



On approval of the Rules for the functioning of a unified gateway to Internet access and a unified gateway of electronic mail of "electronic government"

Unofficial translation

Order of the Minister of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan dated October 13, 2020 No. 386/HK. Registered with the Ministry of Justice of the Republic of Kazakhstan on October 15, 2020 No 21436

Unofficial translation

In accordance with subclause 17-1) of article 7-1 of the Law of the Republic of Kazakhstan dated November 24, 2015 "In Informatization" I HEREBY ORDER:

1. To approve:

1) Rules for functioning of a unified gateway to Internet access, according to Appendix 1 to this order;

2) Rules for functioning of a unified gateway of electronic mail of "electronic government", according to Appendix 2 to this order.

2. The Information Security Committee of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan, in accordance with the procedure, established by law, shall ensure:

1) state registration of this order with the Ministry of Justice of the Republic of Kazakhstan;

2) placement of this order on the Internet resource of the Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan after its official publication;

3) within ten working days after the state registration of this order, submission to the Legal Department of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan of information about implementation of measures, stipulated by subclauses 1) and 2) of this clause.

3. Control over execution of this order shall be entrusted to the supervising Vice Minister of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan.

4. This order shall come into force upon expiry of ten calendar days after the date of its first official publication.

*Minister of Digital Development,
Innovations and Aerospace Industry
of the Republic of Kazakhstan*

B.Mussin

" A G R E E D "

National
of the Republic of Kazakhstan

Security

Committee

Rules for functioning of a unified gateway to Internet access

Chapter 1. General Provisions

1. These Rules for functioning of a unified gateway to Internet access (hereinafter referred to as the Rules) have been developed in accordance with subclause 17-1) of article 7-1 of the Law of the Republic of Kazakhstan dated November 24, 2015 “On Informatization” and shall determine the procedure for functioning of a unified gateway to Internet access (hereinafter referred to as the UGIA).

2. Connection of local, departmental and corporate telecommunication networks of state bodies, local government bodies, state legal entities, subjects of the quasi-public sector, possessors or owners of critical objects of information and communication infrastructure to the Internet shall be carried out by telecom operators through a unified gateway to Internet access.

Special state and law enforcement bodies for the operational purposes, the National Bank of the Republic of Kazakhstan in accordance with clause 3 of article 30 Of the Law of the Republic of Kazakhstan dated November 24, 2015 “On Informatization” may organize connections to the Internet without using the unified gateway to Internet access.

3. The following definitions are used in these Rules:

1) information security incident - separately or serially occurring failures in the operation of the information and communication infrastructure or its individual objects, which threaten their proper functioning and (or) the conditions for illegally obtaining, copying, distributing, modifying, destroying or blocking electronic information resources;

2) telecommunications service provider – an individual or legal entity registered in the territory of the Republic of Kazakhstan, providing telecommunications services and (or) operating telecommunications networks;

3) firewall for protection of web applications - technology for the protection of Internet resources (hereinafter referred to as the IR) from unauthorized access to data and their modification, even if critical vulnerabilities are present on the IR, by automatically detecting and blocking attacks;

4) protection from unauthorized alterations of web pages – technology that allows detecting modification and distortion of IR web pages by intruders, as well as restoring the IR to its original state in automatic mode;

5) UGIA root certificate – a dataset of a special format containing but not limited to the public key and located at the top level of a hierarchical tree of certificates used by UGIA equipment to pass Internet traffic containing protocols that support encryption;

6) technical capacity to connect to the UGIA – availability of functioning technical means and communication facilities necessary for connecting communication channels of communication operators to the UGIA and passing traffic of communication operators through the UGIA;

7) a UGIA user (hereinafter referred to as the User) – state body, local self-government body, state legal entity, subject of the quasi-public sector, owner or owner of critical objects of information and communication infrastructure, having connection of local, departmental and corporate telecommunication networks to the Internet through the UGIA;

8) application processing system (hereinafter referred to as the APS) – the IR, located at the address <https://support.sts.kz>, for the receipt of applications from telecommunications service providers and the Users;

9) telecommunications network – a complex of telecommunication facilities and communication lines providing transmission of telecommunication messages, consisting of switching equipment (stations, substations, concentrators), line-cable structures (subscriber lines, connecting lines and communication channels), transmission systems and subscriber devices.

Chapter 2. Procedure for UGIA functioning

4. "State Technical Service" Joint Stock Company (hereinafter referred to as the STS) carries out the UGIA support, ensures its uninterrupted operation.

The grounds for connection to the UGIA shall be a contract, concluded between the telecommunications service provider and the User in accordance with the legislation on state procurement.

5. For connection to the UGIA, the telecommunications service providers shall submit to the STS an application for the connection of telecommunications channels to the UGIA with arrangement of the main and reserve channel, in the form according to Appendix 1 to these Rules (hereinafter referred to as the application).

6. The STS, if it is technically possible to connect to UGIA, within ten working days from the date of receipt of the application, shall send to the telecommunication service provider the technical specifications for connection to the UGIA according to Appendix 2 to these Rules (hereinafter referred to as the technical specifications).

7. The telecommunications service provider, within seven working days after the receipt of technical specifications, shall notify the STS with an official letter, on the readiness for connection to the UGIA.

8. In case of failure to provide information to the STS, about readiness for connection to the UGIA, stipulated in clause 7 of these Rules, the telecommunications service provider shall re-submit an application, according to clause 5 of these Rules.

9. The telecommunications service provider shall ensure pursuance of technical specifications for the entire period of connection to the UGIA.

10. If there is no technical capability to connect to UGIA, the STS, within ten working days from the date of receipt of the application, shall send a notification to the telecommunication service provider about the rejection of the application, with indication of the reasons.

11. In the event of non-compliance with the requirements of the technical specifications, the telecommunications service provider, within five working days from the date of receipt of the notification of the rejection of the application from the STS, shall eliminate the identified inconsistencies in the connection to the UGIA.

12. The telecommunications service providers shall carry out the connection of Users to the UGIA.

13. The telecommunications service provider on the IR "IP-addresses Catalogue" (<https://catalog.sts.kz>), shall, on a continuous basis, actualize the information about the Users.

14. In the event of an information security incident, the telecommunications service provider or the User shall inform thereof the STS Duty Service by email support@sts.kz or by sending a request through the APS.

15. The User, at least once a year, shall submit to the STS a list of IR categories and lists of network addresses of the User's information and communication networks for use on the UGIA equipment, according to subclauses 2), 3) of clause 133 of the Uniform Requirements in the field of information and communication technologies and support information security, approved by the Government of the Republic of Kazakhstan dated December 20, 2016 No. 832.

16. The STS, within ten working days upon receipt from the User of the list of IR categories and lists of network addresses of the User's information and communication networks, shall apply the corresponding policies on the UGIA equipment and shall notify the User about the performed measure.

17. For the purposes of implementation of measures on IR protection, the User shall submit to the STS through the APS an application for the receipt of the service of additional IR protection by connection to the network firewall for protection of web-applications and shall provide necessary data, according to Appendix 3 to these Rules (hereinafter referred to as the application for the receipt of additional protection service).

The STS, subject to the availability of technical capabilities and the condition of receiving all the necessary data from the User, shall connect the IR specified in the application for

additional protection service to the network firewall to protect web applications within ten working days from the date of receipt of the application for additional protection service to the STS. Connection shall be carried out free of charge.

If there is no technical capability to connect to the network firewall to protect web applications, the STS, within ten working days from the date of receipt of the application for additional protection services, shall send to the User a notification of the rejection of the application, with indication of the reasons.

Upon receipt of a notification from the STS about rejection of the application, the User, upon expiry of thirty calendar days, shall re-submit an application for additional protection service through the APS.

18. For the purposes of implementation of measures on protection from unauthorized modifications of the IR web pages, the User shall submit to the STS through the APS an application for a connection to the system of protection from unauthorized modifications to the IR web pages and shall provide the necessary data, according to Appendix 4 to these Rules.

The STS, subject to the availability of technical capabilities and the condition of receiving from the User all the necessary data and access, shall connect the IR specified in the application for the receipt of the service of connection to the system of protection from unauthorized modifications to the IR web pages, to the protection system against unauthorized changes to the IR web pages within ten working days from the date of receipt of the specified application by STS. The connection shall be carried out free of charge.

If there is no technical capability to connect to the system of protection from unauthorized modifications to the IR web-pages, The STS, within ten working days from the date of receipt of the application for the service of connection to the system of protection from unauthorized modifications to the IR web pages, shall send to the User a notification of the rejection of the application, with indication of the reasons.

Upon receipt of a notification from the STS about rejection of the application, the User, upon expiry of thirty calendar days, shall re-submit an application for the service of connection to the system of protection from unauthorized modifications to the IR web pages through the APS.

19. The User, in case of termination of the use of the IR or changes in information about the IR (domain name, IP-address of the IR, responsible employee of the User, technical characteristics of the IR, telecom operator connecting to the UGIA), within five working days shall submit to the STS a corresponding official notification. The STS shall perform the necessary organizational and technical measures using the UGIA equipment.

20. For the timely detection and blocking of malicious content, the STS on the UGIA equipment shall implement appropriate technical measures to be able to analyze the encrypted traffic of Users.

21. The STS generates, transfers to telecommunication service providers and ensures the validity of the UGIA root certificate. As a new root certificate is generated, the STS shall inform the telecommunication service provider.

22. The telecommunications service provider shall transfer to its Users the UGIA root certificate.

23. The Users shall install the UGIA root certificate on their workstations.

Appendix 1
to the Rules for the functioning of
a unified gateway to Internet
access
Form
"State Technical Service" JSC
from _____
(name of organization)

APPLICATION

for the connection of telecommunications channels to the UGIA

Please connect communication channels with the following bandwidth:

_____ (measurement unit - 1 Gbps; minimum value - 1 Gbps)

for _____

_____.

_____ (planned period of the access to the UGIA)

We undertake to provide data via communication channels, contact details, documents and create conditions for a fault-tolerant connection to the UGIA.

_____ (surname, name, patronymic,
signature of the head of organization)

Seal (if any) " _____ " _____ 20 _____

Appendix 2
to the Rules for the functioning of
a unified gateway to Internet
access

TECHNICAL SPECIFICATIONS

№. __ на подключение к UGIA

Name and address of the object:

Name of the telecommunication service provider: _____

Active equipment connection point: _____

Integrated digital interface technology: 10G, full-duplex, SM.

Connection specifications:

To provide guaranteed service in a fault-tolerant mode, it is necessary to connect the main and backup communication channels through independent physical channels.

Requirements for laying optical patchcords:

1. Lay the optical patchcords (SC-LC) between the optical shelves in a corrugated pipe along the existing metal structures.
2. Optical patchcords (SC-LC) must be marked to identify their affiliation.
3. Before performing work on the installation of optical patchcords, coordinate the work with an STS representative

General issues:

Technical specifications are valid within 60 (sixty) calendar days.

If the work is not completed, the technical specifications must be confirmed and renegotiated in the STS. If not renewed 10 days before expiry date, technical specifications will automatically be canceled.

Appendix 3 to the Rules for the
functioning of a unified gateway to
Internet access
Form
"State Technical Service" JSC
from _____
(name of organization)

APPLICATION

for the receipt of a service of additional IR protection through the connection to the network firewall for protection of web applications

Please connect the IR <<domain name>> to the network firewall for protection of web applications.

We undertake to submit required data according to the list:

No	Required data	Notice
1	Domain name and IR IP-address	
2	Name of the telecommunication service provider, provided the connection to the Internet through the UGIA	
3	Name of the web server with indication of the version	Possible names: IIS, Apache, Apache Tomcat, Netscape Enterprise Server, IBM Lotus Domino, Nginx, JBoss, IBM Websphere, Lighttpd, Caucho Resin, JRun Web server, WebLogic. *Name of web server shall be provided with obligatory indication of the version.
4	Balancing system name (if available) with indication of the version	Possible names: Keepalived, Nginx etc.
5	The name of the database management system (DBMS) with indication of the version	Possible names: Oracle, MySQL, MSSQL, DB2, Sybase, PostgreSQL etc.

6	Name of the content management system CMS with indication of the version	Possible names: WordPress, Drupal, Struts, SharePoint
7	Certificate and private key, when using the https protocol	To implement IR protection using https
8	Application server name (if available) with indication of the version	Possible names: Apache Tomcat,
9	Contacts of responsible technical specialists	surname, name, patronymic, E-mail, office phone, mobile phone

_____ (surname, name, patronymic, signature of the head of organization)

Seal (if any) " _____ 20 _____

Appendix 4
to the Rules for the functioning of
a unified gateway to Internet
access
Form
"State Technical Service" JSC
from _____
(name of organization)

APPLICATION

for the receipt of the service of connection to the system of protection from unauthorized modifications of the IR web pages

Please connect the IR <<domain name>> to the system of protection from unauthorized modifications of the IR web pages.

We undertake to submit required data according to the list:

No	Required data	Notice
1	Domain name and IR IP-address	
2	Name of the telecommunication service provider, provided the connection to the Internet through the UGIA	
3	Name of the web server with indication of the version	Possible names: IIS, Apache, Apache Tomcat, Netscape Enterprise Server, IBM Lotus Domino, Nginx, JBoss, IBM Websphere, Lighttpd, Caucho Resin, JRun Web server, WebLogic. * Name of web server shall be provided with obligatory indication of the version.
4	Balancing system name (if available) with indication of the version	Possible names Keepalived, Nginx etc.
5	The name of the database management system (DBMS) with indication of the version	Possible names Oracle, MySQL, MSSQL, DB2, Sybase, PostgreSQL etc.
6	Name of the content management system CMS with indication of the version	Possible names WordPress, Drupal, Struts, SharePoint
7	Certificate and private key, when using the https protocol	To implement IR protection using https

8	Application server name (if available) with indication of the version	Possible names: Apache Tomcat,
9	Access to the IR root directory via FTP and / or SSH protocols	
10	Contacts of responsible technical specialists	surname, name, patronymic, E-mail, office phone, mobile phone
11	Registration details (login and password, a key for authorization, if key access is used) of a user with read and write permission to the root directory of a web resource on the server via ssh, ftp, sftp protocols	Login and password

_____ (surname, name, patronymic, signature of the head of organization)

Seal (if any) " _____ " _____ 20 _____

Appendix 2
to the order of the Minister of
Digital Development, Innovations
and Aerospace Industry of the
Republic of Kazakhstan
dated October 13, 2020
No. 386/HK

Rules for functioning of a unified gateway of electronic mail of "electronic government"

Chapter 1. General Provisions

1. These Rules for functioning of a unified gateway of electronic mail of "electronic government" (hereinafter referred to as the Rules) have been developed in accordance with подclause 17-1) of article 7-1 of the Law of the Republic of Kazakhstan dated November 24, 2015 "On Informatization" (hereinafter referred to as the Закон) and shall determine the procedure for the functioning of a unified gateway of electronic mail of "electronic government" (hereinafter referred to as the UGEM).

2. These Rules shall apply to state bodies, local government bodies, state legal entities, subjects of the quasi-public sector, possessors or owners of critical objects of information and communication infrastructure.

3. The following concepts are used in these Rules:

1) an applicant – a state body, local government body, state legal entity, a subject of quasi-public sector, possessor or owner of critical object of information and communication infrastructure, submitted an application for the receipt of a service for connection of e-mail of the Applicant to the UGEM;

2) the UGEM User (hereinafter referred to as the User) – a state body, local government body, state legal entity, a subject of quasi-public sector, possessor or owner of critical object of information and communication infrastructure, which electronic interaction of e-mail with external e-mail is carried out through redirecting emails via the UGEM;

3) external e-mail – an e-mail, not related to the departmental (corporate) email of the Applicant;

4) application processing system (hereinafter referred to as the APS) - an Internet resource located at <https://support.sts.kz> for accepting applications from Applicants and Users.

Chapter 2. Procedure for the UGEM functioning

4. The functioning of the UGEM shall be ensured through its support, which includes measures for technical support, connecting Applicants to the UGEM and processing requests / applications of Users on the UGEM issues.

5. "State Technical Service" Joint Stock Company (hereinafter referred to as the STS) shall carry out the UGEM support in accordance with подclause 6) of clause 1 of article 14 of the Law.

6. The STS shall ensure the uninterrupted operation of the UGEM.

7. To connect to the UGEM, the Applicant, through the APS or by official letter, shall apply for the service of connecting the mail system to the UGEM (hereinafter referred to as the application) in the STS in the form, according to Appendix to these Rules.

8. The STS, within five working days from the date of receipt of the application, shall test for the compliance of classifying the Applicant as a state body, local government body, state legal entity, quasi-public sector, possessor or owner of critical information and communication infrastructure facilities, as well as the availability of technical the possibilities (of functioning technical means and communication facilities) of connecting the Applicant's e-mail to the UGEM.

9. If there is technical capability to connect the Applicant's mail system to UGEM, the STS, within five working days from the date of receipt of the application, shall perform technical activities together with the Applicant to connect the mail system to UGEM and shall send a notification to the Applicant about the measures taken on the application.

10. If there is no technical capability to connect the Applicant's mail system to the UGEM, the STS, within five working days from the date of receipt of the application, shall send the Applicant a notice of rejection of the application, with indication of the reasons.

The Applicant, after receiving a notice of rejection of the application from the STS, upon expiry of thirty calendar days, shall re-submit the application through the APS.

11. If the User's status changes to something other than the subject of a state body, local government body, state legal entity, quasi-public sector, possessor or owner of critical objects of information and communication infrastructure, the User shall notify the STS by an official letter of the need to disconnect the mail system from the UGEM. The STS, within the period agreed with the User, shall disconnect the mail system from the UGEM.

No. _____ Date _____

"State Technical Service" JSC
from _____
(name of organization)

APPLICATION

for the receipt of a service of connection of mail system to the UGEM

Please pass the mail traffic through the UGEM:

(name of the e-mail domain connected to UGEM, the owner of the e-mail domain and the IP address of the mail server)

We undertake to provide data on the email domain, contact details, documents and create conditions for a fault-tolerant connection to the UGEM.

Provision of contacts of technical specialists on behalf of the user (surname, name, patronymic, mobile and office phone, e-mail) _____

(surname, name, patronymic, signature of the head of organization)

Seal (if any) " _____ " 20 _____