based on efficiency check of the Physical Security and Counter-Terrorism Protection System of the Facility for Critical Zones by analysing response times of the Site Security Unit (SSU) to intercept UAA by an Offender in the following basic scenarios:

* blocking a Critical Zone/element before the UAA;
* intercepting the Offender before/during preparation for the UAA.
  + 1. The analysis compares the total time required for the Offender to get to the target and commit the UAA (**t**o) and the time required for SSU responding to SES signals (**t**ssu).

The UAA is considered intercepted if (**t**ssu) is admittedly less than (**t**o), and not intercepted if (**t**ssu) is more than (**t**o), or if these time intervals are relatively the same.

* + 1. Basic scenario checks are conducted for each Critical Zone against basic Threats and Offender Models for such zones/elements as established in the vulnerability assessment and according to the established Offender Model.
    2. In the basic scenario of blocking the Critical Zone before the UAA, the UAA is considered intercepted if SSU manages to block the Critical Zone in advance, after Facility Perimeter SES actuates. In this case, the time starts when an alarm on intrusion to the Facility is actuated.

The total SSU response time is calculated as follows:

**(tssu) =** **(tgather) + (tmove) + (tblock)**, where:

*(****t****ssu) is the total SSU response time;*

*(****t****gather)is the time required to gather and arm SSU;*

*(****t****move) is the time required for SSU to get from the SSU room to the Critical Zone;*

*(****t****block) is the time required for SSU to block the Critical Zone.*

Offender’s operation time is calculated as follows:

**(to) = (tovercome) + (tmove) + (tuaa)**, where:

*(****t****o) is the Offender’s total operation time;*

*(****t****overcome) is the time required to overcome the Perimeter (after actuation of SSE);*

*(****t****move) is the time required for the Offender to get to the Critical Zone;*

*(****t****uaa) is the time required to prepare for the UAA.*

* + 1. In the basic scenario of blocking the Critical Zone before the UAA, the UAA is considered intercepted if SSU responds to the signal of the target indicating SES (e.g. at the Guarded Zone perimeter). In this case, the time starts when an alarm is actuated at the Guarded Zone perimeter.

In this case, the total SSU response time is calculated as follows:

**(tssu) = (tgather) + (tmove)**, where:

*(****t****ssu) is the total SSU response time;*

*(****t****gather)is the time required to gather and arm SSU;*

*(****t****move) is the time required for SSU to get from the SSU room to the Critical Zone.*

Offender’s operation time is calculated as follows:

**(to) = (tintrude) + (tuua)**, where:

*(****t****o) is the Offender’s total operation time;*

*(****t****intrude) is the time required to intrude to the site of UAA;*

*(****t****uaa) is the time required to prepare for the UAA.*

* + 1. Components of the formulas in 10.38. and 10.39. of the Regulations are established according to:
* the time to gather and arm SSU (***t****gather*) – based on the established standards for SSU;
* the time to move (***t****move*), overcome physical barriers (***t****overcome*) – analytically, based on standard movement velocities of SSU and the distance from the SSU room to the Critical Zone, or in the course of drills/trainings based on the actual time required for SSU to move to a specific Critical Zone after several attempts;
* time required to prepare and commit the UAA (***t****uaa*) – during identification of Critical Zones of the Facility.
  + 1. The time is analysed in the following order:
* Determine the most probable routes of the Offender to the target based on the established Offender Model (study Facility plot plan, layouts of buildings, constructions, etc.);
* Evaluate SSU and Offender response times using formulas from 5.6.38. and 5.6.39. of the Regulations;
* Compare SSU time (**t**ssu) with Offender time (**t**o), make conclusion about adequacy of Physical Protection of the Critical Zone.
  + 1. Results of the efficiency check are included as a table in the Facility Security Certificate and are considered in development of the ATP Certificate. The obtained data is used to make a conclusion about achievement of the UAA interception objective:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Critical Zone** | **UAA prevention method** | **Offender Model** | **Estimated security unit response time**  **(tssu), min** | **Estimated Offender operation time (to), min** | **Conclusion on**  **UAA interception objectives** |
|  |  |  |  |  |  |  |

* + 1. Results of the Critical Zones protection adequacy check are included as a table in the Facility Security Certificate and are considered in development of the ATP Certificate. The obtained data is used to make a conclusion about adequacy or inadequacy of Critical Zone Protection activities and additional measures:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Critical Zone** | **Fulfilment of the established**  **requirements** | **Achievement of the Physical Protection objective** | **Achievement**  **of**  **UAA prevention objectives** | **Conclusion on adequacy**  **of protection**  **activities** | **Addi­tional measures** |
|  |  |  |  |  |  |  |

***Building (improving) the Physical Security and Counter-Terrorism Protection System of the Facility***

* + 1. Following evaluation of the adequacy of Facility protection, the Commission issues generally recommended organisational and technical activities to build/improve the Physical Security and Counter-Terrorism Protection System of the Facility to ensure Physical Protection of Critical Zones according to the established protection levels.
    2. Measures to build/create the Physical Security and Counter-Terrorism Protection System of the Facility are implemented taking into account the existing limitations of financial, human, time and other resources. The first to be implemented are the measures that maximise performance of the Physical Security and Counter-Terrorism Protection System of the Facility for the highest-ranked Critical Zones using the least amount of resources.
    3. Building principles of the Physical Security and Counter-Terrorism Protection System:
* **correspondence with the established Threat models** (established organisational and administrative measures, technical methods of protection of the Facilities and their elements correspond with the established Threats and Offender Models);
* **zoned structure** (providing and building Restricted Access and Secured Zones to ensure staged protection of the Guarded Facilities and Critical Zones)[[1]](#footnote-1);
* **strength balance** (ensuring the required performance of the Physical Security and Counter-Terrorism Protection System of the Facility for all Offender types and UAA methods identified by the vulnerability assessment);
* **adaptivity** (operation of the Facility and adapting the Physical Security and Counter-Terrorism Protection System to process features according to the process and fire safety measures at the Facility, including those in case of an emergency.)
  + 1. The Physical Security and Counter-Terrorism Protection System of the Facility is built as functionally complete components capable of assigning appropriate requirements for them in internal documents of the Company.

**Physical Security and Counter-Terrorism Protection System of the Facility**

**Weapons**

**Package**

**SES**

**Organisational activities**

Special devices

Weapons

Engineering means (physical barriers)

A group of measures by management of SDE (SDE CSU) and SSU

Management and personnel of SDE (SDE CSU)

Communication devices, etc.

Management and personnel of SSU (Guard posts)

Package

SE

Managerial documents of SDEs (SDE CSU) and SSU

Management and

personnel of SES package

**Personnel**

* + 1. The main components of the Physical Security and Counter-Terrorism Protection System of the Facility are:
* personnel of CSU and SSU;
* equipment of SSU (special and auxiliary means, weapons, communication equipment, etc.);
* SES complex (engineering systems, SE complex);
* organisational activities
  + 1. Personnel of the Physical Security and Counter-Terrorism Protection System of the Facility includes:
* a body that manages the Physical Security and Counter-Terrorism Protection System of the Facility – Facility administration, site CSU personnel;
* a body that manages Security Guards and SSU personnel;
* a body that manages SES maintenance personnel.
  + 1. The main activities, objectives, functions, structure and staffing of the body that manages the Physical Security and Counter-Terrorism Protection System of the Facility, rights, duties and responsibilities of Employees, procedures to appoint and terminate appointment are governed by duly adopted internal documents of the Company.
    2. Incorporation, reorganisation and dissolution of Security units, appointing and terminating appointments of SSU managers and personnel, rights, duties and responsibility of SSU employees, and guarantees of their personal safety, legal and social protection are governed by the security activities law and internal documents of Security Companies.
    3. Rights, duties and responsibilities of SSU managers and employees who operate and maintain the SES package in the course of their employment duties at the Guarded Facility are governed by internal Company documents in arrangement and provision of Access Control and Site Security Arrangements, and contracts for the corresponding services.
    4. Organisational activities of the Physical Security and Counter-Terrorism Protection System of Company Facilities include a group of measures to be implemented by management bodies listed in Sub-Clause 10.49. of the Regulations, and all managerial documents governing such measures.
    5. The managerial documents in Physical Protection of Facilities are developed with due account for specifics of the Physical Security and Counter-Terrorism Protection System of a specific Facility (category of the Facility, SSU organisational chart, availability of SES, features of Guarded Zones, etc.)
    6. According to the Facility category, the managerial documents of the Physical Security and Counter-Terrorism Protection System are:

|  |  |  |  |
| --- | --- | --- | --- |
| **Title**  **of the managerial document[[2]](#footnote-2)** | **Facility Category** | | |
| **High** | **Medium** | **Low** |
| Facility Security Certificate | + | + | +/− |
| ATP certificate (*if classified as a FVTA)* | + | + | +/− |
| Security unit provisions | + | + | +/− |
| Facility Security Guarding/defence plan | + | +/− | +/− |
| Site Security and Access Control Arrangements Instructions | + | + | +/− |
| Emergency response instructions | + | + | +/− |
| Provision on interactions in regular conditions and in case of an emergency *(with Facility personnel, state authorities)* | + | +/− | +/− |
| SES technical condition and operation inspections plan | + | + | +/− |

* + 1. Condition of Facility Physical Protection system is regularly inspected at the Company level and at the Facility level, drills and trainings are held to establish how effective it is, and to master interactions with SSU, law enforcement and other state authorities.
    2. Following evaluation of the adequacy of Facility protection, the Commission issues the following general recommended organisational and technical activities to build/improve the Physical Security and Counter-Terrorism Protection System of the Facility:

|  |  |  |  |
| --- | --- | --- | --- |
| List of Facility Physical Protection and Security Guarding activities | | | |
| **Activities** | **Facility Category[[3]](#footnote-3)** | | |
| **High** | **Medium** | **Low** |
| Make arrangements to guard the Facility as required for the current security guarding type of the Facility | + | + | + |
| Physically protect Critical Zones | + | + | + |
| Provide a Physical Protection and/or Security Guarding unit at the Facility | + | + | +/− |
| Provide Access Control Arrangements | + | + | +/− |
| Provide Site Security Arrangements | + | + | + |
| Allocate Guarded Zones within the Facility | + | + | +/− |
| Allocate restricted areas within the Facility | + | + | + |
| Establish control point(s) | + | + | +/− |
| Make arrangements for interaction with Facility personnel | + | + | +/− |
| Make arrangements for interaction with the Ministry of Internal Affairs | + | + | + |
| Make arrangements for interaction with the Emergency Ministry | + | + | + |
| Make arrangements for interaction with the National Security Committee | + | +/− | +/− |
| Make arrangements to supervise fulfilment of requirements for Physical Protection and Security Guarding | + | + | + |
| Make arrangements to supervise technical condition of SES | + | + | + |
| Provide professional training for personnel of the Physical Security and Counter-Terrorism Protection System of the Facility | + | + | + |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| List of organisational and technical activities for Physical Protection of Critical Zones within the Facility | | | | | |
| **Activities** | **Protection level** | | | | |
|  | I | II | III | IV | V |
| **Organisational activities to protect critical elements** | | | | | |
| Limit the number of persons who have access to Critical Zones | + | + | + | + | +/− |
| Arrange the critical element in a restricted access zone | − | − | − | − | +/− |
| Arrange the critical element in a protected zone | − | − | − | +/− | +/− |
| Arrange the critical element in an internal zone | + | + | + | +/− | − |
| Arrange the critical element in a highly important zone | + | +/− | − | − | − |
| Monitor psychological and physiological condition and reliability of personnel who have access to Critical Zones of the Facility | + | + | + | +/− | +/− |
| Check reliability of personnel who have access to Critical Zones within legally established limits | + | + | +/− | +/− | +/− |
| Establish the rule of two (three) for team work to reduce the probability of UAAs | + | + | +/− | +/− | +/− |
| **Engineering and technical activities to protect Critical Zones** | | | | | |
| Provide fencing for Perimeters of Guarded Zones (restricted access zones) | + | + | + | + | + |
| Provide engineering barriers for Perimeters of Guarded Zones | + | + | + | + | + |
| Arrange gate houses or posts with access control functions in secured buildings, constructions, rooms | + | + | + | + | + |
| Provide firefighting equipment (fixed and portable) for Guarded Zones | + | + | + | + | + |
| Provide reinforcements for doors, windows and process openings of civil structures accommodating Critical Zones | + | + | + | + | + |
| Use safety containers, screens, etc. to handle and store toxic and explosive materials and substances | + | + | + | + | + |
| Use protective properties of civil structures and terrain | + | + | + | + | + |
| **SES of Guarded zones, including:** | | | | | |
| - Security alarm | + | + | + | + | + |
| - Warning alarm | + | + | + | + | + |
| - Access Control System | + | + | + | +/− | + |
| - Close Circuit Television | + | + | +/− | +/− | − |
| - Detection of carried prohibited objects | + | + | + | +/− | − |
| - Information protection | + | + | + | +/− | + |
| - Communication and public address | + | + | + | + | + |
| - Power supply (electricity, security lighting) | + | + | + | +/− | + |

* 1. **The unified legal regulation mechanism for the System of Facility Security Guarding by Security Companies**
     1. The Company employs the unified legal regulation mechanism for the System of Facility Security Guarding by Security Companies that is ensured by legal and other regulations, these Regulations, other internal documents of KMG and SDE, Fund standards and republican, departmental and international standards duly adopted and applied in the Company.
     2. Subjects of Security Guarding activity provide the following Security Guarding services for the Company Facilities:

1. protection of life and health of private individuals;
2. Security Guarding of Facilities and/or property of private individuals and legal entities, inter alia, during transportation;
3. consulting and preparing recommended Security Guarding methods and legal protection against unlawful attacks.
   * 1. For Security Guarding services, the Company duly involves Security Companies, including the Security Subsidiary, through procurement and entering into contracts for Security Guarding Services (long term, mid-term, short-term).
     2. Security Guarding services are procured by the Company under the procurement legislation of the Republic of Kazakhstan and valid procurement management regulations, standards and corporate requirements of KMG, including procurement categories, valid as of entering into a Security Guarding services contract.
     3. Execution, performance, termination of Security Guarding service contracts, liability of parties under contracts are defined by the civil law according to specifics provided by the Security Guarding legislation, and requirements of Company’s and Fund’s internal corporate documents for execution, performance and termination of contracts.
     4. Responsibilities of parties under Security Guarding services contracts for FVTAs are established by the civil law with due account for specifics provided by the Security Guarding and counter-terrorism legislation.

A Security Guarding service contract for a FVTA shall stipulate liability and obligations of a Security Company to ensure Counter-Terrorism Protection and the proper level of Security.

* + 1. A Security Guarding service contract is entered into in a written format and shall include:

1. details about contracting parties, including numbers and dates of Security Guarding service provider licenses;
2. types of Security Guarding services, including service provider duties;
3. scope of the contract;
4. term and date of the contract;
5. liability of the parties.
   * 1. Company Facilities that are being handed over to be guarded by the Security Subsidiary shall be included in the list of Facilities (name, location) to be handed over to be guarded by the Security Subsidiary, which shall be duly submitted to an authorised body (licenser) in supervision of Security Guarding activities.
     2. The Security Subsidiary shall have the right to provide Security Guarding services only to KMG and its affiliates.
     3. Conditions of a Security Guarding service contract shall not contradict the requirements hereof, format and conditions of a typical Security Guarding service procurement contract approved by Resolution of the KMG Legal Governance Council dated 25 December 2017, Minutes No. 45.
     4. For the purposes hereof, the following basic organisational, technical and other requirements are established for Security Companies involved to Guard Facilities:

|  |  |
| --- | --- |
| **1.** | **The companies shall have:** |
| * state registration in justice authorities of the Republic of Kazakhstan and duly approved Articles of Association; * security guarding service license; * license for use of ionising radiation devices and units (X-ray examination equipment); * international certificates of conformity to ISO 9001:2015 – Quality Management System, and ISO 45001:2018 – Occupational Health and Safety Management; * permissions from an authorised body to use a radio frequency spectrum (RFS) at the premises and locations of serviced Facilities; * reliable business reputation and favourable references / recommendations; * steady solvency (have no outstanding tax debts of more than three months, encumbered or seized property, ongoing bankruptcy or liquidation procedures, business suspension in accordance with the law of the Republic of Kazakhstan); * service experience of at least 5 years at trunk pipelines, fields, oil and gas refining storage and sales facilities, major administrative buildings, business centres and other places of mass gatherings of people; * value of the total scope of work under a single contract of at least 100 mln tenge each year; * at least 100% share of local content in services; * currently deployed network of regional offices/branches in locations of services; * central and regional: * full-time duty dispatcher units and technical support units for Security Guarding and safety systems (security and fire alarm, access control, video surveillance, automated fire extinguishing systems); * full-time K9 unit (if K9 posts are provided), weaponry unit, health and safety unit. * resources to ensure and provide: * guarantees of compensation for the material damage as a result of unlawful actions of third parties at guarded Facilities through voluntary civil liability (professional liability) insurance for at least 10% of the total insurance liabilities under all existing contracts; * mandatory life and health insurance for employees involved to provide services; * pre-shift and periodic mandatory medical examinations for employees under the available contracts with medical institutions; * safe working conditions for employees at the place of service, including conditions for eating, domestic appliances and first aid kits; * substitutes for employees if a responsible customer representative has complaints about the latter, unconditionally and without additional checks of facts the customer is referring to; * round-the-clock quality management and control of the services; * enhanced Security Guarding of Facilities during mass events; * effective remuneration and compensation system for employees and annual indexation of salaries based on the inflation rate and corporate requirements of the Customer; * delivery of Security Guarding personnel to the place of work and arrangements for rotational work. |

|  |  |
| --- | --- |
| **2.** | **Personnel of the Security Company shall have:** |
| * as many competent and trained employees as required to provide services under the contract with the Customer, but not more than the standard number established by the Government of the Republic of Kazakhstan; * responsible full-time employees who have experience and education in industrial and fire safety, and who have been trained in radiation safety for work with ray examination units, other special programs; * Special requirements for personnel of Security companies: * at least 19 years of age; * Kazakhstan citizens; * at least one (1) year of experience in security or law enforcement; * physically fit and proficient in self-defence techniques; * meet the requirements of Clause 6 Article 10 of Law No. 85-II of the Republic of Kazakhstan dated 19 October 2000 – On Security Guarding Activities; * have certificates of special training and advanced training (special training courses), including anti-terrorist training; * have permissions to carry, store and use special devices and arms; * have certificates of basic industrial safety and fire safety training courses. * The Companies shall employ full-time personnel meeting the requirements of Order No.959 of the Minister of Internal Affairs of Republic of Kazakhstan dated 30 December 2014, and:  1. health and safety employees, employees educated in fire safety who have passed special training courses in radiation safety for work with ray examination units (*notarised copies of certificates*); 2. managers, including mid-rank managers who have been trained in health and safety, basic fire safety and industrial safety (*notarised copies of certificates*). |

|  |  |
| --- | --- |
| **3.** | **Security Guarding Companies shall have the following materials and equipment, etc., as required for provision of appropriate services (requirements for materials and equipment):** |
| * on the rights of ownership: * duty rifles and smooth-bore weapons with the necessary licenses and storage locations, with 1 piece of spare weapon for each 10 pcs of one type of deployed weapons for all security guarding types, and minimum stock of cartridges per weapon unit according to the standards established by the Government of the Republic of Kazakhstan; * main and redundant communication devices, including stationary, vehicle based and wearable radio stations, GSM telephones, necessary accessories (chargers, holders, belt clips, antennas, headsets and loudspeaker manipulators, at least 2 batteries for each radio station); * GPS monitoring system to track movement of Mobile Teams and personnel; * special devices (utility belts, metal detectors, rubber clubs, security check mirrors, torches, whistles, handcuffs, high visibility vests, etc.), as many and as good as required for the number of Security Guarding posts and the tasks they address; * optical surveillance and event-recording devices, including binoculars, night vision devices, thermal cameras, photo and video equipment, etc.; * winter and summer service uniform (male and female) for offices and field facilities, with a company logo, according to weather conditions and legal requirements (main and replacement garment sets based on weather conditions and being able to clean and repair them without affecting the quality of services); * all-terrain vehicles for Mobile Teams, including at least 1 standby vehicle for each 5 operated vehicles, with installed GPS, video registration system, flashing beacons and colour designs; * at least 4 working dogs for one K9 post, associated K9 equipment and tools. * on the rights of ownership or leasehold basis: * mobile and permanent constructions to provide proper housing conditions for personnel during rotational shifts, inter alia, to work, eat, rest between shifts, maintain equipment, etc., according to the requirements of sanitary standards and guidelines, with the necessary furniture, appliances, hot and cold water, heating, primary firefighting equipment; * rooms to store weapons; * equipped vehicles to transport rotational shifts to the place of service. |

|  |  |
| --- | --- |
| **4.** | **Security companies shall be able to (service quality control):** |
| * regularly inspect Security Guarded Facilities; * develop, get approval by the Customer and supervise maintaining of documents governing procedures and methods of Services (job descriptions of employees, security guarding instructions, personnel time sheets, duty schedule, layouts of the guarded facility, routes of vehicles across the territory, etc.); * have joint interaction plans with law enforcement; * keep proper sanitary condition of rooms provided by the Customer to arrange security guard posts, neat appearance, bearing and behaviour (code of ethics) of employees; * effectively manage and administratively support provision of the services (record working hours, issue VAT invoices, etc.), inter alia, by training employees in provision of services, requirements of internal Customer documents governing security; * constantly interact with the Customer to provide appropriate service and submit documented evidence to confirm fulfilment of Customer’s requirements; * hold regular trainings to check professional level of employees at training centres and guarded Facilities; * as approved by the Customer, do other actions to improve quality control of the provided Security Guarding Services. |

* + 1. A mandatory step (condition) before entering into a security guarding service contract is inspection of the Facility, i.e. to study its condition, properties and features, to establish how resistant it is against UAA, including Unlawful Attacks and Acts of Terrorism, and develop organisational and technical solutions for Physical Protection and Security Guarding.
    2. Facilities are inspected by a working team comprising authorised representatives of Company SCU and Security Company. During the inspection, the working team:

1. evaluates the Facility, reviews its features according to the current condition of security systems, the assigned Category, Potential and Real Threats and Risk factors;
2. determines potential ways to overcome Security boundaries, Security alarm lines;
3. develops recommended quantities of manpower and methods of Security Guarding, weapons for SSU and SES for the Facility.
   * 1. To review Potential and Real Threats and Risk factors, the Working Team establishes the degree of Threats and vulnerabilities of the Facility, the most important valuables to be guarded (people, information, buildings, constructions and rooms, equipment, environment, etc.), Risk priorities, counteractions and cost of services.
     2. The necessary Security Guarding manpower, methods and procedures, SSU weapons, the necessary SES are determined according to the requirements hereof, and:
4. specifics of terrain where the Facility is located, its area, remoteness from industrial centres, population density and criminal situation in the area, availability of territorial offices of law enforcement and special bodies in the vicinity, emergency departments;
5. harmful industries within the Facility;
6. number of categorised buildings, constructions and rooms, high security facilities, number and properties of PHA and Critical Zones;
7. quantities of available and additionally required SES;
8. quantities and types of gate houses;
9. if the Facility qualifies as FVTA.
   * 1. Results of the Facility inspections are issued by the Working Team as a Facility Inspection Record. The Facility Inspection Record is issued in two copies, one for each party, includes date, position of inspectors, their full names. The Record is signed by responsible representatives (with written authority) of each party and sealed.
   1. **General requirements for arrangements and procedures of Facility Security Guarding**
      1. According to Guarded Facilities inspection results, their Categorisation and operational features, SDE CSU, together with the Security Company, establishes the Security Guarding System for Facilities, which includes the total quantity of forces and means to complete Security Guarding and defence objectives.
      2. The Security Guarding System of Facilities shall be consistent with their process features, the level of SES, surrounding situation, and ensure the most effective and economically reasonable use of the available forces and means of Security Guarding and SES.
      3. The Security Guarding System of Facilities is built as stages: on the approaches to Facilities, in the guarded zone along the Perimeter, at gate houses and the most important and vulnerable production sites that provide steady operation of the Facility.
      4. The Facility Security Guarding System defines the tactics (methods) of Security Guarding and Physical Protection of the Facility against UAA, including Unlawful Attacks and Acts of Terrorism, as follows: screening the territory, patrolling (on foot, using vehicles and other means of transportation), using SES, working dogs, combined methods i.e. using several tactics.
      5. The following Guard posts are used according to category and operational features of different Facility types, their Critical Zones, established Threats and Offender Models assigned to the Facility, process safety and other safety measures at the Facility:
10. Gate houses at entrances/exits to/from the Guarded Facility (administrative building or territory) to implement Access Control, limit traffic and pedestrian movement in a certain area.
11. Stationary post provided for a single standalone Facility or several Facilities within an outdoor site or fenced off territory, with not more than 100 m to be walked around by a security guard;
12. Inspection post to guard one or more Facilities by walking around them, when it is over 100 meters, but not more than 300 meters long;
13. Technical post provided in a room with SE package to monitor and collect information;
14. Mobile Team that patrols protected zones of trunk pipelines to inspect them periodically, take measures to Secure them and prevent attempted UAA, including Unlawful Attacks and Acts of Terrorism against them;
15. First Response Team intended for immediate response after actuation of alarm of high security and other premises, and in case of complications of the situation until integrated forces, including law enforcement, arrive.
16. Perimeter post provided at border of the guarded territory, inter alia, at a watch tower, to block Access to the Guarded Facility outside of the Gate House.
17. K9 post (if working dogs are used);
18. Preventive post provided in addition to the available Security Guarding Forces.
    * 1. The following **Single Standards of Security forces and mid-level management** are used for regulatory control of the number of security guarding forces involved to ensure Physical Security and Counter-Terrorism Protection of Company Facilities, different types of Guard Posts for the purposes hereof:

|  |  |  |
| --- | --- | --- |
| **Security Forces standards[[4]](#footnote-4)** | | |
| **No.** | **Location of the post / special conditions** | **Quantity** |
| **Screening of Facilities[[5]](#footnote-5):** | | |
| 1) | Gate houses to pass and check personnel and visitors | One round-the-clock Stationary Guard post for each Gate House, with one Security Guard passing up to 50 private individuals per hour if the gate house does not have automated ACS (gate passes are checked manually) and up to 100 private individuals per hour if there is an automated ACS. |
| 2) | Gate houses to examine and admit motor vehicles | One round-the-clock Stationary Guard post for each vehicle entrance, with up to 10-20 vehicles per hour passing through one gate house |
| 3) | Combined gate house to admit and examine private individuals and vehicles[[6]](#footnote-6) | Two round-the-clock Stationary Guard Posts per GH |
| 4) | Gate houses for railway transportation[[7]](#footnote-7) | Two round-the-clock Stationary Guard Posts per GH |
| 5) | Standalone facility or several facilities within an outdoor area or a fenced-off territory | One round-the-clock stationary Guard post at entrance or at a route up to 100 meters long |
| 6) | Standalone, fenced-off territory of one or more Facilities | One round-the-clock Inspection Guard Post at a 100m-300m route  When guard is kept by a Security Guard armed with a stub-barrelled duty weapon or tubeless duty weapon with non-lethal cartridges, one round-the-clock Inspection Post is provided for a route up to 250 m long |
| 7) | Guarding and defending the Facility by watching from watch towers | When the Facility is guarded and defended by a Security Guard by watching from watch towers, one round-the-clock Stationary Post or Perimeter Post is assigned to a section up to 400 meters long (up to 250 meters in the forest and up to 300 meters at water) |
| 8) | To improve  reliability of Security Guarding | One round-the-clock Preventive Post is provided for each five round-the-clock Guard Posts |
| 9) | To improve efficiency of Security Guarding and ensure Physical Security | K9 guard posts with four working dogs can be used per K9 post[[8]](#footnote-8) |
| 10) | Guarding cargoes transported by rail transportation and motor vehicles | The number Security Guards is determined by the contract within the standards established for Security Guarding of stationary Facilities |
| **Patrolling of Facilities[[9]](#footnote-9):** | | |
| 11) | Linear  part of trunk oil pipelines | One round-the-clock Mobile Team with not more than 13.5 full-time Security Guards for 40-80 kilometres of the linear part of a trunk oil pipeline, given side roads, difficult terrain, service roads, remoteness from settlements, technical protections of the linear part, Threat review and criminal situation in the area |
| 12) | Linear Part of a Trunk Gas Pipeline | One round-the-clock Mobile Team with not more than 13.5 full-time Security Guards for 100-160 kilometres of the linear part of a trunk gas pipeline, given side roads, difficult terrain, service roads, remoteness from settlements, technical protections of the linear part, Threat review and criminal situation in the area |
| 13) | Fields (field outlet lines) and field pipelines[[10]](#footnote-10) | One Mobile Team comprising three Security Guards for:   * up to 15 square meters for Security Guarding of a workshop/field; * up to 25 km for patrolling and guarding of Perimeter/field; * up to 50 km for Security Guarding of field oil and gas pipelines, water pipelines, given difficult terrain along the service road, remoteness from settlements, technical protections of the linear part, Real Threat review and criminal situation in the area |
| 14) | For preventive activities | One round-the-clock preventive post for three mobile teams |
| 15) | For quick response to unlawful attacks against trunk pipeline. | According to the estimated time required to arrive to the Guarded Facility, First Response Teams comprising 3 security employees at the same time can also be involved |
| 16) | For security guarding of VIP facilities and other facilities with quick response of the First Response Team[[11]](#footnote-11) | First Response Teams comprising 3 security guards at the same time if the estimated time required to arrive to the Guarded Facility is 5-15 minutes (at 600 m/min) |
| **Security guarding using technical equipment[[12]](#footnote-12):** | | |
| 17) | Technical guard panel | One round-the-clock technical Guard post (operator/technician) |
| 18) | Video monitoring panel | One round-the-clock technical guard post if the guarded facility has up to 30 video cameras |
| 19) | Response to actuation of SES at the Guarded facilities. | One round-the-clock technical post for each 30 buildings and rooms with SE |
| 20) | Facility perimeter with fencing and SE | One round-the-clock technical post for a section up to 1000 m long |
| **Standard number of mid-level Security managers[[13]](#footnote-13):** | | |
| **No.** | **Title** | **Standard[[14]](#footnote-14)** |
| 21) | Head of a regional site | Appointed to manage Security Guarding forces at a group of standalone Facilities within the same site, if very far from the original office/branch of the Private Security Company |
| 22) | Supervisor | Appointed to manage and supervise Security Guarding forces at a group of Facilities or linear part of trunk pipelines owned by the same SDE. One inspector supervises 10-12 Facilities or 5-10 Mobile Teams |
| 23) | Head of Site Security | One Head of Site Security for each standalone stationary Facility guarded by 5 or more posts or 3 posts and one or more Mobile Teams assigned to the Facility |
| 24) | Head of a Guard post | One Head of Guard post for each standalone stationary Facility guarded by 2-4 posts |

* + 1. SSU staffing, quantities of weapons and special and auxiliary equipment are established based on standards defined by the Government of the Republic of Kazakhstan and corporate KMG documents, including these Regulations, and shall not exceed them.
    2. Based on the assigned category of the Guarded Facility and adequate provision of the protection level requirement, Security Guarding personnel is armed with smooth-bore, long and short barrelled duty weapons, tubeless firearms, gas weapons to be able to fire non-lethal cartridges, electric weapons, and special devices, on conditions and under standards established by the legislation of the Republic of Kazakhstan in security guarding and state control of certain types of weapons.
    3. SSU of the Security Subsidiary shall also have the right to use long-barrelled duty rifles and short-barrelled duty weapons at trunk pipeline facilities and oil and gas refineries.
    4. To perform their duties and for operational control of personnel, SSU is provided with communication and public address devices:
* city telephone communication (public telephone network);
* intercom of the Facility;
* direct telephones between Guard posts;
* radio communications and personal radio paging equipment.
  + 1. Based on conditions of the service, SSU is additionally provided with:
* vehicles of different types and passing ability;
* binoculars, night vision devices, etc.;
* portable electric torches with rechargeable batteries;
* different types of metal detectors, detectors of weapons, explosive substances and devices, radioactive, chemical and other toxic substances (special devices);
* additional gear (cloaks, etc.).
  + 1. Internal documents of the Security Company governing arrangements for and provision of Security Guarding activities shall include:

1. formats and methods of management;
2. how to arrange and carry out security guarding activities at Guarded Facilities;
3. arrangements, procedures and condition of service at Facilities;
4. management of work of the existing duty units of the Private Security Company and its regional departments;
5. rights and obligations of Security Guarding Personnel protecting the Guarded Facilities;
6. actions of Security personnel in case of an emergency;
7. how to accept and release Facilities under guard;
8. how to accept and release Facilities storing commodities under guard;
9. how to arrange interactions between the Private Security Company and administration of the Guarded Facilities, law enforcement and other state authorities;
10. instructions approved by administration of the Guarded Facility and describing actions of the Security Guarding Personnel to provide Access Control and Site Security Arrangements, examine personal belongings, products and tools carried to and from the Facility, vehicles and other means of transportation;
11. tactics (methods) of duty during Security Guarding of different Facility types (stationary, linear part of trunk and other pipelines, transported, etc.);
12. how to arrange supervision over duty of the Security Guarding personnel;
13. organisational and methodological support of Security Guarding activities;
14. other organisational and practical measures and actions of Security Guarding personnel to provide Security and Guard Facilities.
    * 1. Types of provided posts and methods of Security Guarding, requirements for tasks, rights and duties of Security Guarding personnel, materials and equipment and staffing of SSU are stipulated by Security Guarding service contracts and guard post provision records signed by responsible representatives (with written authority) of the contracting parties, and sealed as in Clause 5.7.16. of the Regulations.
    1. **General requirements for Engineering Fortification and SES of Facilities**
       1. Single approaches of the Company to Engineering Fortification and SES of Facilities are established based on the Hazard/Risk Category of the Facility (A, B, C, D) and category of the Facility by main sources, types and kinds of Security Threats (I, II, III) as specified in Clause 5.5. hereof.
       2. Approaches to Engineering Fortification of FVTA are defined according to requirements for Counter-Terrorism Protection of FVTA duly approved by the Government of the Republic of Kazakhstan.
       3. Design, construction, upgrade, retrofitting, overhaul of a FVTA define if the Facility meets the FVTA classification criteria and provide the necessary equipment and systems.
       4. Given their specifics, Facilities are fitted with:
15. engineering devices and constructions to fence off the Perimeter, zones and individual areas of the Facility/site to prevent free trespassing and consistent with security arrangements of the Facility;
16. anti-ramming devices/barriers, engineering barriers and vehicle slowing devices (planters, architectural and landscaping elements, bollards, etc.);
17. Gate Houses;
18. systems, means of alarm (including mobile or stationary alarm push buttons) and evacuation control;
19. security alarm systems and equipment;
20. access control (restriction) systems and equipment;
21. video surveillance system;
22. video analytics system (smart information systems to recognise faces, detect objects and situations);
23. security check systems and equipment;
24. security lighting systems and equipment;
25. communication systems and equipment;
26. power supply systems and equipment;
27. engineering means to reinforce walls, ceilings and partitions of buildings, constructions and rooms;
28. Right of Way;
29. trace control strips, security squad trails and guard roads;
30. watch towers, watch booths, guard boxes, rooms for guard units and watch, other external parameter monitoring systems;
31. warning and boundary signs;
32. protections of windows and doors of buildings (bulletproof glass, blast resistant film, grilles), constructions, rooms, padlocks and locking devices;
33. security equipment control points;
34. unmanned flying vehicles counteraction systems;
35. fire safety systems developed as established by the fire safety law of the Republic of Kazakhstan.

***Technical fortification of external enclosing structures***

* + 1. Company facility with a site shall have perimeter fencing to prevent free access of people and entry of vehicles to and from the Facility past the gate house.
    2. If there are sufficient grounds and funds, trunk pipelines and fields can also be fitted with a fencing to prevent free access of people and vehicles to guarded zones of Facilities past gate houses.
    3. The main fencing along the Facility Perimeter shall:
  1. be high and buried into ground to prevent free crossing and meet security arrangements of the Facility;
  2. have simple design, be highly resilient and durable;
  3. have no assemblies and structures, which make it easy to be crossed.
     1. Perimeter fencing shall be:

1) resistant to external climatic factors of all seasons and corresponding climatic zones;

2) protected against industrial interference and interference caused by vehicles, birds and animals.

* + 1. The main fencing is a permanent structure and shall be constructed as per typical designs; where required, shall be provided with reinforced concrete base to prevent being dug under or rebar basket buried 200-400 mm down into the ground.
    2. The main fencing of the Facility site shall be at least 2.5 meters high, or at least 3 m high in areas with snow cover over 1 m deep, shall be straight, without unnecessary bends and turns, restrict vision and make it hard to use SE, have no external protrusions or cavities.
    3. As required according to Category and operational features of Facilities, Yegoza type barbed wire cap or another device can be provided along the top edge of the external fencing of Facilities. Extra fencing is also installed on roofs of single-storey buildings adjacent to the fencing.
    4. There shall be no permanently open doors, gates, wickets, manholes, breaks or other damage in the external fencing.

The fencing shall not be adjacent to any attachments, except for buildings that are a part of the Perimeter. Ground-floor windows facing unguarded territory shall have metal grilles. Where required to match the general ensemble of the adjacent constructions, glazed surfaces reinforced with special film and other technical measures can be used as approved by Facility administration and the Security Company.

* + 1. The territory directly adjacent to the Facility fencing shall be provided with an Exclusion Zone with a trace control strip (TCS) that shall be wider that SE detection coverage.
    2. As required, a Right of Way is provided on the inside of the external fencing, which includes:
  1. external fencing (along the Perimeter);
  2. inspection post trail;
  3. TCS;
  4. electric lighting systems;
  5. guard boxes or towers;
  6. perimeter security systems and communication means;
  7. video surveillance systems;
  8. Right of Way fencing.
     1. The following requirements are applicable to the Right of Way:
  9. the Right of Way shall be thoroughly graded and cleared; there shall be no constructions or objects that make it difficult to use security equipment and visual control systems.
  10. Width of the Right of Way shall be selected so that to be able to arrange SE and shall be at least 3 meters;
      1. The Right of Way can be used for working dogs.

***Trace Control Strip***

* + 1. TCS is provided to detect traces of Offenders. It can be artificial or natural and shall:

1) be continuous along the entire Facility Perimeter;

2) be wide enough so that it cannot be jumped over;

3) not have objects that make it easier to pass it without leaving traces;

4) make it possible to use mechanical equipment to treat the entire length of the strip.

* + 1. An artificial strip shall be at least 3 meters wide; a natural strip can be wider based on location of Facilities. Areas where a wide enough strip cannot be provided shall be covered with engineering barriers.
    2. A natural TCS can be:
* soil (sand or other loose soil);
* vegetation (even grass cover, usually lawn grasses that can retain traces of passage through them);
* snow (natural snow cover).
  + 1. A natural TCS is built by marking its boundaries and preparing the terrain where it is to be located (clearing off foreign objects, levelling the guarded zone, providing drains for rainwater, meltwater, ground water, seeding lawn grass and other work).
    2. A natural TCS is ploughed or filled, the ploughing depth/filling height shall be at least 15 cm.
    3. TCS at crossings with railways, highways and dirt roads shall be filled.

Provide small bridges/walkways with filled TCS where TCS passes, creeks, ditches or ravines to avoid gaps. The space under the bridge/walkway shall be closed with engineering barriers and fitted with detection equipment.

* + 1. To prevent TCS from being washed by rainwater and meltwater, it is periodically drained to avoid accumulation of water at TCS, surface water is diverted to ditches through culverts and drain pipes, which are closed with gratings and fitted with detection equipment.
    2. To maintain proper condition of TCS at Facilities:
* surface of the strip is cleared off foreign objects;
* the strip is periodically weeded, ploughed, dragged and graded;
* filled parts of TCS are periodically filled with more soil;
* culverts and drain pipes are repaired.
  + 1. TCS is ploughed and dragged all over during spring, after snow has melted and the soil is dry, and in autumn before first frosts. New layers of soil are filled, dragged and graded where soil from TCS is blown off by wind or washed by water.

***Special roads (Guard roads)***

* + 1. Security Guards in vehicles move along site roads and special roads (Guard roads) which can be:
* gravel, crushed stone, slag with binder;
* asphalt concrete and cement concrete;
* prefabricated reinforced concrete.
  + 1. Guard roads shall run outside of detection equipment coverage, have minimised crossings with the existing motor and railway roads and be fitted with regular road signs.
    2. A Security Squad Trail is designed for convenient movement of security guards and is built along TCS if there is no Security Road or if it is more than 4 meters away from TCS.
    3. A Security Squad Trail can be soil, wooden, asphalt, concrete or reinforced concrete, and shall be designed as follows:

1. soil roadbed is provided on plain land and slopes;
2. wooden roadbed of shields or boards is provided on damp and waterlogged land. Height of the Security Squad Trail depends on floodwater level;
3. concrete and reinforced concrete pavement is provided where perimeter configuration of the Guarded Zone of the Facility will not be changed in the future, and where relief of the terrain does not complicate construction. Such trails can be in-situ or prefabricated reinforced concrete slabs.
4. any Security Squad Trail shall be 0.75-1.0 m wide. The entire length of the Security Squad Trail, except for wooden one, shall be fitted with ditches.
5. crossings over water obstacles and ravines shall be provided with bridges with handrails, with the top of the bridge decking, where possible, level with the Security Squad Trail.
6. steep slopes are provided with sloping staircases with handrails. A step shall be 20 cm, 25-30 cm wide; a flight of steps shall not have more than 15 steps. During winter, pedestrian bridges and sloping staircases are cleaned off snow and ice; slippery points are powdered with sand or fine slag.

***Gate houses***

* + 1. External and/or internal gate houses are provided at Facilities with established or intended Access Control arrangements. Gate houses shall be minimised and ensure the necessary throughput of people in vehicles.
    2. An external gate house is provided, if there is a fencing.
    3. External enclosing structures (walls and ceilings) of gate house buildings/constructions shall be resistant to external effects, including Unlawful Attacks, have a good field of vision and ensure protection of a Security Guard against an attack.
    4. According to Access Control Arrangements, the gate house includes a special room to store paper and electronic gate passes.
    5. The main vehicle Gate House of the Facility, where possible, shall be located near the central Gate House to pass Personnel.
    6. Road sections to the vehicle gate house shall turn 90 degrees not more than 30 meters away from the gates. Such sections shall be fenced off by concrete structures to prevent driving over them. There can be other structural anti-ramming solutions.
    7. Gate houses for motor vehicles and railway transport may be combined.
    8. Facility gate houses are fitted with a chamber to store personal belongings of Personnel, security check room, amenity room for Security Guards, security equipment systems (concentrators, panels, closed-circuit television devices, etc.), access opening/closing controls and security lighting, and a lavatory.
    9. A gate house is fitted with automated or mechanised manual devices, turnstiles, wickets, etc.; as required, with security check mirrors (vehicle gate houses), stationary and manual security check devices capable to distinguish between different types of metal; as required for work, with detectors of explosives.
    10. Security check equipment is used at Facilities to detect weapons and other objects and substances which are prohibited to be carried in/out the Facility. Security check equipment of the Facility shall be consistent with the characteristic threats and operational features of the Facility.
    11. According to operational features of Facilities, central gate houses can be fitted with portable radiation control devices to detect -, - and radiation.
    12. Vehicle gate houses are fitted with typical electric, remotely controlled sliding or swinging gates, emergency shutdown and manual opening devices.

Gates are fitted with limiters or stops to prevent them from being inadvertently opened/moved.

* + 1. Fencing of vehicle gate houses and other entrances to FVTA are fitted with gates designed to be rigidly closed.

Closing and locking devices of gates and wickets at FVTA shall ensure the necessary protection against destructive impacts, retain operation within the ambient temperatures and humidity ranges of the climatic zone when directly exposed to water, snow, hail, sand and other factors.

* + 1. Vehicle gate houses are fitted with security check platforms or ramps, boom barriers. Railway gate houses are fitted with a tower and a platform to examine rolling stock. As required, entrances and exits are fitted with traffic lights and traffic signs.
    2. A vehicle examination site shall:

1. be at least 20 meters long and at least 3 meters wider than a lorry on each side;
2. be fitted with a vehicle bottom examination pit (where possible), towers or a ramp to examine sides and top of vehicles;
3. be fenced off by a main fencing type fence.
   * 1. Railway gate houses are fitted with:
   1. gates and a wagon examination site;
   2. electromechanical drive and a manual opening gear;
   3. forced stopping devices (wooden blocks, switches, deflecting tracks, etc.) to prevent unauthorised entry of transport to/exit from the Facility and prevent the rolling stock from running into the gates accidentally.
      1. In addition to examination platforms, railway transport is examined using:
4. watch towers, gangways, examination ramps, step ladders, suspended step boards;
5. top hatches and roofs of wagons of unmoving transport are examined using mobile towers and ladders;
6. safety during examination of transport on the examination platform is ensured by paired brake shoes.
   * 1. A wagon examination platform shall be designed as follows:
7. a wagon examination site shall be long enough to check 3-4 wagons at the same time;
8. the platform shall be fitted with a pit to examine bottom of wagons, and towers and ramps to examine sides and top;
9. the examination platform shall be transversely sloped at no more than 2 degrees relative to the place of duty of a Gate House Security Guard towards the sides (normal to the travel way). The platforms shall not be sloped longitudinally;
10. travel way of the platform shall have a place to stop transport to be examined, limited by two lines and a Stop sign in the state language and in Russian in white paint. Stop plates can be installed;
11. a transverse line and a Stop sign are also provided in front of the entrance to the examination platform, on the outside of the main and additional gates, not closer than 3 meters from them.
    * 1. To ensure safe movement of transport, a One Line Ahead sign is installed at least 100 meters away from the gates on the right or above the road, and a 5 km/h speed limit sign is installed 50 meters away.
      2. A gate control panel is located in the gate house or on its external wall so that unauthorised people shall not have access to it.
      3. The gate house room is fitted with communication, firefighting equipment and warning alarm system.

***Engineering fortification of buildings and constructions***

* + 1. Note the following general requirements for arrangement of buildings and constructions within the Facility:
  1. buildings and constructions, including buildings with continuous production cycle equipment, where possible, shall be as far as possible from the Protected Zone perimeter and covered by other buildings and constructions.
  2. quantity of above-ground utilities is calculated according to standards approved by legal acts of the Republic of Kazakhstan;

3) the Protected Zone can include an internal zone in the form of a group of standalone buildings or constructions with borders at walls of such buildings or at a special fencing.

* + 1. Engineering fortification of buildings and constructions of Facilities shall prevent easy access of Offenders to the Facility and movement inside of it, UAA, including unlawful attacks and Acts of Terrorism.
    2. Architectural design and layout and security systems of facilities and rooms shall together ensure the appropriate protection.
    3. All individual rooms within the Facility are divided into three main accessibility zones:

1. **Zone 1** – rooms with unrestricted access;
2. **Zone 2** – rooms that can only be accessed by a limited group of people;
3. **Zone 3** – rooms that can only be accessed by a strictly limited group of people.
   * 1. Strength of external walls of Category I facilities and rooms shall be equivalent to:

1) masonry, brick, block, concrete and hollow reinforced concrete structures over 500 mm thick;

2) cast in-situ fibrous concrete structures over 200 mm thick;

3) non-permanent walls reinforced (on the inside) with steel rebar basket welded at joints, of at least 10 mm thick bars, with >150x150 mesh size.

* + 1. Strength of external walls of Category II and III facilities and rooms shall be equivalent to:
  1. 250-500 mm thick masonry, brick, block, concrete and hollow reinforced concrete structures;
  2. 100-200 mm thick cast- in-situ reinforced concrete structures;
  3. 400 mm thick (or more) light concrete structures (cellular, aerated);
  4. non-permanent walls reinforced with a steel rebar basket welded at each bar joint.
     1. Strength of entrance doors of rooms at Category I and II facilities shall be equivalent to:
  5. wooden doors reinforced on both sides with steel sheet at least 0.6 mm thick, with the sheet folded towards the door inner surface or overlapping the leaf end, attached along the perimeter and diagonals of the leaf with 3 mm, 40 mm long nails spaced at not more than 50 mm;
  6. metals steel doors with at least 4 mm thick sheet;
  7. doors with a glass leaf with or without a metal frame, with safety glass resistant to knocking out a human-size hole with a heavy 2 kg metal object after at least 30-50 blows;
  8. non-permanent door with additional internal steel lattice doors (swinging, sliding or folding). Door frames shall have additional fasteners of steel bars, and hinges shall be additionally fitted by end hooks. Safety glass shall be resistant to knocking out a hole with a heavy 2 kg metal object after at least 30-50 blows.
     1. There may be an airlock with a second door or a lattice door between the entrance door and the main room. Additional swinging lattice doors with eyes for padlock shall be installed on the inside.
     2. The door frame shall be steel shapes. Wooden door frames can be used that are reinforced with 30x40x5 mm steel angles and attached to the wall with steel barbed nails at least 12 mm in diameter.
     3. Windows of warehouses, cash registers, weaponry rooms, Security Guard rooms, rooms where confidential and other restricted information is handled shall be provided with metal grilles of steel bar at least 16 mm in diameter forming a 150x150 mm mesh.

Decorative grilles or louvres can be used if their strength and intrusion resistance are on par with the above grilles.

According to the design of windows frames, grilles can be installed both on the inside of the room or between frames.

* + 1. Regular and decorative (non-sliding and non-swinging) grills can be installed on the outside if their strength is on par with the above grilles.
    2. Where all windows in a room are grilled, one of the grilles shall be swinging or sliding with a tamper-proof padlock.
    3. Strength of entrance doors of rooms at Category III facilities shall be equivalent to:

1. internal wooden doors with solid leaves which are at least 40 mm thick;
2. external wooden doors with at least 40 mm thick leaves, blind and glazed with multi-layered glass, resistant to a single blow and withstanding 3 blows of a 4 kg steel ball dropped from 3.5 meters or higher;
3. doors with glass leaves with or without metal frames, with safety glass resistant to a single blow and withstanding 3 blows of a 4 kg steel ball dropped from 3.5 meters or higher.
   * 1. For rooms in Category I and II facilities, a Facility entrance door is recommended to have electromechanical and/or mechanical locks with at least 100,000 code/key combinations.
     2. Locking devices shall be installed according to fire safety requirements:
4. external escape doors of buildings shall not have latches that cannot be opened from the inside without a key;
5. doors of staircases to common corridors, doors of elevator halls and airlocks shall have self-closers and seals at jambs, and shall not have latches preventing them from being opened without a key.
   * 1. Doors, windows, hatches, elevator shafts, etc. shall be provided with mortise locks that cannot be automatically snapped, rim locks, padlocks, internal hooks, latches, deadbolts, snoot bolts, etc.
     2. Entrance doors of facilities and internal doors of Category I rooms shall be locked with high security, lever tumbler locks with a double bending key, cylinder pin locks with two or more rows. Lever tumbler locks shall have at least six tumblers (symmetrical or asymmetrical).
     3. Internal doors of Category II rooms are locked with low security cylinder plate or cylinder pin single row locks. Rim locks are only used for internal rooms of Category III rooms.
     4. Doors, gates, grilles, shutters, etc. are locked using padlocks with a hardened steel shackle and solid body. Locations of padlocks on locked structures shall have protective covers, plates or other devices to prevent eyes and lock shackles from being wound out or sawed off.
     5. Lock mechanisms are placed inside covers to protect them against deliberate damage using small tools and sealed.
     6. A part of the mortise lock cylinder protruding beyond the door leaf on the outside of the door shall be secured against breaking or knocking off by a safety pad, socket, shield. The protruding cylinder part, after installation of a safety pad, socket, shield, shall be not more than 2 mm.
     7. Door hinges shall be strong and steel. They shall be attached using screws.
     8. When a door is opened outwards, door hinges are provided with end hooks to prevent accessing the room by breaking or mechanically damaging the hinges. When the door is closed, the end hooks enter anchor plates on the door frame or similar elements. If a door is metal, the end hooks are welded, if a door is wooden, they are attached by screws.
     9. Locking boards are 4-6 mm metal strip at least 70 mm wide. Eyes for padlocks are 6x40 mm metal strip. Door hooks are metal bar at least 15 mm in diameter.
     10. Hooks and boards are attached to walls, door frames and other locations with bolts or bribed nails at least 15 mm in diameter. The inserted bolts are secured on the inside of the room using washers and nuts, the bolt ends are riveted.
     11. Doors of elevator shaft doors are locked by padlocks, crossbars, detectors, etc.
     12. Strength of windows, ground-floor showcases of rooms at Category I and II facilities shall be equivalent to:
   1. windows with regular glazing additionally protected by rolling shutters of at least 1 mm thick steel sheet;
   2. windows with regular glazing additionally protected by metal grilles (swinging, sliding, etc.) or adequately strong louvres;
   3. special windows with safety glass resistant to a single blow and withstanding 3 blows of a 4 kg steel ball dropped from 9.5 meters or higher.
      1. In areas with complex situation, windows and showcases are recommended to have safety glass (film) resistant to knocking out a human-size hole with a heavy 2 kg metal object after at least 30-50 blows, or bulletproof safety glass (film).
      2. Strength of windows, ground-floor showcases of rooms at Category III facilities shall be equivalent to:

1) windows with safety glass resistant to a single blow and withstanding 3 blows of a 4 kg steel ball dropped from 3.5 meters or higher;

2) windows with regular glazing, reinforced with metal grilles, randomly designed mesh;

3) windows with regular glazing protected by additional rolling shutters.

Underground and aboveground utilities with inlets and outlets designed as manholes, hatches, shafts, open pipelines, channels and similar that can be used to access buildings and constructions shall have permanent or removable grilles, covers, doors with locking devices or other SE.

* + 1. Protections for windows, doors of buildings (bulletproof glass, blast resistant film, grilles), constructions, rooms, locks and locking devices, other technical solutions at Facilities shall be used to improve their security and compensate for other lacking SES.

***Engineering fortification of Guard Post rooms of light steel structures***

* + 1. Technical fortification of Guard Post rooms of modular light steel structures (LSS) shall meet the following requirements:

1. external LSS walls shall be reinforced on the inside with a metal reinforcement basket of at least 5 mm rebars forming 70x70 mm, but not more than 10 mm in diameter, with 150x150 mesh size. The basket shall be at least 2.5 meters above the ground;
2. new LSS rooms are constructed on a brick or concrete base at least 1 meter above the ground;
3. metal lattice doors of 75x75x6 mm steel angle or 15 mm rebars forming a mesh with not more than 150x15 0mm between bars are installed on the inside of rooms.

***Machinery handling boxes***

* + 1. Machinery handling boxes in rooms of Category I and II Facilities shall have metal gates; machinery handling boxes in rooms of Category III facilities can be fitted with wooden gates.
    2. Cargo handover rooms shall be arranged in the vicinity of the machinery handling boxes. Doors of such rooms shall open towards the boxes and have the same tamper-proofing provisions as the gates.
    3. Gates of boxes and doors of machinery reloading rooms are locked using electromechanical and/or mechanical locks (mortise locks or padlocks). Locking mechanisms are installed on the inside of box gates and doors to rooms of the Facility.

***Security unit premises***

* + 1. Rooms of Security unit are usually arranged at the ground floor of buildings. Requirements for design of such rooms shall be consistent with the requirements for the corresponding building category. Strength of the external perimeter (walls, doors and windows) of Security unit rooms shall be equivalent to that required for structures of rooms of Category II facilities.
    2. Engineering equipment of Guard posts, which include watch towers, guard boxes, and booths, and partitions designed as barriers of Security Guard duty locations in buildings and at high security rooms are subject to the following requirements:

1. watch towers can be brick, wooden, metal or prefabricated reinforced concrete, and designed to improve visibility and monitoring by Security Guards of approaches to the Facility and the Right of Way. Height and location of the tower are determined according to terrain, configuration and local conditions.
2. depending on operational specifics and Security Guarding of the Facility, the towers are fitted with duty communication devices, warning alarms, portable radio stations, public address communication, surveillance equipment, controlled/uncontrolled floodlights. The scope of equipment for the towers is defined in the terms of reference;
3. tower shall be designed taking into account the local climatic conditions according to season (glazing, winterisation and air conditioning) and protect a Security Guard against being struck with firearms;
4. guard boxes designed to arrange duty communication equipment, warning alarms, post uniforms are placed in the Right of Way, usually in the centre of post sites, not more than 1 meter away from the Security Squad Trail;
5. guard boxes are wooden or steel structures with wooden and plastic parts;
6. guard booths designed to arrange communication equipment, warning alarms, examples of gate passes, signatures and seals, post uniforms are placed at Gate houses or the Right of Way;
7. guard booths can be brick, wooden or prefabricated reinforced concrete, steel structures, plastic, pressed and wooden parts. A guard booth shall be designed according to the local climatic conditions and season (glazing, winterisation and air conditioning, etc.) Sizes and types of guard booths are defined by the designer;
8. “Access Restricted”, “Do Not Enter” signs in the state language and in Russian, in certain cases – “Authorised Entry Only” and “Warning Guard Dog” signs are installed along the fencing of the Right of Way to warn about the restricted access to the Right of Way;
9. the warning signs are placed along the external and internal fencing of the Right of Way, not more than 50 meters from each other, on the existing fencing supports or dedicated stands. Warning signs shall be provided at turns (corners) of the restricted zone, wickets and gates of the Right of Way;
10. borders of guard post sites within the Right of Way are identified by boundary signs which are numbered and progressively placed along the Right of Way so that they are clearly visible for Security Squads, but cannot be seen by outsiders from outside the Right of Way.
    * 1. Rooms of technical Guard posts, video surveillance posts and similar are arranged at the first, second floors of buildings. If such rooms are arranged at the ground floor, strength of the civil structures (walls, doors, windows) shall be equivalent to that of structures of Category B Facilities. Rooms are designed in accordance with health and safety, production sanitation requirements.

***Establishing a gate pass office***

* + 1. As required, a gate pass office is arranged at the Facility, which shall be arranged near the central entrance and have a separate entrance and exit outdoors i.e. outside of the Facility.
    2. According to operational specifics of the Facility, the established Security Guarding arrangements, the Gate Pass Office shall be fitted with security, fire, warning alarm equipment and video surveillance system wired to the central guard post to monitor the situation inside the office, a system to check authenticity of documents.
    3. A visitor’s room is equipped with a stationary walk-through detector with a remote-control panel in the security room, the guard post is equipped with a manual metal detector.

***Providing SES for Facilities***

* + 1. SES complex, including engineering equipment and SE, as one of the core elements of the Physical Security and Counter-Terrorism Protection System of the Facility:

1. ensures continuous online control of the Physical Security and Counter-Terrorism Protection System of the Facility;
2. ensures the established Access Control to the Guarded zones;
3. makes it harder for Offenders to attempt an unauthorised access to the Guarded Zones, buildings, construction, rooms;
4. prevents ramming breakthrough of vehicles to the Guarded Zone;
5. issues signals to control points of the Physical Security and Counter-Terrorism Protection System of the Facility about attempted and committed UAA;
6. creates favourable conditions for Security forces to perform their employment duties and facilitate apprehension of Offenders;
7. remotely monitors the Perimeter of Guarded Zones, guarded buildings, rooms, constructions and evaluates the situation;
8. ensures manoeuvring of SSE forces and means;
9. identifies boundaries of Guarded and monitored zones;
10. records signals from SE, instructions and commands issued by management bodies and reports of personnel of the Physical Security and Counter-Terrorism Protection System of the Facility;
11. protects Personnel of the Physical Security and Counter-Terrorism Protection System of the Facility during duty at control points, gate houses, posts, and interception of UAA and apprehension of involved individuals;
12. prevents prohibited objects, substances and materials, etc. from being carried in and out of the Facility.
    * 1. SE packages of Facilities include the following basic structural components (functional systems):

* security and warning alarm (including mobile or stationary alarm devices – Alarm push buttons);
* access control;
* close circuit television;
* operative communication and public address;
* information protection;
* power supply;
* lighting;
* public address;
* unmanned flying vehicles counteraction systems.
  + 1. SE shall ensure that they operate reliably and are consistent with conditions of application:

1. have an acceptable explosion protection or enclosure ingress protection rating of electrical equipment and instruments according to explosion hazard class of the Guarded Facilities;
2. withstand:

* temperature conditions of the area;
* air humidity over acceptable limits;

1. be resistant to:

* radio interference;
* switching pulse interference;
* overvoltages and voltage drops in the power mains;
* lightning interferences;
* stray earth current interferences.
  + 1. To improve efficiency of Facility protection systems, create the necessary conditions for Security personnel to carry out their tasks, facilities use engineering protections, which include engineering constructions, structures and physical barriers.
    2. Engineering protections include:
* civil structures (walls, ceilings, gates, doors, etc.);
* gate houses;
* fencing (main perimeter, fencing of Guarded zones) of the Facility;
* engineering barriers (stationary and portable);
* reinforcements of doors, windows, process openings;
* anti-ramming devices (permanent and portable including planters, architectural and landscaping elements, bollards, etc.);
* protections of control panel operators, Security Guards at gate houses against small and other weapons and sudden attacks.
  + 1. Company FVTA are equipped with SES according to FVTA Counter-Terrorism Protection requirements duly approved by the Government of the Republic of Kazakhstan.
    2. FVTA shall be equipped with closed circuit television and public address systems. Technical requirements for video surveillance systems included in the closed-circuit television system of FVTA shall be consistent with the minimum technical capabilities of video surveillance systems provided by the National Video Monitoring System Operational Guidelines duly approved by the Chairman of the National Security Committee of the Republic of Kazakhstan.
  1. **Training activities** 
     1. The following drills are provided to maintain proper preparedness of Company CSU, Security Companies, Facility employees, and take the following formats:

1. briefings;
2. trainings (training exercises);
3. drills;
4. experiment (at FVTA)
   * 1. Training activities teach Personnel of the Company CSU, Security Companies, companies maintaining SE, Facility personnel how to respond to committed/threatened Unlawful Attacks or Acts of Terrorism, how to prevent and stop them, protect against their consequences, how to safely and timely evacuate from the Facility, and other necessary skills.
     2. There are scheduled and unscheduled training activities according to their nature and time.
     3. Frequency of training activities, except for unscheduled activities, is defined as approved by CSD and SDE CSU, and involved Security Companies based on annual plans/schedules, which include:
5. topic of a training activity;
6. facility name, activity date and time;
7. participants;
8. introductory tasks for participants.
   * 1. Unscheduled training activities and their content are defined on case-by-case basis according to causes and circumstances necessitating them.
     2. Practical and theoretical training activities in briefing format are held individually or for groups, trainings (exercises) or drills can be conducted for a group of Employees of similar Facilities.
     3. Procedure, frequency, topics and formats of training and preventive activities at FVTA, including experiments, are defined according to the valid FVTA counter-terrorism requirements approved by an authorised body.
     4. Theoretical classes teach participants information on the subject, practical exercises help master:
9. safe and unobstructed evacuation from the Facility;
10. response to a committed or threatened Unlawful Attack including an Act of Terrorism at the Facility (public address, primary response, interactions between participants, etc.);
11. how to act after detection of suspicious individuals and objects at the Facility, and in other scenarios of Unlawful Attacks, including Acts of Terrorism, typical for the Facility.
    * 1. The main goals of drills are:
12. develop the relevant skills and preparedness in personnel to respond to abnormal situations;
13. teach personnel to think, be initiative, independent and be able to assess the real situation, take decisions and quickly implement them;
14. improve interactions between units involved in the system of joint forces (CSD and SDE, Security Companies, Internal Affairs, National Security Committee, Emergency Ministry, etc.) during Unlawful Attacks, including Acts of Terrorism, and to prevent them;
15. improve efficiency of duty services;
16. check actuality and performance of Facility security guarding and defence plans, communication sequence, and other organisational documents.
    * 1. Preparation for a drill includes development of a drill plan which specifies time and location, drill leader, list, duties and actions of participants, expected solutions, materials and equipment for the drill. Introductory tasks are developed and attached to the plan.
      2. Regardless of composition, scale and methods, drills are as close as possible to the actual situation.

The drill can be complicated by adding new tasks. To develop and complicate the tasks for drill participants, the drill leader may decide to implement the corresponding operation plans.

* + 1. At the end of the drill, it shall be summed up to evaluate:

1. actions of the drill participants, how quickly they responded to the incoming signals and inputs;
2. the regular scenario for involvement of the available forces and means;
3. whether the participants are ready to quickly address practical tasks in difficult conditions and whether they are able to act;
4. whether the gear of the involved forces and means meets the established requirements.
   * 1. Particular attention is paid to explaining the participants the errors they made during the drill.
     2. Training activities are recorded in the training activities log, including:
5. date of the training activity;
6. type of the training activity;
7. topic, subjects (for an exercise or drill);
8. number of participating employees;
9. full name and position of a person who conducted the activity or was in charge of it;
10. signature of a person who conducted the activity or was in charge of it;
11. signature of the training activity participant (for briefing).
    * 1. The counter-terrorism training activities log is maintained according to the valid FVTA counter-terrorism protection requirements approved by an authorised body.
      2. If a training activity involves many participants (more than 20 people), it can be documented in a report or record.
      3. Topics of training activities may include, but not be limited to:
12. access control and site security arrangements. How to use security check equipment and metal detectors;
13. unauthorised intrusion at the Facility using fake documents;
14. carrying valuables in/out the Facility without authorisation;
15. unauthorised intrusion at the Facility by overcoming the fencing;
16. attack on the Facility;
17. unauthorised intrusion at the Facility using a vehicle;
18. carrying prohibited objects, devices and substances to the Facility.
19. response of Facility personnel to a terroristic threat;
20. activities to evacuate from premises in case of a terroristic threat;
21. how to act after detection of a suspicious object that looks like an explosive device;
22. how to act if terroristic threats are made by the phone;
23. how to act if terroristic threats are made in a written note;
24. hostage situation. Actions guide for hostages;
25. actions to enhance alertness of Facility personnel to prevent Acts of Terrorism.
    * 1. Following a training exercise or drill, actions of each participant are summed up, and flaws, errors are discussed and practical measures are taken to eliminate them.
    1. Main areas of the Physical Security and Counter-Terrorism Protection System of the Company
       1. Physical Security and Counter-Terrorism Protection of the Company is provided through:
26. exercising the single policy of Physical Security and Counter-Terrorism Protection System of the Company to protect Security Objects against Unlawful Attacks;
27. making arrangements to inspect and categorise Company Facilities to establish effective measures to counteract different types of Unlawful Attacks, implement activities to improve Physical Security and Counter-Terrorism Protection System of Facilities, including provision of SES for Facilities;
28. making arrangements to share information, record, systematise, evaluate and review Real and Potential Threats to the Company;
29. holding interactions inside the Company, with state bodies and organisations, non-government organisations, private individuals and legal entities;
30. assigning CSU employees to specific Facilities, including FVTA, to manage and support this work consistently;
31. engagement of Company Employees in activities to counteract Unlawful Attacks, cultivating intolerance to any Unlawful Manifestations among Employees;
32. prevention of Real and Potential Threats and Risks, Unlawful Attacks against Security Objects.
    * 1. Activities to provide Physical Security and Counter-Terrorism Protection for the purposes hereof include:
    1. developing and introducing internal documents and procedures to provide Physical Security and Counter-Terrorism Protection of Company Facilities;
    2. reviewing and examining the adopted regulative and managerial documents for vulnerabilities creating conditions for Unlawful Attacks against Security Objects, and inclusion of preventive measures in them;
    3. developing work plans, reports, monitoring the level of Physical Security and Counter-Terrorism Protection of Company Facilities, including plans, activities to prevent Unlawful Attacks at the Facilities;
    4. processing and reviewing information on monitoring of Physical Security and Counter-Terrorism Protection (production facilities, contract territories, etc.);
    5. developing organisational and practical measures to improve efficiency of Access Control, among other things, using state-of-the-art technical protections, access control and video surveillance systems at Fund facilities, and PC and SDE;
    6. holding counter-terrorism activities, including counter-terrorism training, advanced training and retraining of Company Personnel, Security Companies involved;
    7. identifying and reviewing risks for Physical Security and Counter-Terrorism Protection, developing and introducing adequate procedures and measures to prevent and minimise them;
    8. restricting access to information resources that are capable of affecting the level of Company’s Physical Security and Counter-Terrorism Protection, or access to protected information resources;
    9. introducing and applying hardware and software to monitor and protect information resources, prevent unauthorised intrusion to information systems of the Company;
    10. checking Employees at appointment to a position and candidates at hiring, Personnel of Contractors and other companies for administrative and criminal offences;
    11. ensuring continuous operation of Information Systems, company confidence systems to raise interest among Employees and other people in reporting signs of Unlawful Actions, timely review reports;
    12. participation, together with Compliance Units, in activities to investigate Company Employees;
    13. conducting informational work and awareness-raising about requirements of these Regulations;
    14. implementing other activities to minimise Threats to Physical Security and Counter-Terrorism Protection by any means that do not contradict the law of the Republic of Kazakhstan.
33. **References**

|  |  |  |
| --- | --- | --- |
| Law No.422-V of the Republic of Kazakhstan dated 24.11.2015 | **-** | Criminal Code of the Republic of Kazakhstan |
| Law No.235-V of the Republic of Kazakhstan dated 05.07.2014 | **-** | Administrative Violations Code of the Republic of Kazakhstan |
| Law No.85-II of the Republic of Kazakhstan dated 19 October 2000 | **-** | On Security Guarding Activities |
| Law No.416-I of the Republic of Kazakhstan dated 13 July 1999 | **-** | On Combating Terrorism |
| Law No.20-V of the Republic of Kazakhstan dated 22 June 2012 | **-** | On Trunk Pipeline |
| Law No.339-I of the Republic of Kazakhstan dated 30 December 1998 | **-** | On State Control over Circulation of Certain Weapons |
| Law No.188-V of the Republic of Kazakhstan dated 11 April 2014 | - | On Civil Protection |
| Resolution No. 407 of the Republic of Kazakhstan Government dated 5 April 2002 | - | On Measures to Implement the Law of the Republic of Kazakhstan − On Security Guarding Activities |
| Resolution No.1176 of the Republic of Kazakhstan Government dated 3 August 2000 | - | On Measures to Implement the Law of the Republic of Kazakhstan − On State Control over Circulation of Certain Weapons |
| Resolution No.909 of the Republic of Kazakhstan Government dated 4 August 2011 | - | On Approval of the Guidelines for Incorporation of Security Companies by National Companies and Amendment to Resolution No.686 of the Republic of Kazakhstan Government dated 10 August 2007 – On Approval of Guidelines for Licensing and Qualification Requirements for Security Guarding Activities, Installation, Commissioning and Maintenance of Security Alarm Equipment Except for Construction and Installation Activities |
| Resolution No.1198 of the Republic of Kazakhstan Government dated 14 November 2014 | - | On Revisions and Amendments to Resolution No.1176 of the Republic of Kazakhstan Government dated 3 August 2000 – On Measures to Implement the Republic of Kazakhstan Law – On State Control Over Circulation of Certain Weapons |
| Resolution No. 191 of the Republic of Kazakhstan Government dated 3 April 2015 | - | On approval of the Requirements for Counter-Terrorism Protection System of Facilities Vulnerable to Terrorist Attack |
| Resolution No. 876 of the Republic of Kazakhstan Government dated 28 August 2013 | - | On Approval of the List of Facilities in the Republic of Kazakhstan Vulnerable to Terrorist Attack |
| Resolution No. 756 of the Republic of Kazakhstan Government dated 2 July 2014 | - | On Establishing Classification for Natural and Man-Made Emergencies |
| Order No. 32 of the Minister of Energy of the Republic of Kazakhstan dated 22 January 2015 | - | On Approval of Guidelines for Security Guarding of Trunk Pipelines |
| Order No. 142 of the Minister of Internal Affairs of the Republic of Kazakhstan dated 23 February 2015 | - | On Approval of Models of Special Garments and Guidelines for Application by Security Guards of Private Security Companies |
| Order No. 959 of the Minister of Internal Affairs of the Republic of Kazakhstan dated 30 December 2014 | - | On Approval of Qualification Requirements and the List of Conformance Evidence Documents for Security Guarding |
| Order No.256 of JSC NC "KazMunayGas" dated 4 August 2015 | - | On Approval of Single Standards for Security Forces and Mid-level Managers for Security Guarding of Facilities of JSC "National Company "KazMunayGas" and its Subsidiaries |

1. **Record Forms**

None for these Regulations.

1. **Revision and Amendment Procedure**

These Regulations are revised and amended as established by internal KMG documents.

1. Critical Zones are located in Guarded Zones (protected, internal, highly important) according to the established protection levels. Zoning of the Facility reinforces its protection from the peripherals to the centre, i.e. to Critical Zones their categories are based upon. Additional protection boundaries can be created inside the existing zones. [↑](#footnote-ref-1)
2. Two or more documents can be combined, other documents can be developed as required. [↑](#footnote-ref-2)
3. “+” and “−” show if an activity is mandatory or optional for the given Facility category. “+” shows that an activity shall be decided upon by a specific Facility based on vulnerability assessment and physical protection system effectiveness evaluation. [↑](#footnote-ref-3)
4. Security Guarding time, number of Security Guards, weapons, technical equipment and special devices are stipulated by a security guarding service contract. [↑](#footnote-ref-4)
5. Actions of security guarding subject for visual surveillance of the Guarded Facility and its Physical Protection against Unlawful Attacks by providing Gate Houses, Guard posts (stationary, inspection, perimeter, preventive posts). [↑](#footnote-ref-5)
6. Combined gate houses are provided according to individual features of the Guarded Facility, review of Real Threats and number of committed unlawful and other actions against each individual Facility. [↑](#footnote-ref-6)
7. Gate houses for the passage of railway transport are introduced taking into account the individual characteristics of the Guarded Facility, analysis of real Threats and the number of illegal and other actions committed in relation to each individual Facility. [↑](#footnote-ref-7)
8. K9 posts may be used according to individual features of the Guarded Facility, review of Real Threats and number of committed unlawful and other actions against each individual Facility. [↑](#footnote-ref-8)
9. Includes Guarding of a trunk pipeline by driving around, walking around, visual surveillance, inter alia, using technical devices, by a group of Security Guards in a vehicle or other means (Mobile Teams, First Response Teams) to stop attempted or prepared Unlawful Attacks directly against trunk pipelines. [↑](#footnote-ref-9)
10. Established depending on the terrain, the availability of roads, vehicle resources and the average statistical time required for the theft of technological equipment and theft of hydrocarbon raw materials, including through criminal tie-ins into field oil pipelines and access to wells. [↑](#footnote-ref-10)
11. Quick response to activation of warning alarm or urgent response to a call from the Facility. The standard is established based on the practicable actions depending on terrain, availability of roads and traffic, vehicle resources and statistically average time required for the team to arrive to the scene and for Offenders to commit an Unlawful Attack (theft, burglary, robbery, etc.) [↑](#footnote-ref-11)
12. Trunk pipeline guarding method using SE involves actions of Security employees to watch the trunk pipeline using SE to physically protect it against Unlawful Attacks (technical posts). [↑](#footnote-ref-12)
13. Mid-level Security managers are a part of guard post staff. [↑](#footnote-ref-13)
14. Where required, such employees work in rotations and their number is increased by 2. [↑](#footnote-ref-14)