

On Cybersecurity

Unofficial translation

Law of the Republic of Kazakhstan dated 24 November 2015 № 418-V.

Unofficial translation

Footnote. The title is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Footnote. The preamble has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026, № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

SECTION 1.

Footnote. The title of Section 1 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Chapter 1. GENERAL PROVISIONS

Article 1. Basic concepts used in this Law

The following basic concepts are used in this Law:

1) information security tool – software, technical and other means designed and used to ensure information security;

2) user with privileged rights – a user with elevated access rights to a digital object, who ensures its normal operational functioning under standard operating conditions;

3) critically important digital objects – digital objects, the disruption or cessation of whose functioning results in the unlawful collection and processing of restricted-access personal data and other information containing legally protected secrets, the occurrence of social and/or man-made emergencies, or significant adverse consequences for defence, security, international relations, the economy, individual sectors of the economy, or the livelihood of the population residing in the relevant territory, including the infrastructure of: heat supply; electricity supply; gas supply; water supply; industry; healthcare; communications; the banking sector; transport; hydraulic engineering structures; law enforcement activities; and the “digital government”;

4) National source codes repository – a repository of source codes and executable codes of digital objects compiled from them;

5) domain name – a symbolic (alphanumeric) designation formed in accordance with the rules of Internet addressing, corresponding to a specific network address and intended for named access to an Internet object;

6) malicious program – a created or existing program or a software product that has been modified to allow for unauthorized access, destruction, blocking, modification or copying of digital data, as well as disruption of the functioning of digital objects;

7) a unified Internet access gateway – a hardware and software complex designed to protect a digital object when accessing the Internet and/or communication networks that have access to the Internet.

8) cybersecurity – the state of protection of digital objects from violation of their confidentiality, integrity or availability;

9) cybersecurity audit – assessment of the security status of digital objects for compliance with cybersecurity requirements;

10) cybersecurity researcher – a specialist in the field of cybersecurity who participates in the program of interaction with cybersecurity researchers;

11) cybersecurity threat – a set of conditions and factors that create the preconditions for the occurrence of a cybersecurity incident;

12) cybersecurity event management system – software or hardware, and software complex designed for automated detection of cybersecurity events by collecting and analysing events logs of a digital object;

13) cybersecurity events monitoring – continuous monitoring of a digital object in order to detect and identify cybersecurity events through a cybersecurity events management system;

14) cybersecurity event – an identified occurrence of a state of a digital object that indicates a possible breach of cybersecurity or a previously unknown situation that may be relevant to ensuring cybersecurity;

15) a program for interaction with cybersecurity researchers – organizational and technical measures that ensure interaction between cybersecurity researchers and digital objects to identify vulnerabilities in them;

16) cybersecurity monitoring system – organizational and technical measures aimed at monitoring the safe use of digital technologies;

17) cybersecurity centre - a legal entity or a structural subdivision of a legal entity that is a resident of the Republic of Kazakhstan without the participation of foreign legal entities and individuals, carrying out activities to protect digital objects;

18) authorized body in the field of cybersecurity (hereinafter - the authorized body) - the central executive body, carrying out management and inter-sectoral coordination in the field of cybersecurity;

19) national institute for development in the field of cybersecurity – a legal entity determined by the Government of the Republic of Kazakhstan for the purpose of developing the cybersecurity sector;

20) cybersecurity incident response service - a legal entity or a structural subdivision of a legal entity that is a resident of the Republic of Kazakhstan without the participation of foreign legal entities and individuals, responding to a cybersecurity incident in accordance with the competence established by this Law;

21) cybersecurity incident – an event or set of events that negatively impact the cybersecurity of a digital object;

22) cybersecurity incident response – actions taken to minimize or eliminate a cybersecurity incident, including actions taken to protect and restore the normal functioning of digital assets and the digital data contained therein, a process that includes identifying, analysing, and taking measures to counter events or violations that may pose a threat to the cybersecurity of digital assets

23) sectoral cybersecurity centre – a legal entity or a structural subdivision of a state body that carries out the organization and coordination of cybersecurity measures with respect to subordinate organizations and/or the regulated area of administration;

24) internal cybersecurity audit – an objective, documented process of monitoring the qualitative and quantitative characteristics of the current state of cybersecurity of digital objects in an organization, carried out by the organization itself in its own interests;

25) cyberculture – a set of norms and values of safe and responsible behaviour in the digital environment;

26) security profile – a list of minimum-security requirements for software and hardware that are components of digital objects;

27) state technical service – a state legal entity created by the decision of the Government of the Republic of Kazakhstan;

28) vulnerability – a flaw in a digital object that creates a threat to cybersecurity;

29) technical means – devices used for collecting, processing, storing, switching and transmitting digital data;

30) automated process control system – a digital infrastructure object designed for automation, management, control and monitoring of production processes in real time;

31) classifier of digital objects (hereinafter - the classifier) – a systematized list of categories aimed at identifying, categorizing, describing and recording digital objects;

32) digital events logging – the process of systematic recording, collecting and storing digital records of events occurring in digital objects for the purpose of subsequent analysis, detection of deviations and investigation of cybersecurity incidents;

33) a unified gateway of “digital government” email– a hardware and software complex that ensures the protection of “digital government” email in accordance with cybersecurity requirements.

Footnote. Article 1 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 2. Legislation of the Republic of Kazakhstan on cybersecurity

1. The legislation of the Republic of Kazakhstan on cybersecurity shall be based on the Constitution of the Republic of Kazakhstan and consists of this Law and other regulatory legal acts of the Republic of Kazakhstan.

2. International treaties ratified by the Republic of Kazakhstan shall take precedence over this Law. The procedure and conditions for the operation of international treaties to which the Republic of Kazakhstan is a party within the territory of the Republic of Kazakhstan shall be determined by the legislation of the Republic of Kazakhstan.

Footnote. Article 2 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry six months after the date of its first official publication).

Article 3. Scope of this Law

The scope of this Law shall be public relations in the field of cybersecurity arising on the territory of the Republic of Kazakhstan between state bodies, individuals and legal entities at all stages of the life cycle of digital objects.

Footnote. Article 3 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 4. The purpose and principles of state regulation of public relations in the field of cybersecurity

1. The purpose of state regulation of public relations in the field of cybersecurity shall be to achieve and maintain the security of digital objects that ensure the sustainable development of the Republic of Kazakhstan.

2. State regulation in the field of cybersecurity shall be based on the following basic principles:

- 1) legality;
- 2) ensuring the security of the individual, society and the state when using digital technologies;
- 3) the balance of rights, freedom and legitimate interests of the individual, society and the state, and their mutual responsibility in the digital environment;
- 4) respect for the rights, freedoms and legitimate interests of individuals, as well as the rights and legitimate interests of legal entities;
- 5) equality of rights, freedoms and legitimate interests of individuals and legal entities to participate in activities in the field of cybersecurity and the use of its results.

Footnote. Article 4 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Chapter 2. State regulation in the field of cybersecurity

Footnote. The title of Chapter 2 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 5. Objectives of state regulation in the field of cybersecurity

The objectives of state regulation in the field of cybersecurity shall be:

- 1) protection of digital objects and critical digital objects at all stages of their life cycle;
- 2) promoting the formation and development of the cybersecurity industry;
- 3) ensuring conditions for the development and implementation of modern cybersecurity solutions in production processes;
- 4) increasing cyberculture;
- 5) formation and implementation of a unified scientific, technical, and state technological policy in the field of cybersecurity;
- 6) monitoring the provision of cybersecurity of digital objects of state bodies, individuals and legal entities;
- 7) prevention and prompt response to cybersecurity incidents, including in the event of social, natural and man-made emergencies, the introduction of a state of emergency or martial law;
- 8) development of solutions in the field of cybersecurity and human resources;
- 9) participation in international cooperation;
- 10) improvement of the legislation of the Republic of Kazakhstan on cybersecurity.

Footnote. Article 5 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 6. Competence of the Government of the Republic of Kazakhstan in the field of cybersecurity

The Government of the Republic of Kazakhstan shall:

- 1) develop the main directions of state policy in the field of cybersecurity and organize their implementation;
- 2) define a national development institute in the field of cybersecurity;
- 3) approve uniform requirements in the areas of digitalization and cybersecurity;
- 4) approve the national anti-crisis plan for responding to cybersecurity incidents;
- 5) perform other functions assigned to it by the Constitution of the Republic of Kazakhstan, this Law, other laws of the Republic of Kazakhstan and acts of the President of the Republic of Kazakhstan.

Footnote. Article 6 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 7. Competence of the authorized body

Footnote. Article 7 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 7-1. Competence of the authorized body

The authorized body shall:

1) formulate and implement state policy in the field of cybersecurity in accordance with the legislation of the Republic of Kazakhstan on the basis of and in implementation of the main directions of the domestic and foreign policy of the state, as determined by the President of the Republic of Kazakhstan, and the main directions of the state's socio-economic policy, defence capability, security, and maintenance of public order, as developed by the Government of the Republic of Kazakhstan;

2) carry out strategic, regulatory, implementation and control functions;

3) develop uniform requirements in the areas of digitalization and cybersecurity;

4) approve the list of critically important digital objects, as well as the rules and criteria for classifying digital objects as critically important;

5) approve the methodology and rules for testing digital objects of the “digital government” and critically important digital objects for compliance with cybersecurity requirements;

6) approve the rules for monitoring cybersecurity events of digital objects of state bodies in agreement with the National Security Committee of the Republic of Kazakhstan;

7) approve the rules for monitoring the cybersecurity of digital objects of the “digital government” and critically important digital objects in agreement with the National Security Committee of the Republic of Kazakhstan;

8) approve the rules for monitoring the implementation of uniform requirements in the areas of digitalization and cybersecurity;

9) monitor the implementation of uniform requirements in the areas of digitalization and cybersecurity;

10) exercise state control in the field of digitalization, as well as compliance with the requirements for electronic documents and electronic digital signatures;

11) send orders for execution upon detection of violations of the requirements of the legislation of the Republic of Kazakhstan in the areas of digitalization and cybersecurity;

12) coordinate activities for the management of digital objects in emergency situations of social, natural and man-made nature, the introduction of a state of emergency or martial law;

13) participate in the commissioning of digital objects of the “digital government”;

14) organize assistance to owners, holders and users of digital objects in matters of safe use of digital technologies, including the prevention of illegal actions to obtain, copy, distribute, modify, destroy or block digital resources;

15) develop a national anti-crisis plan for responding to cybersecurity incidents;

16) determine the administrator and registrar of domain names, approve the rules for registration, use and distribution of domain names in the space of the Kazakhstan segment of the Internet;

17) approve the rules for the operation of the unified national backup platform for storing digital resources, the frequency of backup of digital resources of critical digital objects;

18) approve the rules for the operation of a unified gateway for Internet access, and a unified gateway for electronic mail of the “digital government” in agreement with the National Security Committee of the Republic of Kazakhstan;

19) approve the rules for the operation of the National sources codes repository;

20) approve protection profiles and the methodology for developing protection profiles;

21) approve the rules for the exchange of information necessary to ensure cybersecurity between cybersecurity centres, industry cybersecurity centres, and the National cybersecurity coordination centre;

22) issue opinions in the field of cybersecurity on investment proposals and financial and economic justifications for budget investments based on the examinations of the state technical service;

23) approve technical documentation, including technical specifications, for the creation or development of digital objects of the “digital government” for compliance with cybersecurity requirements based on the examinations of the state technical service, with the exception of digital objects of special state bodies of the Republic of Kazakhstan;

24) approve the rules for the operation of the program for interaction with cybersecurity researchers;

25) coordinate the activities of the national development institute in the field of cybersecurity;

26) file a claim in court to compel the subject to perform the actions specified in the order or act in the event of failure to comply with an order or act on the elimination of violations in terms of compliance with requirements in the areas of digitalization and cybersecurity within the specified time period;

27) process personal data, the security of which has been compromised, for the purpose of informing subjects of personal data on the “digital government” web portal through their personal account;

28) exercise other powers provided for by this Law, other laws of the Republic of Kazakhstan, acts of the President of the Republic of Kazakhstan and the Government of the Republic of Kazakhstan.

Footnote. Article 7-1 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 7-2. Competence of central executive bodies and state bodies directly subordinate and accountable to the President of the Republic of Kazakhstan in the field of cybersecurity

Central executive bodies and state bodies directly subordinate and accountable to the President of the Republic of Kazakhstan shall:

- 1) ensure compliance with uniform requirements in the areas of digitalization and cybersecurity;
- 2) ensure compliance with the basic principles of cyberculture recommended by the authorized body;
- 3) identify digital objects that are considered critically important digital objects within their area of competence;
- 4) provide workstations with access to digital objects for employees of the National Coordination Centre for Cybersecurity, with the exception of the authorized body for regulation, control and supervision of the financial market and financial organizations, special state bodies and the Armed Forces of the Republic of Kazakhstan;
- 5) exercise other powers provided for by this Law, other laws of the Republic of Kazakhstan and acts of the President of the Republic of Kazakhstan.

The competence of central executive bodies shall also be determined by acts of the Government of the Republic of Kazakhstan.

Footnote. Article 7-2 as amended by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 7-3. Competence of local executive bodies in the field of cybersecurity

Local executive bodies shall:

- 1) ensure compliance with uniform requirements in the areas of digitalization and cybersecurity, and data management requirements;
- 2) monitor the implementation of uniform requirements in the areas of digitalization and cybersecurity;
- 3) create conditions for improving cyberculture;
- 4) identify digital objects that are considered critically important digital objects within their competence;
- 5) exercise state control in the field of digitalization in relation to private business entities within the relevant administrative-territorial unit;
- 6) promote the development of the cybersecurity industry, including by attracting investment;
- 7) exercise, in the interests of local government, other powers assigned to local executive bodies by the legislation of the Republic of Kazakhstan.

2. Local executive bodies of the region, city of republican significance and the capital shall exercise state control over compliance with the requirements for electronic documents and electronic digital signatures, with the exception of sources of acquisition of the National Archives of the Republic of Kazakhstan and the central state archives;

Footnote. Article 7-3 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 7-4. State cybersecurity operation centre

1. State cybersecurity operation centre shall:

1) monitor the cybersecurity assurance of digital objects of the “digital government” through the cybersecurity monitoring system of the National cybersecurity coordination centre;

2) monitor cybersecurity events of digital objects of state bodies;

3) carry out measures to identify, prevent and investigate cybersecurity threats and incidents at digital facilities of the “digital government” and formulate recommendations for their elimination or prevention;

4) coordinate activities to ensure the cybersecurity of digital objects of the “digital government”, as well as responding to cybersecurity incidents;

5) ensure the functioning of the program of interaction with cybersecurity researchers on digital objects of state bodies;

6) carry out, together with the operator of the “digital government”, measures to ensure the cybersecurity of the “digital government” platform in accordance with the regulations for ensuring the cybersecurity of the “digital government” platform, approved by the authorized body in agreement with the National Security Committee of the Republic of Kazakhstan;

7) notify the authorized body in the field of personal data protection of a breach of personal data security within three hours from the moment of its discovery.

2. Employees of the State cybersecurity operations centre shall be responsible for the disclosure of commercial or other legally protected secrets obtained by them as a result of their activities, in accordance with the laws of the Republic of Kazakhstan.

Footnote. Article 7-4 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 7-5. Cybersecurity assurance centre

1. The cybersecurity assurance centre shall:

1) carry out activities to detect, assess, forecast, localize, neutralize and prevent cybersecurity threats to digital objects connected to the cybersecurity assurance centre;

2) take measures to minimize cybersecurity threats, immediately inform the owner and (or) holder of the digital object, as well as the National cybersecurity coordination centre, about the facts of identifying incidents and threats to cybersecurity;

3) monitor the cybersecurity of critically important digital objects that are not related to digital objects of the “digital government”;

4) exchange information necessary to ensure the cybersecurity of digital objects connected to the cybersecurity centre with the industry cybersecurity centre, the National cybersecurity coordination centre and other cybersecurity assurance centres;

5) collect, consolidate, analyse and store information about cybersecurity events and incidents;

6) provide owners and (or) holders of critically important digital objects with information necessary to ensure the cybersecurity of digital objects, including information on cybersecurity threats, vulnerabilities of software, devices and technologies, methods of implementing cybersecurity threats, prerequisites for the occurrence of cybersecurity incidents, as well as methods of preventing them and eliminating their consequences;

7) ensure the safety of restricted information that has become known to the cybersecurity assurance centre in the course of its activities;

8) provide the National cybersecurity coordination centre with access to events logs of digital objects of the “digital government” connected to the cybersecurity assurance centre;

9) have the right to create its own program of interaction with cybersecurity researchers or to purchase the service of using the program of interaction with cybersecurity researchers from third parties in accordance with the Civil Code of the Republic of Kazakhstan;

10) ensure cybersecurity of automated process control systems;

11) notify the authorized body in the field of personal data protection of a breach of personal data security within three hours from the moment of its discovery;

12) have the right, with the consent of the authorized body in the field of personal data protection, to process personal data, the security of which has been violated, for the purpose of informing subjects of personal data on the “digital government” web portal through their personal account;

13) conduct a national technical audit of data processing centres;

14) ensure compliance with uniform requirements in the areas of digitalization and cybersecurity at its digital facilities;

15) conduct cybersecurity audits;

16) monitor and log digital events of cybersecurity of digital objects, including those that collect and process personal data.

2. The cybersecurity assurance centre shall carry out its activities on the basis of a license to provide services for identifying technical channels of information leakage and special technical means intended for operational investigative activities.

3. Employees of the cybersecurity assurance centre shall be responsible for the disclosure of commercial or other legally protected secrets obtained by them as a result of their activities, in accordance with the laws of the Republic of Kazakhstan.

4. The requirement of paragraph 2 of this Article shall not apply to law enforcement and special state bodies of the Republic of Kazakhstan, second-tier banks of the Republic of Kazakhstan, in which the functions of the cybersecurity assurance centre are carried out by their structural divisions.

Footnote. Article 7-5 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 7-6. Competence of the authorized body in the field of electronic industry

Footnote. Article 7-6 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 7-7. National service for cybersecurity computer incidents response

1. National service for cybersecurity computer incidents response shall:

1) carry out inter-sectoral coordination on issues of monitoring the provision of cybersecurity, protection and secure operation of digital objects of the “digital government”, the Kazakhstani segment of the Internet, as well as critically important digital objects, responding to cybersecurity incidents with the implementation of joint measures to ensure cybersecurity in the manner established by the legislation of the Republic of Kazakhstan;

2) assist owners, holders and users of digital objects on issues of ensuring cybersecurity;

3) notify the authorized body in the field of personal data protection of a breach of personal data security within three hours from the moment of its discovery.

2. Employees of the National service for cybersecurity computer incidents response shall be responsible for the disclosure of commercial or other legally protected secrets obtained by them as a result of their activities, in accordance with the laws of the Republic of Kazakhstan.

Footnote. Article 7-7 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 7-8. Cybersecurity incidents response service

1. Cybersecurity incidents response service shall:

1) collect and analyse information on cybersecurity incidents and current cybersecurity threats, and provide recommendations for their elimination;

2) develop recommendations aimed at countering cybersecurity threats;

3) inform owners and holders of digital objects, as well as the National cybersecurity coordination centre, about known incidents and threats to cybersecurity;

4) have the right to create its own program of interaction with cybersecurity researchers or to purchase the service of using the program of interaction with cybersecurity researchers from third parties in accordance with the Civil Code of the Republic of Kazakhstan;

5) notify the authorized body in the field of personal data protection of a breach of personal data security within three hours from the moment of its discovery;

6) ensure compliance with uniform requirements in the areas of digitalization and cybersecurity at its digital facilities.

2. The cybersecurity incidents response service shall operate under a license to provide services for identifying technical channels of information leakage and special technical means intended for operational investigative activities.

3. Employees of the cybersecurity incidents response service shall be responsible for the disclosure of commercial or other legally protected secrets obtained by them as a result of their activities, in accordance with the laws of the Republic of Kazakhstan.

4. The requirement of paragraph 2 of this Article shall not apply to second-tier banks of the Republic of Kazakhstan, in which the functions of the cybersecurity incident response service are carried out by their structural divisions.

Footnote. Articles 7-8 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 8. Expert council

Footnote. Article 8 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 9. National cybersecurity coordination centre

1. National cybersecurity coordination centre shall:

1) collect, analyse, and summarize information from industry cybersecurity centres and cybersecurity support centres on cybersecurity incidents at digital objects of the “digital government” and critically important digital objects;

2) implement the tasks and functions of the National service for cybersecurity computer incidents response;

3) implement the tasks and functions of the State cybersecurity operation centre;

4) notify the authorized body in the field of personal data protection of a breach of personal data security within three hours from the moment of its discovery.

2. Employees of the National cybersecurity coordination centre shall be responsible for the disclosure of commercial or other legally protected secrets obtained by them as a result of their activities, in accordance with the laws of the Republic of Kazakhstan.

Footnote. Article 9 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 9-1. Information security licensing

Footnote. Article 9-1 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 10. Sectoral cybersecurity centre

1. The sectoral cybersecurity centre shall organise and coordinate the provision of cybersecurity by the owners or operators of digital objects in the respective sector (area) of state regulation, and also:

1) carry out activities to analyse, assess, forecast and prevent cybersecurity threats to organisations;

2) exchange information necessary to ensure cybersecurity with the National cybersecurity coordination centre;

3) collect, consolidate, analyse, and store information on cybersecurity events and incidents received from owners or holders of digital objects in the relevant sector (sphere);

4) provide information necessary to ensure cybersecurity to owners or holders of digital objects of the relevant sector (sphere), including information on cybersecurity threats, vulnerabilities in digital objects of the relevant sector (sphere), prerequisites for the occurrence of cybersecurity incidents, as well as methods for their prevention and elimination of consequences;

5) ensure the safety of restricted information that has become known to the sectoral cybersecurity centre in the course of its activities;

6) notify the authorized body in the field of personal data protection of a breach of personal data security within three hours from the moment of its discovery;

7) coordinate the provision of cybersecurity for automated process control systems and process control systems that are part of critically important digital facilities, in the manner and within the timeframes established by the internal regulations of the industry cybersecurity centre;

8) develop, on the basis of uniform requirements in the areas of digitalization and cybersecurity, additional requirements for ensuring cybersecurity in the relevant sector (sphere) of state regulation.

2. Employees of the sectoral cybersecurity centre shall be responsible for the disclosure of commercial, banking or other legally protected secrets obtained by them as a result of their activities, in accordance with the laws of the Republic of Kazakhstan.

3. The sectoral cybersecurity centre, in order to carry out its functions, uses a digital object for collecting, processing, and exchanging information on cybersecurity events and incidents, the procedure for connecting to and using which by sectoral organizations shall be determined by the authorized body of the relevant sector (sphere) of state regulation.

Footnote. Article 10 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 11. National institute of development in the field of information and communication technologies

Footnote. Article 11 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 12. Service integrator of "electronic government"

Footnote. Article 12 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 13. Operator

Footnote. Article 13 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 13-1. International technological park "Astana Hub"

Footnote. Chapter 2 is supplemented by Article 13-1, in accordance with the Law of the Republic of Kazakhstan dated 04.07.2018 № 174-VI (shall be enforced upon expiry of ten calendar days after its first official publication); excluded by the Law of the Republic of Kazakhstan dated 27.09.2025 № 220-VIII (effective ten calendar days after the date of its first official publication).

Article 13-2. Competence of the operator of the national artificial intelligence platform

Footnote. Chapter 2 is supplemented by Article 13-2 in accordance with the Law of the Republic of Kazakhstan dated 02.01.2021 № 399-VI (shall be enforced ten calendar days after the day of its first official publication); as excluded by the Law of the Republic of Kazakhstan dated 17.11.2025 № 231-VIII (shall enter into force upon expiry of sixty calendar days after the day of its first official publication).

Article 13-3. Data processing center

Footnote. Article 13-3 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 13-4. Cloud computing

Footnote. Article 13-4 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 14. State technical service

1. The state technical service shall carry out the following activities in the areas of digitalization and cybersecurity, which are classified as a state monopoly:

1) ensures the functioning of a unified Internet access gateway and a unified e-mail gateway for the “digital government”;

2) conducts testing for compliance with cybersecurity requirements of digital objects of the “digital government”;

3) carries out an examination of the investment proposal and the financial and economic justification of budget investments and the technical specifications for the creation or development of a digital object of the “digital government” for compliance with cybersecurity requirements;

4) monitors Internet resources, as well as monitors the functioning of the domain name system in the space of the Kazakhstan segment of the Internet;

5) implements the tasks and functions of the National cybersecurity coordination centre;

6) administers access rights, monitors the functioning and monitors the cybersecurity of the National video monitoring system;

7) carries out an inspection of the security of the processes of storage, processing and distribution of personal data contained in digital objects;

8) ensures the functioning of digital objects of the National cybersecurity coordination centre;

9) ensures the functioning of a unified national backup platform for storing digital resources, establishes the frequency of backup copies of digital resources of critically important digital objects in the manner determined by the authorized body;

10) participates in the implementation of state control in the field of digitalization;

11) provides services for using the National source codes repository;

2. Prices for the goods (works, services) specified in paragraph 1 of this Article, produced and (or) sold by the state technical service, shall be established by the National Security Committee of the Republic of Kazakhstan in agreement with the antimonopoly authority.

Footnote. Article 14 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 14-1. National institute for development in the sphere of cybersecurity

National institute for development in the sphere of cybersecurity shall:

1) participate in the implementation of state policy in the field of cybersecurity;

2) develop documents on standardization in the field of cybersecurity;

3) carry out scientific and technical activities in the field of cybersecurity;

4) conduct scientific and technical expertise of projects in the field of cybersecurity;

5) carry out training, retraining and advanced training in the field of cybersecurity.

Footnote. Article 14-1 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 15. Single contact center

Footnote. Article 15 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Chapter 3. Rights and obligations of owners and holders of digital objects in the field of cybersecurity, obligations of the owner and (or) holder of critical digital objects

Footnote. The title of Chapter 3 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 16. Rights and obligations of owners of digital objects

1. The owner of digital objects shall have the right to:
 - 1) transfer digital objects for lease, trust management, economic management or operational management and otherwise dispose of them;
 - 2) establish, within the limits of its competence, the regime and rules for processing, protection and access to digital objects;
 - 3) determine the conditions for the disposal of digital objects during their storage, copying and distribution;
 - 4) determine the conditions of ownership and use of digital objects;
 - 5) enjoy other rights established by this Law and the laws of the Republic of Kazakhstan.
2. The owner of digital objects shall be obliged to:
 - 1) ensure cybersecurity of digital objects;
 - 2) distribute, provide, restrict or prohibit access to digital resources and digital infrastructure objects in accordance with this Law and other laws of the Republic of Kazakhstan;
 - 3) perform other duties in accordance with this Law and other laws of the Republic of Kazakhstan.
3. The owner of a digital object containing personal data shall be obliged to take measures stipulated by the legislation of the Republic of Kazakhstan on personal data and their protection.
4. The owner of a digital object shall be responsible to the owner and (or) holder of digital resources for the security of storage and protection of digital resources located on digital objects owned by him.

Footnote. Article 16 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 17. Rights and obligations of the owner of digital objects

1. The owner of a digital object shall have the right to:
 - 1) own and use digital objects under the conditions determined by the owner;
 - 2) determine the conditions of access and use of digital objects in accordance with subparagraph 1) of this paragraph;
 - 3) determine the conditions for processing digital resources in a digital system;
 - 4) enjoy other rights established by this Law and the laws of the Republic of Kazakhstan.

2. The owner of digital objects shall be obliged to:

- 1) ensure cybersecurity of digital objects;
- 2) respect the rights, freedoms and legitimate interests of the owner of digital objects and third parties;
- 3) perform other duties in accordance with this Law and other laws of the Republic of Kazakhstan.

3. The owner of a digital object containing personal data shall be obliged to take measures stipulated by the legislation of the Republic of Kazakhstan on personal data and their protection.

4. The owner of a digital object shall be responsible to the owner and (or) holder of digital resources, digital objects for the security of storage and protection of digital resources, digital objects located on objects belonging to him.

Footnote. Article 17 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 18. Obligations of the owner and (or) holder of critically important digital objects

1. The owner or holder of critically important digital objects shall be obliged to:

- 1) create own cybersecurity centre and ensure its functioning or purchase the services of a cybersecurity centre from third parties in accordance with the Civil Code of the Republic of Kazakhstan in the volume (in the set) established by uniform requirements in the areas of digitalization and cybersecurity;

- 2) ensure for critically important digital objects that are digital objects of the “digital government,” the connection of cybersecurity digital events logging systems to the technical means of the cybersecurity monitoring system of the National cybersecurity coordination centre is ensured independently or by purchasing services from third parties in accordance with the civil legislation of the Republic of Kazakhstan;

- 3) notify the National cybersecurity coordination centre and the cybersecurity centre to which critical digital objects are connected about independently identified cybersecurity incidents in the manner and within the timeframes determined by the rules for monitoring the cybersecurity of digital objects of the “digital government” and critically important digital objects, unless otherwise established by the laws of the Republic of Kazakhstan;

- 4) transfer backup copies of digital resources to a unified national backup platform for storing digital resources in the manner and within the timeframes determined by the authorized body, unless otherwise established by the laws of the Republic of Kazakhstan.

Access to a copy of digital resources stored on the unified national digital resource storage platform shall be prohibited, except by the owner or holder of the digital resource.

2. The owner and/or holder of critically important digital objects processing data containing legally protected secrets shall conduct a cybersecurity audit at least once a year.

Cybersecurity audit of second-tier banks shall be conducted in accordance with the requirements of the banking legislation of the Republic of Kazakhstan.

Footnote. Article 18 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 18-1. Rights and obligations of the owner and possessor of an intelligent robot

Footnote. Chapter 3 is supplemented by Article 18-1 in accordance with the Law of the Republic of Kazakhstan dated 25.06.2020 № 347-VI (shall be enforced ten calendar days after the day of its first official publication); as excluded by the Law of the Republic of Kazakhstan dated 17.11.2025 № 231-VIII (shall enter into force upon expiry of sixty calendar days after the day of its first official publication).

Article 18-2. Activities of a foreign online platform and instant messaging service on the territory of the Republic of Kazakhstan

Footnote. Chapter 3 as amended by Article 18-2 in accordance with the Law of the Republic of Kazakhstan dated 03.05.2022 № 118-VII (shall be enforced upon expiry of sixty calendar days after the day of its first official publication); is excluded by the Law of the Republic of Kazakhstan dated 10.07.2023 № 19-VIII (shall be enforced sixty calendar days after the date of its first official publication).

Article 19. Types of services provided in electronic form

Footnote. Article 19 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 20. Submission of information in provision of services in electronic form

Footnote. Article 20 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 20-1. Use of a simple electronic signature

1. A simple electronic signature is an electronic digital form of confirmation of a person's signature through the use of codes, passwords or other means of identification.

2. Entities of private entrepreneurship, when interacting with foreigners, foreign legal entities, legal entities with foreign participation, have the right to use a simple electronic signature.

3. Transactions certified by a simple electronic signature of a person authorized to sign them, are equivalent to signed documents on paper, with the exception of transactions subject to notarization or mandatory state registration in accordance with the legislation of the Republic of Kazakhstan, and transactions, the list of which is approved by the authorized body, subject to the following conditions:

1) the parties to the transaction have reached an agreement in writing on the use of a simple electronic signature when concluding transactions between them;

2) the parties to the transaction, by an agreement between them in writing, recognize the authenticity and validity of the transactions concluded between them by means of a simple electronic signature.

The requirements of this article shall be valid within the framework of the pilot project until July 1, 2026.

Footnote. Chapter 3 is supplemented by Article 20-1 in accordance with the Law of the Republic of Kazakhstan dated May 21, 2024 № 86-VIII (shall come into force sixty calendar days after the day of its first official publication).

SECTION 2.

Footnote. The title of Section 2 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Chapter 4. Subjects and objects of cybersecurity assurance

Footnote. The title of Chapter 4 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 21. The operation of "electronic government"

Footnote. Article 21 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 22. Architecture of the "electronic government"

Footnote. Article 22 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 23. Architecture of state agency

Footnote. Article 23 excluded by the Law of the Republic of Kazakhstan dated 14.07.2022 № 141-VII (shall be enforced from 01.01.2023).

Article 24. Standard architecture of "electronic akimat"

Footnote. Article 24 excluded by the Law of the Republic of Kazakhstan dated 14.07.2022 № 141-VII (shall be enforced from 01.01.2023).

Article 25. Automation of state functions and provision of state services resulting from them

Footnote. Article 25 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 26. Information and communication platform of "electronic government"

Footnote. Article 26 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 27. Web portal of “electronic government”

Footnote. Article 27 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 28. Payment gateway of "electronic government"

Footnote. Article 28 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 28-1. Cybersecurity researcher

1. A cybersecurity researcher shall:
 - 1) search for vulnerabilities within the boundaries established by the owner and (or) holder of the digital object;
 - 2) submit a report describing the identified vulnerabilities;
 - 3) inform owners and (or) holders of digital objects about identified vulnerabilities;
 - 4) not disclose information about the identified vulnerability until it is completely eliminated and officially authorized by the owner and (or) holder of the digital object;
 - 5) not use discovered vulnerabilities for personal or illegal purposes;
 - 6) not disrupt the normal functioning of the digital object when searching for vulnerabilities.
2. A cybersecurity researcher shall be responsible for the disclosure of commercial or other legally protected secrets obtained by him/her as a result of his/her activities, in accordance with the laws of the Republic of Kazakhstan.

Footnote. Article 28-1 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 28-2. Licensing in the field of cybersecurity

1. Activities in the field of cybersecurity shall be subject to licensing in accordance with the procedure established by the legislation of the Republic of Kazakhstan on permits and notifications.
2. Licensees in the field of cybersecurity shall submit to the licensor reports, notifications, the list, forms and frequency of which are determined by the licensor within the framework of the qualification requirements.

Footnote. Article 28-2 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 29. Unified transport environment of state bodies

1. The unified transport environment of state bodies is a telecommunications network that forms part of the “digital government” infrastructure and is intended to ensure interaction among local telecommunications networks (except for local networks having access to the Internet), departmental and corporate telecommunications networks of state bodies, their subordinate organizations and local self-government bodies, as well as other digital ecosystem entities designated by the authorized body, while maintaining the required level of cybersecurity.

2. State bodies, their subordinate organizations and local government bodies, as well as other entities of the digital environment determined by the authorized body, shall be required to use exclusively the unified transport environment of state bodies for the interaction of local (except for local networks having access to the Internet), departmental and corporate networks.

3. In order to ensure cybersecurity, the connection of local, departmental and corporate networks connected to the unified transport environment of state bodies to public telecommunications networks and other telecommunications networks shall be carried out in accordance with uniform requirements in the areas of digitalization and cybersecurity.

Footnote. Article 29 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 30. Unified Internet access gateway and unified e-mail gateway for the “digital government”

1. Connection of digital objects of state bodies, local government bodies, state legal entities, quasi-public sector entities, as well as owners or holders of critically important digital objects to the Internet shall be carried out by communications operators through a unified Internet access gateway.

2. Connecting digital objects of state bodies and local governments to the Internet shall be carried out in accordance with uniform requirements in the areas of digitalization and cybersecurity.

3. For operational purposes, special state and law enforcement agencies of the Republic of Kazakhstan and military intelligence agencies of the Ministry of Defence of the Republic of Kazakhstan, as well as the National Bank of the Republic of Kazakhstan, may organize connections to the Internet without using a unified Internet access gateway.

The authorized body for regulation, control and supervision of the financial market and financial organizations may organize Internet connections without the use of a unified Internet access gateway, taking into account the implementation of the functions of the industry cybersecurity centre.

4. Electronic interaction between the email of state bodies and owners and (or) holders of critically important digital objects and the external email of other persons shall be carried out by redirecting electronic messages.

Footnote. Article 30 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 30-1. National video monitoring system

1. The National video monitoring system is a digital system that is a set of software and hardware tools that collect, process, and store video images to address the challenges of ensuring national security and public order.

2. It shall not be permitted to use information obtained by the National video monitoring system to solve problems not provided for in paragraph 1 of this Article.

3. The categories of objects subject to mandatory connection to the National video monitoring system shall be:

- 1) video surveillance systems of central state and local executive bodies;
- 2) video surveillance systems for objects vulnerable to terrorism;
- 3) video surveillance systems for public and road safety.

The list of objects subject to mandatory connection to the National video monitoring system shall be determined by the National Security Committee of the Republic of Kazakhstan in agreement with the State Security Service of the Republic of Kazakhstan.

4. The users of the National video monitoring system shall be special state bodies and internal affairs agencies of the Republic of Kazakhstan.

The list of services, divisions and categories of employees entitled to use the National video monitoring system shall be determined by the heads of special state bodies and internal affairs agencies of the Republic of Kazakhstan.

Information obtained as a result of the operation of the National video monitoring system may be provided to other state bodies in cases established by the laws of the Republic of Kazakhstan.

5. The rules for the operation of the National video monitoring system shall be approved by the National Security Committee of the Republic of Kazakhstan.

Footnote. Article 30-1 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 30-2. Logging of digital events

1. Digital events logging shall be ensured through the collection, recording, storage, and preservation of the integrity of digital events logs.

2. Digital events logging shall be used to ensure the monitoring, analysis, and storage of digital events logs generated as a result of actions performed by users with privileged rights within the digital objects of state bodies and within the digital objects of other entities that are used by state bodies for the digitalization of their activities.

3. The procedure for carrying out digital events logging shall be determined by the authorized body.

The Law has been supplemented by Article 30-2 in accordance with the Law of the Republic of Kazakhstan dated 09.01.2026, № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 31. Architectural portal of "electronic government"

Footnote. Article 31 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Chapter 5.

Footnote. The title of Chapter 5 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 32. Types of electronic information resources

Footnote. Article 32 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 33. Legal regime of electronic information resources

Footnote. Article 33 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 33-1. Legal regime of circulation of digital assets

Footnote. Chapter 5 is supplemented by Article 33-1 in accordance with the Law of the Republic of Kazakhstan dated 25.06.2020 № 347-VI (shall be enforced ten calendar days after the day of its first official publication); excluded by the Law of the Republic of Kazakhstan dated 06.02.2023 № 194-VII (shall be enforced from 01.04.2023).

Article 34. Formation and use of electronic information resources

Footnote. Article 34 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 35. Access to electronic information resources

Footnote. Article 35 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 36. Electronic information resources containing personal data

Footnote. Article 36 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Chapter 6.

Footnote. The title of Chapter 6 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 37. Types of information systems

Footnote. Article 37 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 38. Cybersecurity requirements for the digital object of the "digital government"

1. The digital object of the “digital government” shall be created, operated and developed in accordance with the legislation of the Republic of Kazakhstan, the standards in force in the territory of the Republic of Kazakhstan, the life cycle of the digital object of the “digital government” and taking into account the provision of:

- 1) uniform requirements in the areas of digitalization and cybersecurity;
- 2) the architecture of the “digital government”, as well as data management requirements;
- 3) integration (if necessary) with other digital objects of the “digital government”;
- 4) information interaction of the digital object of the “digital government” with the cybersecurity event monitoring system of the National cybersecurity coordination centre;
- 5) creation of an in-house cybersecurity centre and ensuring its operation or acquisition of cybersecurity centre services from third parties in accordance with the Civil Code of the Republic of Kazakhstan in the volume (set) established by uniform requirements in the areas of digitalization and cybersecurity;
- 6) the priority of free software;
- 7) assignment of a class in accordance with the classifier;
- 8) access for users with disabilities.

2. The digital system of a state legal entity and a non-state digital system intended for the formation of state digital resources shall be created, operated and developed in accordance with the legislation of the Republic of Kazakhstan, the standards in force in the territory of the Republic of Kazakhstan, the life cycle of the digital system and subject to the fulfilment of the following requirements:

- 1) technical specifications agreed upon with the authorized body and the authorized body in the field of digitalization;
- 2) testing reports with positive testing results for compliance with cybersecurity requirements;
- 3) integration of the digital system of a state body with a non-governmental digital system only through an external “digital government” gateway put into industrial operation;
- 4) uniform requirements in the areas of digitalization and cybersecurity.

3. Information contained in the digital resource, regulatory and technical documentation, as well as other related documents of the digital system of state bodies shall be created and stored in Kazakh and Russian.

4. The owner or holder of the digital system of a state body or a person authorized by him/her shall provide the National cybersecurity coordination centre with access to the digital system of the state body at its location for the purpose of monitoring cybersecurity.

Footnote. Article 38 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 39. Creation and development of the objects of informatization of "electronic government"

Footnote. Article 39 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 39-1. The order of creation and development of the information system of special state bodies of the Republic of Kazakhstan

Footnote. Article 39-1 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 40. Industrial operation of the object of informatization of "electronic government"

Footnote. Article 40 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 41. Termination of industrial operation of the object of informatization of "electronic government"

Footnote. Article 41 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 41-1. Write-off of objects of informatization of "electronic government"

Footnote. Article 41-1 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 42. Mandatory requirements for the means of processing, storing and backing up digital resources in the digital infrastructure of the "digital government"

1. To ensure the reliability and security of functioning of digital infrastructure objects of the "digital government", the technical means used for storing, processing and transmitting digital resources must comply with the requirements of the legislation of the Republic of Kazakhstan in the field of technical regulation.

2. The owner or holder of a digital infrastructure object of the digital government, as well as the operator of the digital government, shall store and, if necessary, ensure the restoration of state digital resources contained in digital infrastructure objects of the digital government, and shall be responsible for the loss, modification, or other failure to ensure the safety of state digital resources in the manner established by the laws of the Republic of Kazakhstan and with the agreement of the parties.

3. Ensuring the production of a backup copy of state digital resources shall be mandatory for the owner and holder of a digital infrastructure object of the “digital government” or the operator of the “digital government”.

The method for producing and storing a backup copy containing state digital resources must ensure the safety of the digital resources until the next backup copy is produced.

The frequency of backups of state digital resources shall be established by the technical documentation for the digital object of the "digital government".

Footnote. Article 42 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 43. Integration of the objects of informatization of “e-government”

Footnote. Article 43 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 44. Requirements for non-state information system that is integrated with the information system of state body

Footnote. Article 44 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Chapter 7. SERVICE MODEL OF INFORMATIZATION

Footnote. Chapter 7 excluded by the Law of the Republic of Kazakhstan dated 14.07.2022 № 141-VII (shall be enforced from 01.01.2023).

Chapter 8. TESTS AND AUDIT OF THE OBJECTS OF INFORMATIZATION

Footnote. The title of chapter 8 is in the wording of the Law of the Republic of Kazakhstan dated 18.03.2019 № 237-VI (shall be enforced upon expiry of ten calendar days after its first official publication).

Article 48. Documentation of electronic information resources and data (information) about the objects of informatization of "electronic government"

Footnote. Article 48 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 49. Testing for compliance with cybersecurity requirements

1. Testing of digital objects for compliance with cybersecurity requirements shall be carried out on a mandatory basis and/or at the initiative of the owner or holder.

2. Testing objects subject to mandatory testing for compliance with cybersecurity requirements include:

- 1) platform software product;
- 2) “digital government” platform;
- 3) the Internet resource of a state body, state legal entity, or quasi-public sector entity;
- 4) digital system of a state body, state legal entity, or quasi-public sector entity;
- 5) critically important digital objects;
- 6) a non-governmental digital system designed to form state digital resources, implement state functions and provide state services.

3. The digital system of a state body and a non-governmental digital system shall not be required to undergo testing for compliance with cybersecurity requirements in order to use the services of the national certification authority of the Republic of Kazakhstan to verify the authenticity of an electronic digital signature.

4. Testing of digital objects (except for digital objects whose owner (holder) and/or customer is a state body) for compliance with cybersecurity requirements shall be carried out by accredited testing laboratories in accordance with this Law and the legislation of the Republic of Kazakhstan in the field of technical regulation.

5. Testing of digital objects for the purpose of assessing their quality shall be carried out in accordance with the legislation of the Republic of Kazakhstan in the field of technical regulation.

Footnote. Article 49 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 50. Cybersecurity audit

1. Cybersecurity audit of digital objects shall be carried out at the initiative of their owner and (or) holder.

2. The owner and (or) holder of digital objects shall have the right to conduct an internal audit or purchase a service in accordance with the Civil Code of the Republic of Kazakhstan from legal entities licensed in the field of cybersecurity.

3. The owner of critically important digital objects or digital objects processing digital data containing legally protected secrets shall conduct a cybersecurity audit at least once a year. The audit results shall be sent to the authorized body and the National cybersecurity coordination centre.

Footnote. Article 50 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 51. Attestation

Footnote. Article 51 is excluded by the Law of the Republic of Kazakhstan dated 18.03.2019 № 237-VI (shall be enforced upon expiry of ten calendar days after its first official publication).

Article 52. Confirmation of conformity in the digital environment

Confirmation of conformity in the digital environment shall be carried out in accordance with the legislation of the Republic of Kazakhstan in the field of technical regulation.

Footnote. Article 52 as amended by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Chapter 9. Protection of digital objects

Footnote. The title of Chapter 9 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 53. Objectives of protecting digital objects

1. Protection of digital objects is the implementation of a set of legal, organizational and technical measures aimed at preserving digital objects, preventing unauthorized and (or) unintentional access and (or) impact on them.

2. The protection of digital objects shall be carried out in accordance with the legislation of the Republic of Kazakhstan and the standards in force in the territory of the Republic of Kazakhstan for the purposes of:

- 1) ensuring the operation of digital resources;
 - 2) ensuring the confidentiality of digital resources with limited access;
 - 3) implementation of the right of cybersecurity subjects to access digital resources;
 - 4) preventing unauthorized and/or unintentional access, leakage and other actions in relation to digital resources, as well as unauthorized and/or unintentional impact on digital infrastructure objects;
 - 5) preventing disruptions in the functioning of digital objects and critically important digital objects;
 - 6) preventing unauthorized and (or) unintentional access to service information about subscribers of telecommunications networks and telecommunications messages;
 - 7) preventing unauthorized and (or) unintentional blocking of the operation of subscriber devices of telecommunication networks.
3. Other unauthorized and (or) unintentional actions in relation to digital objects shall be:

- 1) blocking of digital resources and digital infrastructure objects, committed in the form of actions leading to the restriction or closure of access to them;
- 2) unauthorized and (or) unintentional modification of digital objects;
- 3) unauthorized and (or) unintentional copying of digital resources;
- 4) unauthorized and (or) unintentional destruction, loss of digital resources;
- 5) disruption of digital objects;
- 6) use of malicious software.

4. Protection of digital objects shall be carried out according to the class assigned in accordance with the classifier.

Footnote. Article 53 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 54. Organization of digital objects protection

1. Protection of digital objects shall be carried out:
 - 1) in relation to digital resources – by their owners, holders and users;
 - 2) in relation to digital infrastructure objects and critically important digital objects – by their owners or holders.
2. Owners or holders of digital infrastructure objects of the “digital government” and critically important digital objects shall be obliged to take measures to ensure:
 - 1) prevention of unauthorized access;
 - 2) timely detection of facts of unauthorized access, if such unauthorized access could not be prevented;
 - 3) minimizing the adverse consequences of violation of the access order;
 - 4) preventing unauthorized influence on the means of processing and transmitting digital resources;
 - 5) elimination of cybersecurity incidents and vulnerabilities;
 - 6) prompt restoration of digital resources modified or destroyed due to unauthorized access to them;
 - 7) immediate notification of the National cybersecurity coordination centre about a cybersecurity incident that has occurred, followed by sending digital data on the measures taken to eliminate the cybersecurity incident, with the exception of owners and (or) holders of digital resources containing information constituting state secrets;
 - 8) information interaction with the National cybersecurity coordination centre on issues of monitoring the cybersecurity of digital objects of the “digital government”;
 - 9) providing access to the National cybersecurity coordination centre to digital objects of the “digital government” and to cybersecurity centres to critically important digital objects for the purpose of conducting organizational and technical measures aimed at implementing monitoring of cybersecurity in accordance with the rules for monitoring the cybersecurity of digital objects of the “digital government” and critically important digital objects.

3. Owners or holders of digital objects of state bodies shall be obliged to take measures to ensure:

1) participation of digital objects with Internet access in the program of interaction with cybersecurity researchers for digital objects of the “digital government”;

2) eliminating vulnerabilities identified through the program of interaction with cybersecurity researchers for digital objects of the “digital government”;

3) performance of other duties in accordance with this Law and other laws of the Republic of Kazakhstan.

4. Owners or holders of non-state digital objects intended for the digitalization of the activities of state bodies, prior to integration with digital objects of state bodies shall:

1) take measures to ensure compliance with uniform requirements in the areas of digitalization and cybersecurity;

2) create their own cybersecurity centre and ensure its functioning or acquire the services of a cybersecurity centre from third parties in accordance with the Civil Code of the Republic of Kazakhstan.

5. Owners or holders of critically important digital objects, with the exception of state bodies, local government bodies, state legal entities, and quasi-public sector entities, within six months from the date of inclusion in the list of critically important digital objects shall:

1) take measures to comply with uniform requirements in the areas of digitalization and cybersecurity related to the field of cybersecurity;

2) create their own cybersecurity centre and ensure its functioning or acquire the services of a cybersecurity centre from third parties in accordance with the Civil Code of the Republic of Kazakhstan;

3) undergo a testing procedure for compliance with cybersecurity requirements;

4) provide information on the conducted cybersecurity audit to the authorized body in the field of cybersecurity.

6. Management of Internet resources and digital infrastructure objects during emergency situations of social, natural and man-made nature, the introduction of a state of emergency or martial law shall be carried out by an authorized body in accordance with the legislation of the Republic of Kazakhstan.

Footnote. Article 54 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 54-1. Uniform requirements in the areas of digitalization and cybersecurity

1. Uniform requirements in the areas of digitalization and cybersecurity shall be approved by the resolution of the Government of the Republic of Kazakhstan.

2. The provisions of the uniform requirements in the areas of digitalization and cybersecurity related to the area of cybersecurity shall be mandatory for application by state bodies, local government bodies, state legal entities, quasi-public sector entities, owners and

holders of non-state digital objects integrated with digital objects of state bodies or intended for the formation of state digital resources, as well as owners and holders of critically important digital objects.

3. The provisions of the uniform requirements in the areas of digitalization and cybersecurity shall not apply to digital systems in a secure design classified as state secrets, digital objects containing information constituting state secrets, as well as special-purpose telecommunications networks and (or) presidential, governmental and secure communications

Footnote. The Law has been supplemented by Article 54-1 in accordance with the Law of the Republic of Kazakhstan dated 09.01.2026, № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 55. Measures for the protection of digital objects

1. Legal measures for the protection of digital objects shall include:

- 1) the requirements of the legislation of the Republic of Kazakhstan and the standards in the field of digitalization in force in the territory of the Republic of Kazakhstan;
- 2) liability for violation of the digital legislation of the Republic of Kazakhstan;
- 3) agreements concluded by the owner or holder of digital objects, which establish the conditions of operation, access or use of these objects, as well as liability for their violation.

2. Organizational measures for the protection of digital objects shall include establishing and ensuring access control to the territory (buildings, premises) where access to digital objects can be achieved, as well as restricting access to them.

3. Technical (software and hardware) measures for protecting digital objects shall include:

- 1) the use of information security tools, and in relation to information constituting state secrets – exclusively with the use of information security tools constituting state secrets, developed, manufactured and (or) accepted into operation in accordance with the legislation of the Republic of Kazakhstan;
- 2) use of access control systems and registration of access to digital objects;
- 3) development of a security assignment to determine protection measures by owners or holders of digital objects based on approved security profiles.

4. The use of technical (software and hardware) measures to protect digital objects must not cause harm or create a threat of harm to the life, health and property of individuals, as well as the property of legal entities and state property.

Footnote. Article 55 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 56. Protection of digital resources containing personal data

Owners and holders of digital systems containing personal data, the owner and (or) operator of the database containing personal data, as well as third parties, shall be obliged to

take measures to protect them in accordance with this Law and the legislation of the Republic of Kazakhstan on personal data and their protection.

This obligation arises from the moment of receipt of digital resources containing personal data, or the collection of personal data, until their destruction or depersonalization.

Footnote. Article 56 as amended by the Law of the Republic of Kazakhstan dated June 25, 2020 № 347-VI (shall be enforced ten calendar days after the day of its first official publication); dated 06.04.2024 № 71-VIII (shall be enforced upon expiry of sixty calendar days after the day of its first official publication); dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months from the date of its first official publication).

Article 56-1. Protection of domain names in the space of the Kazakhstan segment of the Internet

1. Internet resource with registered domain names. KZ and (or). KAZ is placed in the space of the Kazakhstan segment of the Internet.

2. The use of .KZ and (or). KAZ domain names in the space of the Kazakhstan segment of the Internet when transmitting data by Internet resources is carried out using security certificates.

Footnote. Chapter 9 is supplemented by Article 56-1 in accordance with the Law of the Republic of Kazakhstan dated 25.06.2020 № 347-VI (shall be enforced ten calendar days after the day of its first official publication).

SECTION 3.

Footnote. The title of Section 3 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Chapter 10. EXPERTISE AND COORDINATION OF DOCUMENTS

Footnote. The title of Chapter 10 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 57. Conclusions in the sphere of informatization and information security ensuring

Footnote. Article 57 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 58. Conclusion of the expertise in the field of informatization for technical and economic justification or financial and economic justification for budget investments

Footnote. Article 58 is excluded by the Law of the Republic of Kazakhstan dated 18.03.2019 № 237-VI (shall be enforced upon expiry of ten calendar days after its first official publication).

Article 59. Coordination of technical documentation and documentation on public-private partnership projects in the areas of digital environment and cybersecurity

1. The approval of the technical specifications for the creation and development of a digital object of the "digital government" shall be carried out by the authorized body in the field of cybersecurity in the manner and within the timeframes determined by the rules for the preparation and review of technical specifications for the creation and development of digital objects of the "digital government", approved by the authorized body in the field of digitalization.

2. Excluded by the Law of the Republic of Kazakhstan dated 14.07.2022 № 141-VII (shall be enforced from 01.01.2023).

3. When creating and developing digital objects of the "digital government" within the framework of national and local public-private partnership projects in the field of digitalization, in accordance with the legislation of the Republic of Kazakhstan in the field of public-private partnership, the authorized body in the field of cybersecurity shall approve the tender documentation of the public-private partnership project, the business plan for the public-private partnership project during direct negotiations to determine the private partner.

Footnote. Article 59 is in the wording of the Law of the Republic of Kazakhstan dated 18.03.2019 № 237-VI (shall be enforced upon expiry of ten calendar days after its first official publication); as amended by the Law of the Republic of Kazakhstan dated 25.06.2020 № 347-VI (shall be enforced ten calendar days after the day of its first official publication); dated 14.07.2022 № 141-VII (shall be enforced from 01.01.2023); dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months from the date of its first official publication).

Article 60. Conclusion of the authorized body on the calculation of costs for state procurement of goods, works and services in the field of informatization

Footnote. Article 60 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Chapter 10-1. State control in the field of digitalization, as well as compliance with requirements for electronic documents and electronic digital signatures

Footnote. The Law has been supplemented with Chapter 10-1 in accordance with the Law of the Republic of Kazakhstan dated 09.01.2026, № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 60-1. State control in the field of digitalization

1. State control in the field of digitalization shall be carried out in the form of inspections, preventive control with a visit to the subject (object) of control, and preventive control without a visit to the subject (object) of control.

2. Inspection and preventive control with a visit to the subject (object) of control shall be carried out in accordance with the Entrepreneurial Code of the Republic of Kazakhstan.

3. Preventive control without visiting the subject (object) of control shall be carried out in accordance with this Law and the Entrepreneurial Code of the Republic of Kazakhstan.

4. State control in the field of digitalization in relation to state bodies shall be carried out in accordance with Article 60-3 of this Law.

5. The requirements of this Article shall not apply to the National Bank of the Republic of Kazakhstan and organizations included in its structure, as well as special state bodies of the Republic of Kazakhstan, unless otherwise provided by the laws of the Republic of Kazakhstan.

Article 60-2. Procedure for conducting preventive control without visiting the subject (object) of control in the field of digitalization

1. Preventive control without visiting the subject (object) of control shall be carried out by the authorized body without visiting the subjects (objects) of control based on the analysis and data of digital systems, open sources, mass media, as well as other information about the activities of the subject (object) of control.

2. The objectives of preventive control without visiting the subject (object) of control shall be the timely suppression and prevention of violations, granting the subject of control the right to independently eliminate violations identified as a result of preventive control without visiting the subject (object) of control, and reducing the administrative burden on the subject of control.

3. In order to grant the right to independently eliminate violations to control subjects, preventive control without visiting the subject (object) of control shall be carried out only for those violations, the consequences of which can be eliminated in accordance with the legislation of the Republic of Kazakhstan.

4. Based on the results of preventive control without visiting the subject (object) of control, a recommendation shall be made to eliminate the identified violations without initiating a case on an administrative offense, with a mandatory explanation to the subject of control of the procedure for their elimination.

5. The recommendation to eliminate the identified violations must be delivered to the subject of control in person against signature or by other means confirming the fact of sending and receipt.

6. A recommendation to eliminate the identified violations, sent in one of the following ways, shall be considered to have been delivered in the following cases:

1) personal delivery – from the date of the note in the recommendation on receipt;

2) by mail – registered letter with notification;

3) electronically - from the date of sending by the authorized body to the email of the subject of control specified in the letter upon request by the authorized body.

7. The recommendation to eliminate the identified violations must be implemented within thirty working days from the day following the day of its delivery.

8. In the event of disagreement with the violations specified in the recommendation to eliminate the identified violations, the subject of control shall have the right to send an objection to the authorized body that sent the recommendation to eliminate the identified violations within five working days from the day following the day of its delivery.

9. Failure to comply within the established timeframe with the recommendation to eliminate the identified violations shall result in the inclusion of the subject (object) of control in the semi-annual list of preventive control with a visit to the subject (object) of control.

10. Preventive control without visiting the subject (object) of control shall be carried out no more than once per quarter.

Article 60-3. Procedure for conducting state control in the field of digitalization in relation to state bodies

1. State control in the field of digitalization in relation to state bodies (hereinafter referred to as audited state bodies) shall be carried out by an authorized body in the form of inspections.

Inspections are divided into periodic and unscheduled.

Periodic inspections of inspected state bodies shall be carried out in accordance with the following sources of information:

- 1) the results of previous inspections;
- 2) results of monitoring reports and information;
- 3) the results of the analysis of Internet resources of state bodies;
- 4) information from the state technical service.

2. Periodic inspections shall be carried out no more than once a year in accordance with the periodic inspection plan approved by the head of the authorized body in the field of cybersecurity.

The authorized body, no later than December 1 of the year preceding the year in which the inspections are carried out, shall approve a plan for conducting periodic inspections.

The plan for conducting periodic inspections shall be posted on the website of the authorized body no later than December 20 of the year preceding the year in which the inspections are conducted.

The periodic inspection plan shall include:

- 1) number and date of approval plan;
- 2) name of the state body;
- 3) the name of the state body being inspected;
- 4) the location of the inspected state body;
- 5) the timing of the inspection;
- 6) subject of inspection;
- 7) signature of the person authorized to sign the plan.

Amendments and additions to the plan for conducting periodic inspections shall be made in cases of liquidation, reorganization of the inspected state body, change of its name, or redistribution of powers between the inspected state bodies.

3. An unscheduled inspection is an inspection appointed by an authorized body in the following cases:

1) the presence of confirmed complaints regarding the inspected state body, received from individuals and legal entities, regarding violations of the requirements of the legislation of the Republic of Kazakhstan on cybersecurity;

2) appeals from individuals and legal entities whose rights and legitimate interests have been violated;

3) the prosecutor's demands regarding specific facts of harm or the threat of harm to the rights and legitimate interests of individuals and legal entities, the state;

4) appeals from state bodies regarding specific facts of harm to the rights and legitimate interests of individuals and legal entities, the state, as well as specific facts of violations of the requirements of the legislation of the Republic of Kazakhstan, the failure to eliminate which entails harm to the rights and legitimate interests of individuals and legal entities;

5) instructions from the criminal prosecution body on the grounds provided for by the Criminal Procedure Code of the Republic of Kazakhstan;

6) the need to monitor the implementation of the report on the inspection results.

4. When conducting an inspection, officials of the authorized body shall have the right to:

1) unimpeded access to the territory and premises of the inspected state body in accordance with the subject of the inspection upon presentation of the documents specified in paragraph 8 of this Article;

2) receive documents (information) on paper and digital media or their copies for inclusion in the report on the inspection results, as well as access to automated databases (digital systems) in accordance with the subject of the inspection;

3) carry out audio, photo and video recording;

4) involve specialists, consultants and experts from state bodies, subordinate and other organizations.

5. The inspected state body or its authorized representative during the inspection shall have the right:

1) not to allow officials of the authorized body who have arrived to conduct the inspection to participate in the inspection in the following cases:

exceeding or expiration of the time limits specified in the act on the appointment of an inspection (additional act on extension, if any) that do not correspond to the time limits established by this Article;

absence of documents specified in paragraph 8 of this Article;

2) to appeal the report on the inspection results in accordance with the procedure established by the legislation of the Republic of Kazakhstan.

6. The inspected state body or its authorized representative, when conducting an inspection, shall be obliged to:

1) ensure unimpeded access of officials of the authorized body to the territory and premises;

2) submit documents (information) on paper and digital media or copies thereof to officials of the authorized body for inclusion in the report on the inspection results, as well as access to automated databases (digital systems) in accordance with the subject of the inspection;

3) make a note on the second copy of the act on the appointment of the inspection and the act on the results of the inspection on the day of its completion.

7. The inspection shall be carried out on the basis of the inspection appointment act.

The act on the appointment of an inspection shall indicate:

1) date and number of the act;

2) name of the state body;

3) the last name, first name, patronymic (if indicated in the identity document) and position of the person(s) authorized to conduct the inspection;

4) information about specialists, consultants and experts from state bodies, subordinate and other organizations involved in conducting the inspection;

5) the name of the state body being inspected and its location.

In the event of an inspection of a structural subdivision of a state body, the act on the appointment of the inspection shall indicate its name and location;

6) subject of inspection;

7) type of inspection;

8) the period of conducting an inspection;

9) grounds for conducting the inspection;

10) the period under inspection;

11) the rights and obligations of the inspected state body;

12) signature of the head of the inspected state body or his/her authorized person on receipt or refusal to receive the act;

13) signature of the person authorized to sign the act.

When conducting an inspection, the authorized body shall be obliged to notify the inspected state body of the inspection commencement at least one day before its commencement, indicating the subject of the inspection.

The inspection commencement is considered to be the date of delivery of the inspection appointment act to the inspected state body.

8. Officials of the authorized body who arrive at the object for inspection shall be required to present to the inspected state body:

1) an act on the appointment of an inspection;

2) service ID or identification card;

3) if necessary – permission from the competent authority to visit restricted areas.

9. The period for conducting the inspection shall be established taking into account the subject of the inspection, as well as the volume of upcoming works, and must not exceed ten working days.

The inspection period may be extended only once, for no more than fifteen working days. The extension shall be granted by decision of the head of the authorized body.

The extension of the inspection deadline shall be formalized by an additional act on the extension of the inspection deadline with notification of the inspected state body, which indicates the date and order number of the previous act on the appointment of the inspection and the reasons for the extension.

A notice of extension of the inspection deadline shall be delivered to the inspected state body by the authorized body one working day before the extension with a delivery confirmation.

10. Based on the results of the inspection, the officials of the authorized body conducting the inspection shall draw up a report on the results of the inspection.

The first copy of the report on the inspection results in electronic form shall be submitted to the state body carrying out activities in the field of state legal statistics and special records within the limits of its competence; the second copy with copies of appendices, with the exception of copies of documents available in the original with the inspected state body, on paper against signature or in electronic form shall be handed to the inspected state body (the head or his/her authorized person) for familiarization and taking measures to eliminate the identified violations and other actions; the third copy remains with the authorized agency.

11. The report on the inspection results shall indicate:

1) date, time and place of drawing up the act;

2) name of the state body;

3) the number and date of the act on the appointment of the inspection (additional act on the extension of the period, if any);

4) the last name, first name, patronymic (if indicated in the identity document) and position of the person(s) who conducted the inspection;

5) information about specialists, consultants and experts from state bodies, subordinate and other organizations involved in conducting the inspection;

6) the name of the inspected state body, and its location;

7) subject of inspection;

8) type of inspection;

9) the term and period of the inspection;

10) information on the results of the inspection, including the violations identified and their nature;

11) requirements to eliminate identified violations of the requirements of the legislation of the Republic of Kazakhstan on cybersecurity, indicating the deadline for their implementation ;

12) information on familiarization or refusal to familiarize with the act by the head of the inspected state body or his/her authorized person, as well as persons present during the inspection, their signatures or a record of refusal to sign;

13) signature of the officials who conducted the inspection.

The report on the inspection results shall be accompanied by documents related to the inspection results (if any) and their copies.

12. If any comments and/or objections are raised based on the inspection results, the inspected government agency shall submit them in writing. These comments and/or objections shall be attached to the inspection results report, and a corresponding note shall be made to this effect.

The authorized body must consider the comments and/or objections of the inspected state body to the report on the inspection results and provide a reasoned response within fifteen working days.

In the event of a refusal to accept the report on the inspection results, a report shall be drawn up, which is signed by the officials conducting the inspection and the head of the inspected state body or his/her authorized representative.

The inspected state body shall have the right to refuse to sign the act, providing a written explanation of the reason for the refusal.

13. The completion of the inspection period shall be considered to be the day on which the inspection results report is delivered to the inspected state body no later than the inspection completion date specified in the inspection appointment report or the additional report on extending the inspection period.

14. The timeframe for executing the report on the inspection results shall be determined taking into account the circumstances that influence the actual possibility of its execution, but not less than ten calendar days from the date of delivery of the report on the inspection results .

15. When determining the deadlines for the execution of the report on the inspection results, the following shall be taken into account:

1) the availability of organizational and technical capabilities of the inspected state body to eliminate violations;

2) the timeframes for obtaining mandatory conclusions, approvals and other documents from state bodies, as established by the laws of the Republic of Kazakhstan.

16. Upon expiration of the period for eliminating the identified violations, as established in the report on the inspection results, the inspected state body shall be obliged, within the period established in the report on the inspection results, to provide the authorized body with information on the elimination of the identified violations with supporting documents.

In the event of failure to provide information on the elimination of the identified violations, the authorized body shall have the right to appoint an unscheduled inspection in accordance with subparagraph 6) of paragraph 3 of this Article.

17. In the event of a violation of the rights and legitimate interests of the inspected state body during the inspection, the inspected state body shall have the right to appeal the decisions, actions (inaction) of officials of the authorized body to a higher official or to the court in the manner established by the legislation of the Republic of Kazakhstan.

Article 60-4. State control over compliance with requirements for electronic documents and electronic digital signatures

State control over compliance with the requirements for electronic documents and electronic digital signatures shall be carried out in the form of an unscheduled inspection and preventive control with a visit to the subject (object) of control in accordance with the Entrepreneurial Code of the Republic of Kazakhstan, unless otherwise established by part two of this paragraph.

In relation to state bodies, state control shall be exercised over compliance with the requirements for electronic documents and electronic digital signatures in accordance with this Law.

The requirement of this paragraph shall not apply to the National Bank of the Republic of Kazakhstan and organizations included in its structure, and legal entities, fifty or more percent of voting shares (interests in the authorized capital) of which belong to the National Bank of the Republic of Kazakhstan or are under its trust management, as well as special state bodies of the Republic of Kazakhstan.

Article 60-5. Procedure for conducting state control over state bodies for compliance with requirements for electronic documents and electronic digital signatures

1. State control over compliance with the requirements for electronic documents and electronic digital signatures in relation to state bodies (hereinafter – subjects of control) shall be carried out by the authorized body in the form of inspections.

Inspections are divided into periodic and unscheduled.

Periodic inspections of controlled entities shall be carried out in accordance with the following sources of information:

- 1) the results of previous inspections;
- 2) results of monitoring reports and information;
- 3) the results of the analysis of Internet resources of state bodied;
- 4) information from the “digital government” operator.

2. Periodic inspections shall be carried out no more than once a year in accordance with the plan for conducting periodic inspections approved by the first head of the authorized body

The authorized body, no later than December 1 of the year preceding the year of inspections, shall approve a plan for conducting periodic inspections.

The plan for conducting periodic inspections shall be posted on the website of the authorized body no later than December 20 of the year preceding the year of inspections.

The periodic inspection plan shall include:

- 1) number and date of approval plan;
- 2) name of the state body;
- 3) name of the subject of control;
- 4) location of the subject (object) of control;
- 5) the timing of the inspection;
- 6) subject of inspection;
- 7) signature of the person authorized to sign the plan.

Amendments and additions to the plan for conducting periodic inspections shall be made in cases of liquidation, reorganization of the subject of control, change of its name or redistribution of powers between subjects of control.

3. An unscheduled inspection is an inspection appointed by an authorized body in the following cases:

1) the presence of confirmed appeals to the subject of control, received from individuals and legal entities, regarding violation of the requirements of the digital legislation of the Republic of Kazakhstan;

2) appeals from individuals and legal entities whose rights and legitimate interests have been violated;

3) the prosecutor's demands regarding specific facts of harm or the threat of harm to the rights and legitimate interests of individuals and legal entities, the state;

4) appeals from state bodies regarding specific facts of harm to the rights and legitimate interests of individuals and legal entities, the state, as well as specific facts of violations of the requirements of the legislation of the Republic of Kazakhstan, the failure to eliminate which entails harm to the rights and legitimate interests of individuals and legal entities;

5) instructions from the criminal prosecution body on the grounds provided for by the Criminal Procedure Code of the Republic of Kazakhstan;

6) the need to monitor the implementation of the report on the inspection results.

4. When conducting an inspection, officials of the authorized body shall have the right to:

1) unimpeded access to the territory and premises of the subject (object) of control in accordance with the subject of the inspection upon presentation of the documents specified in paragraph 8 of this Article;

2) receive documents (information) on paper and electronic media or their copies for inclusion in the report on the inspection results, as well as access to automated databases (digital systems) in accordance with the subject of inspection;

3) carry out audio, photo and video recording;

4) involve specialists, consultants and experts from state bodies, subordinate and other organizations.

5. During an inspection, the subjects of control or their authorized representatives shall have the right:

1) not to allow the officials of the authorized body who have arrived to conduct the inspection to participate in the inspection in the following cases:

exceeding or expiring the time limits specified in the act on appointing an inspection (additional act on extending the time limit, if any), which do not correspond to the time limits established by this Article;

absence of documents specified in paragraph 8 of this Article;

2) to appeal the report on the inspection results in accordance with the procedure established by the legislation of the Republic of Kazakhstan.

6. Subjects of control or their authorized representatives during the inspection shall be obliged to:

1) ensure unimpeded access of officials of the authorized body to the territory and premises of the subject (object) of control;

2) submit documents (information) on paper and electronic media or copies thereof to officials of the authorized body for inclusion in the report on the inspection results, as well as access to automated databases (digital systems) in accordance with the subject of the inspection;

3) make a note on the second copy of the act on the appointment of the inspection and the act on the results of the inspection on the day of its completion.

7. The inspection shall be carried out on the basis of the inspection appointment report.

The report on the appointment of an inspection shall indicate:

1) date and number of the report;

2) name of the state body;

3) the last name, first name, patronymic (if indicated in the identity document) and position of the person(s) authorized to conduct the inspection;

4) information about specialists, consultants and experts from state bodies, subordinate and other organizations involved in conducting the inspection;

5) the name of the subject of control, its location.

In the event of an inspection of a structural subdivision of a state body, the report on the appointment of the inspection shall indicate its name and location;

6) subject of inspection;

7) type of inspection;

8) the period of conducting an inspection;

9) grounds for conducting the inspection;

10) the period under inspection;

11) rights and obligations of the subject of control;

12) signature of the head of the subject of control or his/her authorized person on receipt or refusal to receive the report;

13) signature of the person authorized to sign the report.

When conducting an inspection, the authorized body shall be obliged to notify the subject of control about the commencement of the inspection at least one day before its start, indicating the subject of the inspection.

The commencement of the inspection shall be considered to be the date of delivery of the inspection appointment report to the subject of control.

8. Officials of the authorized body who arrive at the object for inspection shall be required to present to the subject of inspection:

- 1) a report on the appointment of an inspection;
- 2) service ID or identification card;
- 3) if necessary – permission from the competent authority to visit restricted areas.

9. The period for conducting the inspection is established taking into account the subject of the inspection, as well as the volume of upcoming work, and must not exceed ten working days.

The inspection period may be extended only once, for no more than fifteen working days. The extension shall be granted by decision of the head of the authorized body.

The extension of the inspection deadline shall be formalized by an additional report on the extension of the inspection deadline with notification of the subject of control, which indicates the date and order number of the previous report on the appointment of the inspection and the reasons for the extension.

A notice of extension of the inspection deadline shall be delivered to the subject of control by the authorized body one working day before the extension with a delivery confirmation.

10. Based on the results of the inspection, the officials of the authorized body conducting the inspection shall draw up a report on the results of the inspection.

The first copy of the report on the inspection results in electronic form shall be submitted to the state body carrying out activities in the field of state legal statistics and special records within the limits of its competence; the second copy with copies of appendices, with the exception of copies of documents that are in the original possession of the subject of control, on paper against signature or in digital form shall be handed over to the subject of control (the head or his/her authorized person) for familiarization and taking measures to eliminate the identified violations and other actions; the third copy remains with the authorized body.

11. The report on the inspection results shall indicate:

- 1) date, time and place of drawing up the report;
- 2) name of the state body;
- 3) the number and date of the report on appointment of the inspection (additional report on the extension of the period, if any);
- 4) the last name, first name, patronymic (if indicated in the identity document) and position of the person(s) who conducted the inspection;

- 5) information about specialists, consultants and experts from state bodies, subordinate and other organizations involved in conducting the inspection;
- 6) the name of the subject of control, its location;
- 7) subject of inspection;
- 8) type of inspection;
- 9) the term and period of the inspection;
- 10) information on the results of the inspection, including the violations identified and their nature;
- 11) requirements to eliminate identified violations of the requirements of the digital legislation of the Republic of Kazakhstan, indicating the deadline for their implementation;
- 12) information on familiarization or refusal to familiarize with the report by the head of the subject of control or his/her authorized person, as well as persons present during the inspection, their signatures or a record of refusal to sign;
- 13) signature of the officials who conducted the inspection.

The report on the inspection results shall be accompanied by documents related to the inspection results (if any) and their copies.

12. If the subject of control has any comments and/or objections based on the results of the audit, they must be submitted in writing. These comments and/or objections must be attached to the audit results report, and a corresponding note must be made to this effect.

The authorized body must consider the comments and/or objections of the subject of control to the report on the inspection results and provide a reasoned response within fifteen working days.

In case of refusal to accept the report on the results of the inspection, an act shall be drawn up, which shall be signed by the officials conducting the inspection and the head of the subject of control or his/her authorized representative.

The subject of control shall have the right to refuse to sign the act, providing a written explanation of the reason for the refusal.

13. The end of the inspection period shall be considered to be the day when the inspection results report is delivered to the subject of control no later than the inspection completion date specified in the inspection appointment report or the additional report on extending the inspection period.

14. The timeframe for executing the report on the inspection results shall be determined taking into account the circumstances that influence the actual possibility of its execution, but not less than ten calendar days from the date of delivery of the report on the inspection results

15. When determining the deadlines for the execution of the report on the inspection results, the following shall be taken into account:

- 1) the presence of organizational and technical capabilities of the subject of control to eliminate violations;

2) the timeframes for obtaining mandatory conclusions, approvals and other documents from state bodies, as established by the laws of the Republic of Kazakhstan.

16. Upon expiration of the period for eliminating the identified violations, established in the report on the inspection results, the subject of control shall be obliged, within the period established in the report on the inspection results, to provide the authorized body with information on the elimination of the identified violations with supporting documents.

In the event of failure to provide information on the elimination of the identified violations, the authorized body shall have the right to appoint an unscheduled inspection in accordance with subparagraph 6) of paragraph 3 of this Article.

17. In the event of a violation of the rights and legitimate interests of the subject of control during the inspection, the subject of control shall have the right to appeal the decisions, actions (inaction) of officials of the authorized body to a higher official or to the court in the manner established by the legislation of the Republic of Kazakhstan.

Chapter 11. Industry development and international cooperation in cybersecurity

Footnote. The title of Chapter 11 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 61. State support for the development of the cybersecurity industry

1. State support for the development of the cybersecurity industry shall be provided by authorized state bodies, the national development institute in the field of cybersecurity and other national development institutes with the aim of stimulating the development of the cybersecurity industry in the Republic of Kazakhstan.

2. The National institute for development in the sphere of cybersecurity shall carry out its activities in accordance with this Law.

3. Key principles of state support for the development of the cybersecurity industry shall be:

1) development of the cybersecurity industry based on private entrepreneurship and public-private partnerships;

2) priority for domestic legal entities when receiving orders for the development of cybersecurity;

3) stimulation of the development of domestic software production, software products and production of technical equipment;

4) development of the cybersecurity market structure;

5) support for fair competition in the cybersecurity market.

4. In accordance with the principles of state support, measures for the development of the cybersecurity industry, in addition to the measures provided for by the Entrepreneurial Code of the Republic of Kazakhstan, shall be:

1) formation and development of the regulatory and methodological framework for activities in the cybersecurity industry, including the implementation of international standards;

2) financing of projects in the cybersecurity industry;

3) creation of conditions for venture and other extra-budgetary reimbursable financing of projects in the cybersecurity industry;

4) investing in projects in the cybersecurity sector through participation in the authorized capital of legal entities, the creation of legal entities, including with foreign participation, and other methods provided for by the legislation of the Republic of Kazakhstan.

Footnote. Article 61 is in the wording of the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 62. Personnel and scientific support for the digital technology sector

1. The state shall create conditions for the training and retraining of specialists with technical, vocational, higher and postgraduate education on specialties in the field of digital technologies in domestic and foreign higher education institutions.

2. Organizations, national companies, and their affiliates shall report as internship bases for students in vocational, technical, higher, and postgraduate education institutions specializing in digital technologies.

3. Scientific support in the field of digital technologies shall be carried out through state support for scientific and scientific-technical activities in the field of digital technologies, including through the creation of conditions for the commercialization of technologies.

Footnote. Article 62 as amended by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Chapter 12.

Footnote. The title of Chapter 12 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 63. International cooperation in the field of cybersecurity

1. International cooperation of the Republic of Kazakhstan in the field of cybersecurity shall be carried out in accordance with international treaties and the legislation of the Republic of Kazakhstan.

2. Subjects of the digital environment of the Republic of Kazakhstan shall have the right to join international organizations and associations, and participate in international and foreign projects and programs.

State bodies, in agreement with the authorized body, shall interact in the field of cybersecurity with state bodies of foreign states, international organizations, and foreign legal entities.

3. International cooperation in the field of cybersecurity shall be carried out in the form of :

1) interaction with state bodies of foreign states, international organizations and foreign legal entities, including participation in the implementation of measures to implement international treaties of the Republic of Kazakhstan;

2) assisting in the formation of a stable and secure system of international (interstate) information interaction using digital technologies, including through the national gateway of the Republic of Kazakhstan;

3) interaction with foreign legal entities to ensure the development of digital technologies, as well as personnel development and scientific cooperation;

4) conducting, on an ongoing basis, jointly with foreign legal entities and international organizations, monitoring and forecasting the development of digital technologies;

5) interaction with state bodies of foreign states and international organizations on issues of the safe use of digital technologies, as well as the establishment of a ban on actions that infringe on the digital infrastructure of the state and undermine the political, economic, social and other spheres of state activity;

6) holding seminars, conferences and trainings in the Republic of Kazakhstan and abroad;

7) establishing a ban on the use of digital technologies to the detriment of individuals, society and the state on the basis of reciprocity;

8) joint financing and implementation of projects in the field of cybersecurity with foreign states, international organizations, foreign legal entities, foreign public organizations and foundations.

4. International cooperation on the issues of digital technologies development, institutional support and exchange of experience and knowledge shall be carried out with the participation of state bodies of foreign states, international organizations and foreign legal entities.

Footnote. Article 63 as amended by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Chapter 13. FINAL AND TRANSITIONAL PROVISIONS

Article 64. State control in the field of informatization

Footnote. Article 64 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 64-1. The procedure for conducting preventive control without visiting the subject (object) of control

Footnote. Article 64-1 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 64-2. The procedure for conducting state control over compliance with the legislation of the Republic of Kazakhstan on informatization in relation to state bodies

Footnote. Article 64-2 has been excluded by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 65. Liability for violation of the legislation of the Republic of Kazakhstan on cybersecurity

Violation of the legislation of the Republic of Kazakhstan on cybersecurity shall entail liability in accordance with the laws of the Republic of Kazakhstan.

Footnote. Article 65 as amended by the Law of the Republic of Kazakhstan dated 09.01.2026 № 256-VIII (shall enter into force upon expiry of six months after the date of its first official publication).

Article 66. Transitional provision

1. State bodies that have Internet resources and information systems of state bodies, introduced into industrial operation before the enactment of this Law and not having the protocol of tests for compliance with information security requirements, certificate of compliance with the requirements of information security, shall conduct their tests for compliance with information security requirements and certification within three years from the date of enactment of this Law.

2. Non-state information systems integrated with information systems of state bodies or intended for forming of the state electronic information resources and not having the protocol of tests for compliance with information security requirements, the certificate of compliance to information security shall be tested for compliance with information security requirements and certification within three years from the date of enactment of the Law.

3. Excluded by the Law of the Republic of Kazakhstan dated 19.06.2024 № 94-VIII (shall come into force sixty calendar days after the day of its first official publication).

Footnote. Article 66 is in the wording of the Law of the Republic of Kazakhstan dated 28.12.2017 № 128-VI (shall be enforced upon expiry of ten calendar days after its first official publication); as amended by the Law of the Republic of Kazakhstan dated 03.05.2022 № 118-VII (shall be enforced upon the expiration of ten calendar days after the day of its first official publication); dated 19.06.2024 № 94-VIII (shall come into force sixty calendar days after the day of its first official publication).

Article 67. Procedure for the enactment of this Law

1. This Law enters into enforce from January 1, 2016.

2. Recognize as invalid the Law of the Republic of Kazakhstan dated January 11, 2007 "On informatization" (Gazette of the Parliament of the Republic of Kazakhstan, 2007, № 2, art. 13; 2009, № 15-16, art. 74; № 18, art. 84; 2010, № 5, art. 23; № 17-18, art. 111; 2011, № 1, art. 2; № 11, art. 102; № 15, art. 118; 2012, № 2, art. 13; № 8, art. 64; № 14, art. 95; № 15, art. 97; 2013, № 5-6, art. 30; № 7, art. 36; № 14, art. 75; 2014, № 1, art. 4; № 19-I, 19-II, art. 96; № 23, art. 143).

*President of the
Republic of Kazakhstan*

N. NAZARBAYEV

© 2012. «Institute of legislation and legal information of the Republic of Kazakhstan» of the Ministry of Justice of the Republic of Kazakhstan