Appendix 2

to the order of Director General

JSC «Aviation administration of Kazakhstan»

from «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_20\_\_

№ \_\_\_\_\_\_\_

**Checklist on aviation security measures**

**Implementation of protection measures of critical aviation systems information and communication technologies from cyber threats in the civil aviation of the Republic of Kazakhstan**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Regulatory reference** | **Conformity assessment**  **(+/-)** | **Nonconformity position number** | **Note** |
| 1 | Have critical aviation information systems been identified; |  |  |  |
| 2 | Are the measures aviation information system security measures been implemented; |  |  |  |
| 3 | Identification of the threat and risk factors posed by possible cyber incidents in relation to flights and critical civil aviation systems, as well as the serious consequences that such incidents may lead to; |  |  |  |
| 4 | Whether there are developed, cybersecurity strategies, policies, and plans in place; |  |  |  |
| 5 | Is the cybersecurity management system implemented; |  |  |  |
| 6 | Is there an exchange of information in the field of cyber threats with interested parties; |  |  |  |
| 7 | Have the legal consequences of actions that putting at risk the safety of aircraft operations by using cyber-vulnerable locations been determined; |  |  |  |
| 8 | Are the methods of monitoring systems and detecting incidents implemented; |  |  |  |
| 9 | Whether it is carried out coordination of to provide incident reporting activities between the civil aviation organization's aviation safety and security units and the national rapid response teams for computer threats (CERT); |  |  |  |
| 10 | When defining critical important systems additionally, is the software and hardware for the critical important information and data systems used in their civil aviation activities specified whether; |  |  |  |
| 11 | Protection of critical aviation systems information and communication technologies (including among them their equipment and software) and data included in the risk assessment processes for each critical aviation system; |  |  |  |
| 12 | The concept, objective, scope and strategy of ensuring security in the organization in accordance with national by legislative acts, regulations, policies and guidance material, as defined by the division of the civil aviation organization responsible for ensuring cybersecurity; |  |  |  |
| 13 | Have civil aviation organizations included relevant provisions in their security programmes to protect critical information and communications technology systems (including their software and equipment) and data from cyber-attacks and interference; |  |  |  |
| 14 | Operators (civil aviation organizations) consider security considerations throughout the entire life cycle of aviation information and communication technology systems, from design and development to the end of the service life and maintenance of systems, up to the safe and proper disposal of equipment and software, as well as when modifying, reviewing, updating and upgrading existing systems, when storing and managing data in these systems; |  |  |  |
| 15 | The responsibility for ensuring the protection of critical information systems lies with properly selected, hired, and trained personnel; |  |  |  |
| 16 | Development clear guidance guidelines by aviation industry operators for the training of all personnel using or installing critical information systems and for their maintenance, as well as for certain flight crews and systems, and for aircraft maintenance personnel; |  |  |  |
| 17 | Regular training its users on best practices related to cybersecurity in general and in particular how cybersecurity relates to information and communications technology systems and data used in the aviation industry; |  |  |  |
| 18 | Providing the authorized organization with a list of all responsible persons for monitoring and ensuring cybersecurity, aviation security and quality control; |  |  |  |
| 19 | Network design and manage them with cyber security compliance in mind; |  |  |  |
| 20 | Inclusion of provisions on information and cybersecurity in the supply and maintenance of new and existing aviation systems, information and communication technologies, and data; |  |  |  |
| 21 | Organization of access control. Measures to restrict access to critical importance systems; |  |  |  |
| 22 | Information Security Continuous Monitoring (ISCM); |  |  |  |
| 23 | Detection. Development of an Information Security Continuous Monitoring regime (ISCM); |  |  |  |
| 24 | Planning of response measures. Ready to respond. Responding to incidents. Incident notifications; |  |  |  |
| 25 | Creating and using a crisis communication plan; |  |  |  |
| 26 | Conducting a follow-up analysis of the information and cybersecurity incidents that have occurred; |  |  |  |
| 27 | Response actions in connection with acts of unlawful interference (cyber-attacks that putting at risk aviation security); |  |  |  |
| 28 | Compliance with the confidentiality on aviation security information. Identification, handling, exchange, destruction; |  |  |  |
| 29 | Providing information about the threat; |  |  |  |
| 30 | Compliance with the authority of the inspector of the authorized organization; |  |  |  |
| 31 | Implementation of quality control measures; |  |  |  |
| 32 | Security measures of the air navigation service. Vulnerability assessment. Determining the extent of possible attacks; |  |  |  |
| 33 | Airfield control room security measures; |  |  |  |
| 34 | Safety measures for air navigation facilities and air navigation systems; |  |  |  |
| 35 | Power supply safety; |  |  |  |
| 36 | Security measures for maintenance facilities; |  |  |  |
|  | Implementation of the Resolution of the Government of the Republic of Kazakhstan dated December 20, 2016 No. 832 «Unified requirements in the field of information and communication technologies and information security» and other legislative acts of the Republic of Kazakhstan regulating information and cybersecurity issues; |  |  |  |
| 37 | Compliance with the requirements of the organization's informatization measures; |  |  |  |
| 38 | Compliance with the organization of information security; |  |  |  |
| 39 | Compliance with the requirements for electronic information resources and Internet resources; |  |  |  |
| 40 | Compliance with the requirements for the application software being developed or purchased; |  |  |  |
| 41 | Compliance with information and communication infrastructure requirements; |  |  |  |
| 42 | Compliance with information system requirements; |  |  |  |
| 43 | Compliance with the requirements for the technology platform; |  |  |  |
| 44 | Compliance with the requirements for the hardware and software complex; |  |  |  |
| 45 | Compliance with telecommunications network requirements; |  |  |  |
| 46 | Compliance with the requirements for the systems of uninterrupted functioning of technical means and information security. |  |  |  |

Decoding abbreviations:

(-1) – a critical discrepancy that poses a threat to aviation security and hinders further activities;

(-2) – inconsistencies that do not hinder further activities, provided that they are eliminated within the agreed time frame or restrictions are imposed;

(-3) – nonconformities that do not interfere with further activities and must be eliminated when improving production and quality systems;

(\*) – not required for this organization;

(+) – meets the requirements;

NA (not applicable) – measures or procedures are not applied or are not used at this organization (for example, the absence of flights requiring increased vigilance, etc.);

NC (not confirmed) – measures or procedures in respect of which inspectors were unable to establish compliance with the requirements of regulatory legal acts (lack of time, conflicting information or for other reasons).