Republika e Kosovës
Republika Kosova - Republic of Kosovo
Qeveria – Vlada – Government

REGULATION (OPM) NO. 05/2024 ON INTERNAL ORGANIZATION AND SYSTEMIZATION OF JOBS IN THE CYBER SECURITY AGENCY[1]

[1] Regulation OPM-No.05/2024 on Internal Organization and Systematization of Jobs in the Cyber Security Agency, was been approved by the Prime Minister, with Decision No. 028/2024, dated 06.03.2024.

Prime Minister of the Republic of Kosovo,

Pursuant to Article 94 (paragraph 10) of the Constitution of the Republic of Kosovo, Article 179 (paragraph 2) of Law No. 08/L-173 on Cyber Security, Article 28 (Paragraph 3) of Law No. 06/L113 on the Organization and Functioning of the State Administration and Independent Agencies in accordance with Article 9 (paragraph 1 sub-paragraph 1.11) of Law No. 08/L-117 for the Government of the Republic of Kosovo as well as Article 9 (paragraph 7) of Regulation No. 01/2020 on Internal Organization Standards and Systematization of Workplaces and Cooperation in State Administration Institutions and Independent Agencies,

Issues:

REGULATION (OPM) NO. 05/2024 ON INTERNAL ORGANIZATION AND SYSTEMIZATION OF JOBS IN THE CYBER SECURITY AGENCY

CHAPTER I
GENERAL PROVISIONS

Article 1
Purpose

The purpose of this Regulation shall be to determine the internal organization and systematization of jobs in the Cyber Security Agency.

Article 2
Scope

1. This shall be enforced by the Cyber Security Agency.

2. The duties and responsibilities of the Agency shall be defined by the relevant Law on Cyber Security.

CHAPTER II
INTERNAL ORGANIZATION AND SYSTEMIZATION OF JOBS IN THE CYBER SECURITY AGENCY

Article 3
The mission of the Cyber Security Agency

The mission of the Cyber Security Agency shall be to protect the national critical infrastructure, enhance the cyber security of citizens and businesses by proactively preventing cyber-attacks and establish a secure cyberspace in the Republic of Kosovo.

Article 4
Organizational structure of the Agency

1. The organizational structure of the Agency shall be as follows:

   1.1. Office of the Executive Director;

   1.2. Departments;

1.3. Divisions;

2. The number of employees in the Agency shall be thirty-three (38).

Article 5
Office of the Executive Director

1. The Office of the Executive Director shall consist of:

1.1. Executive Director;

1.2. Professional staff;

1.3. Support staff.

2. The duties and responsibilities of the Executive Director shall be defined by the relevant Law on Cyber Security, the Law on the Organization and Functioning of State Administration and Independent Agencies, the relevant Law on Public Officials, as well as other applicable legislation.

3. The duties and responsibilities of the professional and support staff of the Office of the Executive Director shall be defined by the relevant legislation on public officials.

4. The number of employees in the Office of the Executive Director shall be six (6).

Article 6
Departments and Divisions of the Agency

1. The Departments and Divisions of the Agency shall be:

1.1. National Center for Prevention and Response to Cyber Incidents:

1.1.1. Incident Analysis and Prevention Division;

1.1.2. Incident Management Division;

1.2. Department for Standards and Supervision:

1.2.1. Standards and Policy Division;

1.2.2. Supervision and Monitoring Division;

1.3. Department for Cyber Security Services:

1.3.1. Equipment and Services Certification Division;

1.3.2. Technical and Advisory Services Division;

1.3.3. Internal ICT Systems Division.

Article 7
National Center for Prevention and Response to Cyber Incidents

1. National Cyber Incident Prevention and Response Center shall have the mission of identifying and addressing cyber threats and risks to prevent cyber attacks, respond to and manage cyber incidents, and prevent their spread on a wider scale.

2. The duties and responsibilities of the National Cyber Incident Prevention and Response Center shall be:

2.1. ensure coordination of activities at the national level for the detection, protection and response to cyber attacks, as well as the implementation of surveillance, monitoring, identification, analysis, investigation and response to cyber security incidents;

2.2. perform the operational functions of cyber security as the Republic of Kosovo's National Computer Emergency Response Team - National CERT;

2.3. responsible for the processing, management of incidents and vulnerabilities, prevention of incidents, analysis of threats, risk management and post-incident service recovery process;

2.4. coordinate work for the resolution of cyber security incidents with responsible institutions in the area of cyber security at national and international levels;

2.5. propose to update the list of cyber incident types or taxonomy in accordance with the applicable legislation;

2.6. create and manage the registry of cyber incidents and threats;

2.7. conduct cyber threat research, analyses and assessments;

2.8. identify, assess and manage cyber risks;

2.9. propose ad-hoc teams approved by the Executive Director, for rapid responses to cyber incidents, assistance in situations when essential service operators and digital service providers lack the technical/human capacities and when the criteria specified in the applicable legislation are met;

2.10. give recommendations for technical improvements to essential service operators and digital service providers, in cases where weaknesses are identified;

2.11. provide through the Flash Rapid Response Team concrete technical support in the rapid treatment of identified cyber threats and vulnerabilities;

2.12. prepare the annual report with analysis, assessments, and predictions for the cyber security situation at the national level (with emphasis on the entities that are under the responsibility of the Agency) and with recommendations for enhancing national cyber resilience.

3. The National Center for Prevention and Response to Cyber Incidents is an equivalent structure to the Department.
4. The Director of the National Cyber Incident Prevention and Response Center shall report to the Executive Director of the Agency;

5. The National Cyber Incident Prevention and Response Center shall consist of two divisions:

5.1. Incident Analysis and Prevention Division;

5.2. Incident Management Division.

6. The number of employees in the National Cyber Incident Prevention and Response Center is twelve (12).

Article 8
Incident Analysis and Prevention Division

1. The Incident Analysis and Prevention Division mission is to analyze and handle cyber threats and risks in order to prevent cyber attacks.

2. The duties and responsibilities of the Incident Analysis and Prevention Division shall be:

2.1. identify anomalies and weaknesses in the network and information systems of operators of essential services and digital service providers, according to cyber security legislation;

2.2. conduct continuous research on developments in the area of cyber security and recommend security updates in case of detection of vulnerabilities and threats that may impact the network and information security integrity;

2.3. submit notifications for improvements to operators of essential services and digital service providers;

2.4. perform vulnerability testing, pen-testing, etc., analyze risk, and assess security for operators of essential services and digital service providers;

2.5. conduct analysis and implementation of security specifications for network and information systems;

2.6. prepare and implement an early warning system for immediate notification in case of cyber incidents, which may have an impact not only on operators of essential services and digital service providers but also on the rest of society;

2.7. through the Flash Rapid Response Team:

2.7.1. Provide concrete technical assistance, and when requested by operators of essential services and digital service providers, it also provides direct support in taking action to address threats and vulnerabilities;

2.7.2. regularly and continuously monitor the availability of patches for addressing threats and vulnerabilities by maintaining ongoing communication with the security departments of device and network system manufacturers;

2.7.3. produce an implementation guide for patches and workarounds launched for the treatment of cyber threats and vulnerabilities.

2.8. create and manage the electronic platform for real-time information exchange with operators of essential services and digital service providers;

2.9. create and manage the registry of cyber risks and threats;

3. The Head of the Incident Analysis and Prevention Division shall report to the Director of the National Center for Prevention and Response to Cyber Incidents.

4. The number of employees in the Incident Analysis and Prevention Division shall be five (5).

Article 9
Incident Management Division

1. The Incident Management Division has as its mission the response and management of cyber incidents and the prevention of their escalation on a wider scale.

2. The duties and responsibilities of the Incident Management Division shall be:

2.1. receive notifications of cyber incidents from operators of essential services and digital service providers, analyze the nature of the incident, and take actions for its treatment and management in accordance with the applicable legislation;

2.2. provide technical assistance in case of cyber incidents, assist in their resolution, and conduct post-incident analysis;

2.3. provide support for the post-incident service recovery process;

2.4. prepare a detailed incident report and submit it to the higher hierarchy;

2.5. establish and manage the cyber incident registry.

3. The Head of the Incident Management Division shall report to the Director of the National Center for Prevention and Response to Cyber Incidents.

4. The number of employees in the Incident Management Division shall be six (6).

Article 10
Department for Standards and Supervision

1. The Department for Standards and Supervision shall have the mission to supervise the implementation of safety measures and preparing procedures and technical standards determined for operators of essential services and digital service providers.

2. The duties and responsibilities of the Department for Standards and Supervision shall be:

2.1. receive and analyze risk assessment reports from operators of essential services and digital service providers;

2.2. evaluate the implementation of organizational, physical and information technology and communication security measures for network and information systems by operators of essential services and digital service providers defined by applicable legislation;
2.3. require operators of essential services and digital service providers to provide:

2.3.1. the necessary information to assess the security of their network and information systems, including documented security policies;

2.3.2. evidence of effective implementation of security policies, such as the results of a security audit conducted by competent institutions, including fundamental evidence, which should be available to the Agency.

2.4. prepare the annual inspection plan which is approved by the executive director of the agency and conduct inspections to determine the implementation of security measures in network and information systems at operators of essential services and digital service providers defined by applicable legislation;

2.5. after evaluating information or based on the results of security inspections, prepare mandatory guidelines for operators of essential services to correct identified deficiencies, which are communicated to operators of essential services and digital service providers with the approval of the Executive Director of the Agency;

2.6. license cyber security auditors and publish licensed entities on the official website of the agency;

2.7. propose amendments to standards and technical policies for implementation by operators of essential services and digital service providers in accordance with existing legislation;

2.8. recommend to the executive director of the Agency the enforcement measures for non-compliance with obligations specified under the applicable legislation by operators of essential services and digital service providers.

3. The Director of the Department for Standards and Supervision shall report to the Executive Director of the Agency.

4. The Department for Standards and Supervision shall consist of two divisions:

4.1. Standards and Policy Division;

4.2. Supervision and Monitoring Division;

5. The number of employees in the Department for Standards and Supervision shall be eight (8).

Article 11
Standards and Policy Division

1. The Standards and Policy Division has as its mission the identification and compliance with international standards, and the review of procedures and technical standards defined for operators of essential services and digital service providers.

2. The duties and responsibilities of the Standards and Policy Division shall be:

2.1. review information security standards, compliance frameworks and minimum security measures that are mandatory for entities subject to the agency's supervision, in accordance with existing legislation, and propose amendments to the bylaws that define them;

2.2. identify international and local information security standards as a common basis for the implementation of national, industry and enterprise requirements, and propose amendments to bylaws as necessary;

2.3. contribute to the development, adaptation and implementation of information security standards and policies by other public institutions;

2.4. develop guidelines for the implementation of minimum security measures and best practices in the area of cyber security;

2.5. provide advice and guidance on standards and policies for entities subject to the agency's supervision;

2.6. license cyber security auditors and publish licensed entities on the official website of the Agency.

3. The Head of the Standards and Policy Division shall report to the Director of the Department for Standards and Supervision;

4. The number of employees in the Standards and Policy Division shall be three (3).

Article 12
Supervision and Monitoring Division

1. The Supervision and Monitoring Division has as its mission the supervision and monitoring of the implementation of security measures defined by the legislation in force for operators of essential services and digital service providers.

2. The duties and responsibilities of the Supervision and Monitoring Division shall be:

2.1. identify, update and maintain the list of entities subject to the Agency's supervision;

2.2. update and maintain the list of chief security officers for operators of essential services and digital service providers;

2.3. receive and analyze assessment reports from operators of essential services and digital service providers;

2.4. prepare mandatory instructions and recommendations and forward them for approval;

2.5. inspect the implementation of security requirements according to the applicable legislation on cyber security;

2.6. exercise the implementation of the mandate of the Agency including communication, minor offences sanctions and preparation of recommendations for restriction or suspension of use or access to networks and information systems;

2.7. maintain the data and documentation collected during the supervision process in accordance with the applicable legislation;

2.8. prepare reports with detailed analysis on general trends and compliance of the entities under the responsibility of the Agency, non-compliance, implementation measures, complaints and challenges.

3. The Head of the Supervision and Monitoring Division shall report to the Director of the Department for Standards and Supervision;

4. The number of employees in the Supervision and Monitoring Division shall be four (4).

Article 13
Department for Cyber Security Services

1. The Department for Cyber Security Services shall have the mission to provide cyber security services to citizens, businesses and public institutions, as well as manage, administer and maintain internal ICT systems and laboratories within the Agency.

2. The duties and responsibilities of the Department for Cyber Security Services shall be:

2.1. perform security certification for information and communications technology, equipment and services, in cases when required by public institutions, according to the applicable legislation;

2.2. prepare the updated list of unreliable providers of information technology and communication equipment and services, according to the applicable legislation;

2.3. create and administer a communication platform with citizens and businesses that will be continuously available (24/7) for reporting cyber incidents;

2.4. respond to interested parties when seeking explanations or advice regarding various cyber threats;

2.5. prepare and publish awareness materials for all categories of society for protection against cyber attacks;

2.6. publish information on cyber threats and preventive measures;

2.7. create and manage the technical administration of the Agency's website.

3. The Director of the Department for Cyber Security Services shall report to the Executive Director of the Agency;

4. The Department for Cyber Security Services shall consist of three divisions:

4.1. Equipment and Services Certification Division;

4.2. Technical and Advisory Services Division;

4.3. Internal ICT Systems Division.

5. The number of employees in the Department for Cyber Security Services shall be twelve (12).

Article 14
Equipment and Services Certification Division

1. The Equipment and Services Certification Division has as its mission the certification of equipment and services for public institutions with the purpose of operating in a secure infrastructure for information and communication systems.

2. The duties and responsibilities of the Equipment and Services Certification Division shall be:

2.1. define the certification procedure, standards and requirements for analyzing the risk of the supply chain of internal ICT devices and services used by public institutions, in accordance with the Administrative Instruction on the rules and procedures for the certification process and preparation of the list of unreliable information technology and communications equipment and services;

2.2. conduct analyses and assessments of devices and services that may pose a risk to the supply chain;

2.3. maintain the list of certified reliable and unreliable sellers and providers of devices and services;

2.4. review and implement best practices in the certification of products and services.

3. The Head of the Equipment and Services Certification Division shall report to the Director of the Department for Cyber Security Services;

4. The number of employees in the Equipment and Services Certification Division shall be three (3).

Article 15
Technical and Advisory Services Division

1. The Technical and Advisory Services Division has the mission to provide support and advice to citizens, businesses and institutions to avoid being the target of cyber attacks.

2. The duties and responsibilities of the Technical and Advisory Services Division shall be:

2.1. administer the communication platform with citizens and businesses that will be continuously available (24/7) for reporting cyber incidents;

2.2. prepare awareness campaigns and publish various educational and instructional materials for protection against cyber attacks;

2.3. provide technical support to citizens and businesses through the publication of various materials and tools;

2.4. develop and provide public cyber security services such as Protective DNS (PDNS) and analysis of malicious software (malware).

3. The Head of the Technical and Advisory Services Division shall report to the Director of the Department for Cyber Security Services.

4. The number of employees in the Technical and Advisory Services Division shall be five (5).

Article 16
Internal ICT Systems Division

1. The Internal ICT Systems Division has as its mission the support of the agency for the realization of its functions through the administration of internal ICT systems and infrastructure.

2. The duties and responsibilities of the Internal ICT Systems Division shall be:

2.1. administer and maintain all the information and communication systems and laboratories of the Agency;

2.2. ensure the optimal functioning and secure access, in accordance with the institutionally approved policy of the computer systems of the Agency;

2.3. provide technical support by responding to requests from users of computer equipment regarding the malfunctioning of one or more components of the equipment or installed software;

2.4. identify the needs and draft the technical specifications for the purchase of equipment and software for the needs of the Agency;

2.5. organize the testing and evaluation of security technologies and specific applications necessary for the optimal functioning of the Agency;

2.6. provide support for the analysis, development, implementation and maintenance of databases and applications specific to the needs of the Agency.

3. The Head of the Internal ICT Systems Division shall report to the Director of the Department for Cyber Security Services.

4. The number of employees in the Internal ICT Systems Division shall be three (3).

CHAPTER III
FINAL PROVISIONS

Article 17
Final Provisions

1. Personnel mobility in accordance with the legislation for public officials within the institution is allowed, if it is considered necessary for the smooth running of the work.

2. The increase or decrease in the number of personnel in accordance with the annual budget law does not create a need to amend this Regulation, except in cases where organizational structures are created and/or extinguished.

3. In accordance with paragraph 2 of this article, the provisions of the annual budget law are an integral part of this Regulation.

Article 18
Annexes

An integral part of this Regulation is Annex 1 - Organizational Chart of the Cyber Security Agency.

Article 19
Entry into force

The shall enter into force on the day of its publication in the Official Gazette of the Republic of Kosovo.

Albin KURTI

_____

Prime Minister of the Republic of Kosovo
06 March 2024

Annex No. 1:
ORGANIZATIONAL CHART OF THE CYBER SECURITY AGENCY

ORGANIZATIONAL CHART OF THE CYBER SECURITY AGENCY			
Structure	**Class**	**Group** (general or specific)	**Number**
1. OFFICE OF THE EXECUTIVE DIRECTOR			**Total 6**
− Executive Director	− Senior Manager		1
− Senior Officer for Managing Operations and Projects	− Professional 1	60. Gr. Cyber Security Specialist	1
− Senior Officer for Information Security Management	− Professional 1	60. Gr. Cyber Security Specialist	1
− Senior Developer of Cyber Security for International Cooperation	− Professional 1	60. Gr. Cyber Security Specialist	1
− Senior Officer for Information and Communication	− Professional 1	10. Gr. Specialist of information and public relation	1
− Administrative Assistant	− Professional 3	58. Gr. Specialist of general administration	1
2. NATIONAL CENTER FOR PREVENTION AND RESPONSE TO CYBER INCIDENTS			**Total 12**
− Director of the National Center for Prevention and Response to Cyber Incidents	− Middle Manager		1
2.1 Incident Analysis and Prevention Division			**Total 5**
− Head of the Incident Analysis and Prevention Division	− Lower Manager		**1**
− Senior Analyst of Cyber Security	− Professional 1	60. Gr. Cyber Security Specialist	1
− Senior Analyst of Vulnerability and Threat Assessment	− Professional 1	60. Gr. Cyber Security Specialist	1
− Senior Officer of Threat and Vulnerability Management	− Professional 1	60. Gr. Cyber Security Specialist	2
2.2 Incident Management Division			**Total 6**
− Head of the Incident Management Division	− Lower Manager		1
− Senior Engineer of Cyber Security	− Professional 1	60. Gr. Cyber Security Specialist	1
− Senior Officer of Incident Response	− Professional 1	60. Gr. Cyber Security Specialist	2
− Senior Officer of Cyber Forensic	− Professional 1	60. Gr. Cyber Security Specialist	2
3. DEPARTMENT FOR STANDARDS AND SUPERVISION			**Total 8**
− Director of the Department for Standards and Supervision	− Middle Manager		1

3.1 Standards and Policy Division − Head of the Standards and Policy Division − Information Security Specialist − Policy and Technical Standards Officer	− Lower Manager − Professional 1 − Professional 1	60. Gr. Cyber Security Specialist 60. Gr. Cyber Security Specialist	**Total 3** 1 1 1
3.2 Standards and Policy Division − Head of the Supervision and Monitoring Division − Cyber Security Inspector − Information Systems Security Developer	− Lower Manager − Professional 1 − Professional 1	60. Gr. Cyber Security Specialist 60. Gr. Cyber Security Specialist	**Total 4** 1 2 1
4. DEPARTMENTFOR CYBER SECURITY SERVICES Director of the Department for Cyber Security Services	− Middle Manager		**Total 12** 1
4.1 Standards and Policy Division − Head of the Equipment and Services Certification Division − Technical Eligibility Assessment Specialist − Unreliable Products and Services Analyst	− Lower Manager − Professional 1 − Professional 1	60. Gr. Cyber Security Specialist 60. Gr. Cyber Security Specialist	**Total 3** 1 1 1
4.2 Technical and Advisory Services Division − Head of the Technical and Advisory Services Division − Officer for Response in Requests and Technical Support − Senior Developer of Systems and Cyber Security Services	− Lower Manager − Professional 1 − Professional 1	60. Gr. Cyber Security Specialist 60. Gr. Cyber Security Specialist	**Total 5** 1 2 2
4.3 Internal ICT Systems Division − Head of the Internal ICT Systems Division − − Senior Administrator of Networks and Systems − Senior Software Developer and Database Administrator	− Lower Manager − Professional 1 − Professional 1	61. Gr. - Specialist of ICT Systems 50. Gr. Specialist of software and applications	**Total 3** 1 1 1

ORGANIZATIONAL CHART OF THE CYBER SECURITY AGENCY