REPUBLIC OF ALBANIA
COUNCIL OF MINISTERS
NATIONAL AUTHORITY FOR ELECTRONIC CERTIFICATION AND CYBER SECURITY

INTERNAL REGULATION ON THE ORGANIZATION AND FUNCTIONING OF THE NATIONAL AUTHORITY FOR ELECTRONIC CERTIFICATION AND CYBER SECURITY

CONTENT

CHAPTER I
GENERAL PROVISIONS
Article 1
Legal basis

This regulation is drafted in support of Article 119 of the Constitution, Article 186, Article 59 point 2 of law no. 9880, dated 25.2.2008 "On electronic signature", Law no. 44/2015, "Code of Administrative Procedures of the Republic of Albania", Law no. 9000, dated 30.1.2003 "On the organization and functioning of the Council of Ministers", of law no. 152/2013 "On civil servants", as amended, of law no. 9131 dated 08.09.2003 "On the rules of ethics in public administration", of decision no.141, dated 22.2.2017 "On the organization and functioning of the National Authority for Electronic Certification and Cyber Security", as well as the order of the Prime Minister no. 6, dated 16.01.2020 "On the approval of the structure and staff of the National Authority for Electronic Certification and Cyber Security".

Article 2
Purpose

The purpose of this regulation is to define the detailed rules and tasks of organization, operation and relations between the different levels of the National Authority for Electronic Certification and Cyber Security, as well as to establish rules on the administration of documentation and equipment, rules of ethics, coordination of standard working functions and procedures, as well as the internal administration of the institution.

Article 3
Mission and responsibilities

1. 1. The mission of the National Authority for Electronic Certification and Cyber Security is to guarantee security for trusted services, electronic transactions between citizens, business and public authorities, as well as to set minimum technical standards for data security and networks / systems in the important and critical information infrastructure, in line with international standards in the field.
2. 2. The object of activity of AKCESK is the supervision of the implementation of the legislation in force, in the field of electronic signature, electronic identification and trusted services, as well as the legislation in the field of cyber security.
3. 3. AKCESK, performs these functional tasks:
   a) Registers / accredits the certification service provider and supervises its activity.
   b) Audits the methods of generation and management of public keys, backup / recovery system.
   ç) Defines the rules and methods for verifying the validity of products generated by trusted services, domestic and foreign, enabling public access to check their validity through trusted lists of EU member states and on-line status protocol of certificates and certificate revocation lists.
   d) Creates and maintains trusted lists of domestic and foreign CSOs, accredited by EU member states.
   dh) Approves the form and content of the agreements, between the qualified trusted service provider and third parties, in case of service transfer.

e) Supervises and controls third parties, in case one or more of the tasks of the trusted services are transferred.
f) Controls / monitors the implementation of standards and procedures for the issuance of qualified certificates by qualified trusted service providers.
g) Supervises the process of issuing qualified electronic certificates and the implementation of electronic signature in public administration services.
h) Ensures the implementation of standards on the secure identification of individuals to whom qualified electronic certificates are issued.
i) Defines the rules for electronic identification schemes, electronic stamps, transfer of tasks of trusted services, electronic transmission service, authentication of websites.
j) Creates and maintains lists of equipment for the creation of qualified electronic certificates in the Republic of Albania.
k) Temporarily, in whole or in part, terminates the activity of the certification service provider, when a violation of applicable laws or security measures is established.
l) Identifies, anticipates and takes the necessary measures for protection against possible cyber threats / attacks, in accordance with the legislation in force.
m) Identifies the operators of critical information infrastructures and important information infrastructures.
n) Proposes policies for ensuring cyber security at the national level, monitoring, identification and response to incidents for protection against cyber attacks / threats to critical and important information infrastructures in the Republic of Albania, and contributes to the development of policies for awareness cyber risks to the population, businesses and public administration.
o) Defines security measures for critical and important information infrastructures in the Republic of Albania.
p) Controls the documentation and implementation of security measures in critical and important information infrastructures.
q) Acts as a focal point of contact at the national level for operators responsible in the field of cyber security and coordinates the work for resolving cyber security incidents.
r) Maintains and administers the electronic register of cyber security incidents.
s) Administers incident reports in the field of cyber security and ensures their storage and recording.
t) Provides assistance and methodological support to responsible operators in the field of cyber security.
u) Carries out analyzes for the identified weaknesses in the field of internet security.
v) Conducts awareness and education activities in the field of cyber security.
w) Acts as a national CSIRT.
x) Propose to the Prime Minister to update at least once every two years, the list of operators of critical and important information infrastructures, and inform the Prime Minister on cyber security issues.
y) Drafts regulations, instructions in accordance with international standards in the field in order to guarantee secure electronic transactions and increase the level of cyber security in important and critical information infrastructures in the Republic of Albania.
z) Promotes the trusted services in public services, provided by public and private institutions, to citizens and business.

Article 4
Abbreviated name of the National Authority for Electronic Certification and Cyber Security, address, official emblem and stamp

1. The abbreviated name of the National Authority for Electronic Certification and Cyber Security is AKCESK.
2. The headquarters of AKCESK is located in Tirana, at the address: Rruga "Papa Gjon Pali II", no.3, Tirana.
3. The official website of AKCESK is www.cesk.gov.al.
4. The official emblem consists of the official emblem of the Republic of Albania and the notes: "Republic of Albania, the Council of Ministers, the National Authority for Electronic Certification and Cyber Security".
5. The AKCESK seal has the form and contains the elements defined in the legislation in force on the production, administration, control and storage of official seals. The stamp contains the identification mark "National Authority for Electronic Certification and Cyber Security".

CHAPTER II
ORGANIZATION AND FUNCTIONING

Article 5
Organizational structure

1. AKCESK is organized as the General Directory and operates according to the structure approved by order no. 6, dated 16.1.2020, of the Prime Minister "On the Approval of the Structure and Organics of the National Authority for Electronic Certification and Cyber Security".
2. The structure of AKCESK determines the degree of hierarchy and responsibility of functions in relation to each other.
3. The organizational structure of AKCESK consists of:
   Directory of Electronic Certification and Control:
   i. Accreditation and Policy Unit;
   ii. Unit of Control;
   iii. Communication and Information Dissemination Unit.

a) Directorate of AL-CSIRT:
   i. Cyber Incident Monitoring Unit;
   ii. Cyber Incident Management Unit;

b) Finance and Support Services Unit.

Article 6
Administrative functions

1. Administrative functions in AKCESK are performed by the staff of this institution, which is a civil service and is organized and functions according to law no. 152/2013 "On civil servants", as amended and bylaws in its implementation.
2. Civil service positions are classified according to categories, classes and the nature of the position.

Article 7
General Director

1. The General Director of AKCESK has these responsibilities:

a) Reports periodically on the activity of the institution to the Secretary General of the Council of Ministers.
b) Prepares analyzes, reports and makes proposals for the progress of the work of the structures under it.
c) Directs, elaborates the annual program for the engagements of the directorates, determines the priorities and guarantees coordination and cooperation in their work.
d) Proposes the taking of legal initiatives for the completion and improvement of the legal framework in force, within the field of activity of AKCESK.
e) Is responsible for defining the specific objectives and tasks of the staff.
f) Organizes the meeting of the directors of the directorates and the heads of the units as a rule, on the first Monday of each month, and for important issues for the progress of the work whenever it deems necessary.
g) Ensures the implementation of policy decisions, regularly following the process and taking measures to solve problems.
h) Ensures the efficient use of material, human and financial resources necessary for the realization and achievement of objectives.
i) Solves various and complex problems that affect the realization of institutional objectives.
j) Carries out strategic decision-making continuously in accordance with the legal framework in force that regulates its activity.
k) Plans the provision and coordination of projects with foreign donors.
l) Ensures the organization of work, in order to enable the continuity of services provided by AKCESK.
m) Ensures the organization of national and international activities.
n) Participates in various working groups, commissions, national and international conferences representing the institution.

Article 8
Delegation and replacement

1. The General Director of AKCESK delegates the competencies and duties to the Director of Electronic Certification and Control or the Director of AL-CSIRT, in accordance with the rules and procedure provided in the Code of Administrative Procedures. In any case, the delegation of competencies is done by a delegation act, which determines the delegated competencies and the deadline for their exercise.
2. The directors of the directorates and the heads of the units are replaced to perform their duties according to the provisions of the Code of Administrative Procedures and the law no. 90/2012 "On the organization and functioning of the state administration".

Article 9
Director of Electronic Certification and Control

1. The Director of Electronic Certification and Control has these responsibilities:

a) Directs the Directory of Electronic Certification and Control in fulfilling its functions, on the activity of qualified trusted service providers and operators who administer critical and important information infrastructure.
b) Accredits entities that operate as qualified trusted service providers, as well as oversees their activity to meet legal and technical requirements and accredits testing and confirmation bodies.
c) Verifies and compiles trusted lists, electronic identification schemes, lists of electronic certificate creation equipment, as well as lists of critical and important information infrastructures, as well as maintains and updates them.
d) Monitors the market to guarantee a legitimate process for the development of activity on electronic identification and trusted services as well as to increase the level of cyber security.
e) Follows the implementation of electronic signature and electronic stamps in public services.
f) Designs and coordinates the plan and calendar of audits of critical and important information infrastructures and trusted service providers.
g) Controls the procedures on the implementation of security measures by the operators that manage the critical and important information infrastructure and the providers of qualified trusted service.
h) Organizes and directs the work between the units of the directorate and is responsible for its quality at the General Director.
i) Defines the objectives of the directorate in fulfilling the functional tasks according to the field it covers (electronic signature, electronic identification and trusted services, as well as cyber security).
j) Organizes the periodic meeting of the subordinate units, to coordinate the progress of work and provides continuous training to increase the capacity of employees. In order to control the implementation of tasks by the respective units, the director periodically requests from the responsible persons a written report on the activity of the unit.
k) Monitors the work of subordinate employees and implements the system of evaluation of work results for them.
l) Shows special care in respecting the deadlines and procedures for performing the work of the unit.
m) Provides concrete solutions to problems encountered during the performance of tasks.
n) Prepares analyzes, reports and makes proposals for the progress of the work of the units of dependence.
o) Initiates inspections on the market monitoring for the exercise of the activity on trusted services and approves the inspection program for each inspection group.
p) Contributes to the preparation of laws and bylaws, in terms of the field of electronic signature, electronic identification and trusted services, as well as within the field of activity of AKCESK.
q) Performs other duties assigned by the General Director according to the job description.

Article 10
Director of AL-CSIRT

1. The Director of AL-CSIRT has these responsibilities:
   a) Proposes policies to ensure cyber security at the national level and contributes to their inclusion in the National Cyber Security Strategy.

b) Directs the monitoring process and ensures that the treatment of incidents is done in a timely manner and in compliance with the legislation and reports on decision-making to the head of the institution.
c) Directs and coordinates the activity of the directorate, in the framework of respecting deadlines and procedures and analyzes data in order to identify statistical indicators that affect the Global Cyber Security Indicators (GCI).
d) Coordinates the work, plans, implements, evaluates and monitors all tasks defined within the national CSIRT.
e) Conducts continuous research on developments in the field of cyber security and recommends security upgrades in case of vulnerability findings.
f) Coordinates the work for the exchange of information and coordination of action with the respective units.
g) Reports to the General Director regarding the prompt and appropriate measures that should be taken by public institutions to correct problems or violations found in the field of cyber security.
h) Monitors and manages cyber incidents in critical and important information infrastructures.
i) Participates in the drafting, consultations, proposals and cooperates with relevant structures for the design of special programs and procedures, in order to improve the level of protection of data and state networks / computer systems, against unauthorized activities and / or attempts to conduct an unauthorized activity.
j) Approves awareness programs, trainings, publication of information and educational materials related to ICT security, security advice for internet users at national level developed by addiction units.
k) Contributes to the preparation of laws and bylaws in the field of cyber security, as well as within the field of activity of AKCESK.
l) Monitors the work of dependent employees and ensures the qualification of employees, to enable the highest level of professionalism required by the implementation of NATO standards in the field of cyber security.
m) Verifies the security and compatibility of applications developed or implemented by state authorities.
n) Ensures the functioning and updating of the electronic register of cyber events / incidents and the register of national / international contact points.
o) Manages any information on cyber security made available by institutions, identifying in a timely manner the issues that need intervention or regulation.
p) Organizes the work between the subordinate employees, in accordance with the objectives and policies, in accordance with the legislation in force that regulates the activity of AKCESK.
q) Performs other tasks according to new field requirements and assigned by the Director of General according to the job description.

Article 11
Head of Unit

1. The head of the unit directs and manages the work of the unit. He maintains direct contacts with the director and managers of other units, to ensure quality in the work he performs.
2. The head of the unit performs these tasks:

a) Directs and contributes to the work of the unit and is responsible for the progress of the work and the tasks assigned by the director;
b) Manages the human resources of the unit;
c) Divides duties and responsibilities among the specialists of the unit;
d) Monitors the work of the unit specialists;
e) Shows special care in respecting the deadlines and procedures for performing the work of the unit;
f) Contributes to the definition of the duties and functions of the specialists of the unit and their formalism in the job description;
g) Holds meetings with subordinate staff and identifies problems;
h) Provides concrete solutions to the problems encountered during the performance of the task;
i) Develops cooperation relations with other units of the directorate and the institution;
j) Implements the system of annual evaluation of the employees of its unit;
k) Contributes to the preparation of laws and bylaws, within the scope of activity of AKCESK;
l) Participates in various working groups, commissions, national and international conferences, when appointed by the Director;
m) Drafts monthly, quarterly and annual work plans, which are submitted to the Director;
n) Drafts the relevant reports on the work performed and submits them to the Director;
o) Exercises competencies and performs tasks according to the job description.

Article 12
Accreditation and Policy Unit

1. The Accreditation and Policy Unit has these responsibilities:
a) Reviews and evaluates the relevant documentation and application submitted by entities for the accreditation process as a qualified trusted service provider.
b) Maintains constant contacts with qualified trusted service providers accredited by AKCESK, and requests the completion of documentation for any technical or operational changes undertaken by the NACC.
c) Manages the documentation of qualified trusted service providers and the documentation of testing and confirmation bodies, as well as maintains the Trust Lists of qualified trusted service providers. Publishes these lists for interaction and mutual recognition of electronic signatures with EU member states.
d) Reports on the conformity of legal and technical documentation submitted by qualified trusted service providers, according to AKCESK criteria, European norms and technical standards of ETSI (European Telecommunications Standards Institute).
e) Evaluates the fulfillment of the criteria of Certification Policies, Statement of Certification Practices, Operational Manual and Time Stamp Policies.
f) Evaluates the documentation submitted for the secure signature creation equipment and the certificates issued by their manufacturer, in order to meet the European level of security.
g) Compiles the report on the request for accreditation / registration of the qualified trusted service provider and suggests to the Director, whether the subject should be granted accreditation or not.

h) Drafts specific rules in accordance with the changes according to international standards, in the field of electronic signature, electronic identification and trusted services and cyber security.
i) Drafts legal and sub-legal acts regarding the field of electronic certification and cyber security, according to the identified needs of the institution, harmonized with the EU acquis.
j) Cooperates and coordinates the work with other institutions, for the implementation of electronic signature, electronic identification and trusted services.
k) Ensures the participation of employees, in national and international conferences and trainings, to increase the professional level of employees.
l) Monitors the implementation of the National Cyber Security Strategy and other policies where AKCESK is a contributor.

Article 13
Control Unit

1. The Control Unit has these responsibilities:

a) Audits qualified trusted service providers (NSDCs) and operators of critical and important information infrastructures (OIKI-OIRI), in relation to the fulfillment of security requirements, defined according to the legislation in force.
b) Controls the documentation and implementation of minimum security measures, technical and organizational, by the operators of critical and important information infrastructures, in accordance with the legal framework in force and international standards.
c) Prepares, drafts and submits for approval to the Director, the audit programs of the NSDC, OIRI and OIKI.
d) Manages the complete audit documentation of qualified trusted service providers and operators of important and critical information infrastructures.
e) Manages the audit process of CSOs and OIKI-OIRI.
f) Checks the technical documentation of the NSCO, so that they are the same as the documentation submitted to AKCESK.
g) Checks if NSC has performed, in the defined time periods, the internal audits.
h) Controls the internal audit reports, the security violations that have been identified and if the necessary measures have been taken to eliminate them, at the NCDC and OIKI,OIRI.
i) Checks the data on the employees of the safe areas and their integrity, at the qualified trusted service provider.
j) Verifies the lists of qualified certificates for their validity, at the NSDC.
k) Controls and audits the management of access control, database, key generation, certificate generation, integrity and security of the IT system, the system of revocation and suspension of certificates, the system of time stamps, of OKSHB.
l) Performs the role of external auditor (Testing and Confirmation Body) for the NSCO, in case there are no such registered with AKCESK.
m) Ensures the functioning and updating of the electronic register for control procedures.
n) Proposes administrative measures in cases of evidence of legal violations, to qualified trusted service providers and operators of important and critical information infrastructures.
o) Manages sensitive data of electronic signature holders, which are verified during audits with qualified trusted service providers, as well as sensitive data of OIRI and OIKI.

p) In accordance with the methodology for identifying critical and important infrastructures, proposes the initiative for reviewing their list.
q) Manages statistical data on the number of qualified certificates and electronic transactions.
r) Manages statistical data on the use of electronic identification and trusted services in electronic public services.

Article 14
Communication and Information Dissemination Unit

1. The Communication and Dissemination Unit has these responsibilities:
a) aManages the process of drafting working methodologies for cyber risk analysis in OIKI / OIRI and oversees the evaluation process.
b) Participates in the working group for cyber risk assessment in OIKI / OIRI.
c) Compiles and disseminates preliminary notices on information security.
d) Analyzes the tasks and commitments to international bodies, in accordance with the policies of the institution.
e) Coordinates and fulfills reporting obligations at the institutional level on various progress reports.
f) Organizes and coordinates various activities within the field of activity of the institution.
g) Maintains relations with international organizations (NATO; OSCE; FESA; ENISA; ETSI; FIRST; TI ECSO, etc.), to fulfill the commitments undertaken by AKCESK, in the field of cyber security and trusted services.
h) Liaises with national and international institutions, in order to determine and identify training programs to increase the capacity of AKCESK employees and proposes them to the superior.

Article 15
Cyber Incident Monitoring Unit

1. The Cyber Incident Monitoring Unit has the following responsibilities:
a) Performs analysis, implementation of security specifications for information systems and networks.
b) Performs evaluation and monitoring of information systems / networks.
c) Monitors systems / networks from unauthorized access, unauthorized modification of data or their destruction.
d) Configures and supports security applications.
e) Conducts continuous research on developments in the field of cyber security and recommends security upgrades in case of vulnerability findings.
f) Participates in various working groups.
g) Coordinates the work with other units to conduct periodic trainings for unit CSIRTs, in order to increase their professional capacity.

Article 16
Cyber Incident Management Unit

1. The Cyber Incident Management Unit has the following responsibilities:
   a) Provides methodological and technical solutions to reported cyber incidents.
   b) Carries out vulnerability testing, risk analysis, and safety assessment.
   c) Identifies anomalies in networks, systems, applications, government portals and those of critical national information infrastructures, in accordance with cyber security legislation.
   d) Coordinates the work for resolving cyber security incidents with the responsible operators in the field of national and international cyber security.
   e) Responds immediately with technical assistance to security incidents, which are reported to AKCESK, supports until resolved, and provides post-incident analysis.
   f) Conducts ongoing research on developments in the field of cyber security and recommends security updates in case of vulnerability findings.
   g) Participates in various working groups.
   h) Coordinates the work with other units to conduct periodic trainings for unit CSIRTs, in order to increase their professional capacity.

Article 17
Finance and Support Services Unit

1. The objective of the Finance and Support Services Unit consists in the efficient and transparent management of the resources that finance the activity of AKCESK in implementation of the budget law and the law on financial management and control, drafting of Medium Term Budget Program (MTBP) documents, as well as supporting the authorizing officer of the institution in decision-making, conveying information about costs in budget financing.
2. The Finance and Support Services Unit has the following responsibilities:

a) Controls the work for the progress of the financial activity of AKCESK, from the correct planning of operating expenses, investments and implementation of financial procedures, in accordance with the legislation in force.
b) Controls the financial administrative activity and ensures the effective use of the institution's funds, including the salary fund, as well as for all financial transactions related to the needs of the institution and in relation to third parties.
c) Controls and ensures the good administration of the assets of AKCESK for the timely execution of the inventory of monetary and material values.
d) Cooperates with the responsible structures of AKCESK for the drafting, monitoring and evaluation of the MTBP in quantitative and budgetary indicators, for each budget program.
e) Periodically monitors the implementation of the budget in accordance with the standards and procedures set out in the budget law and the relevant instructions for drafting and implementing the budget.
f) Controls, monitors and prepares documentation financially, during the procurement process, in accordance with the legal framework in force.

g) Controls the annual financial statements prepared by specialists.
h) Organizes and connects warehouse documents.
i) For services inside and outside the country, this unit is charged to calculate the costs immediately after the end of the service, after the submission of the required documents to prove the expenses by the employees.

CHAPTER III
ADMINISTRATIVE ACTS, TREATMENT OF DOCUMENTS AND CORRESPONDENCE

Article 18
Drafting of administrative acts

1. During the performance of administrative functions, the General Director of AKCESK, drafts administrative acts in accordance with the legislation in force that regulates the activity of this institution.

2. Unless otherwise provided by law, the administrative act has a written form, in paper or electronic, verbal or any other appropriate form and in these cases it is confirmed according to the rules set out in the Code of Administrative Procedures.

3. Administrative acts drafted by the General Director of AKCESK, written in paper or electronic, must contain the following necessary elements:

a) Introductory part containing:
   i. The name of the public body that issues the act
   ii. The parties to whom the act is addressed
   iii. Date of approval
   iv. Legal basisPjesën arsyetuese.

b) The enacting clause that indicates:
   i. The commanding part that shows what is set;
   ii. Time of entry into force of the act;
   iii. The right to appeal, including the public body or the court where the appeal can be filed, the means of appeal, the deadline and the manner of its calculation for filing an appeal;

Article 19
Drafting of papers

1. The model of the order of the General Director of AKCESK, as well as any other document that is drafted during the exercise of the activity of this institution, is according to the appendices of the Unified Rules of Procedure with documents in the public authorities of the Republic of Albania approved by the Council of Top of Archives.
2. Copies of documents or practices handled by the charge officer, which are kept in the relevant unit, are initialed by the specialist himself, the head of the unit, the director of the directorate and / or the General Director.

Article 20
Archive and Protocol

1. Secretary / Archivist The protocol performs, follows and maintains all written practice of AKCESK, according to the provisions of law no. 9154, dated 06.11.2003 "On archives", as well as the technical-professional and methodological norms of the archival service in the Republic of Albania.

2. All official practices, which enter on behalf of AKCESK, after being recorded by the protocol employee (protocol number and date are set), are administered by the latter until the full treatment and storage care after the practice treatment.

3. Any new official practice which enters for the first time in AKCESK. is assigned a (progressive) protocol number and entry date, while each practice which belongs to a problematic is continuously assigned a sequential number (with the same fractional protocol number passed and the entry date).

4. The data of the protocol number and the date are evidenced within the format of the AKCESK stamp produced for this purpose.

5. Official correspondences recorded and recorded in the protocol book of AKCESK are submitted by the protocol officer every day to the General Director.

6. The protocol employee, after returning the correspondence from the General Director, submits it to the directors of the directorates to distribute it for treatment.

7. The administration of documents classified "state secret" is done by the protocol office according to the provisions of law no. 8457, dated 11.2.1999 "On information classified" state secret "", as amended and bylaws in its implementation.

8. Secretary / Archivist The protocolist makes the archival processing of written practices, according to the rules defined in the law on archives.

9. Secretary / Archivist The protocolist submits the documents to the state archives, according to the legal deadlines..

KREU IV
RULES OF ETHICS
Article 21
Working hours and stay during working hours

1. The employee of AKCESK must respect and strictly follow the official working hours determined by the decision of the Council of Ministers.
2. The official working hours of AKCESK are from Monday to Thursday 08: 00-16: 30 and on Friday 08: 00-14.00.
3. During the official working hours, the employee is obliged to use the working time only for work purposes and for the performance of functional duties.
4. During the official working hours, the employee may leave for work, health or other justified reasons with the permission of the direct superior.
5. An employee who does not show up for work due to health reasons, must inform his superior without delay. In case of illness the clerk must be provided with a medical report.
6. Alcoholic beverages may not be consumed during working hours.
7. Smoking can only be done in open spaces designated specifically for this purpose.

8. Employees' clothing should be appropriate in accordance with the official ethics of staying in public administration.

Article 22
Submission of work

1. The rules of submission of the material base of work and documentation that the employee has in possession at the moment of dismissal, transfer, specializations or trainings, vacations, are regulated according to the civil service legislation.
2. At the end of the employment relationship, the employee is obliged to submit all equipment and documentation to the responsible persons or direct superior, within 5 (five) days. Failure to comply with this provision constitutes a disciplinary violation under civil service legislation.

Article 23
Conflict of interest

1. The directors and employees of AKCESK are subject to the provisions of law no. 9367, dated 7.4.2005 "On the prevention of conflict of interest in the exercise of public functions", as amended and in law no. 9049, dated 10.4.2003 "On the declaration and control of assets, financial obligations of elected officials and some public servants", as amended.
2. The AKCESK employee must take measures so that private interests do not affect the duty and avoid any possible conflict of interest.
3. Based on Article 41, point 2 of law no. 9367, dated 7.4.2005, "On the prevention of conflict of interest in the exercise of public functions", as amended, the General Director by internal order appoints at least 2 (two) of AKCESK employees, to establish a Responsible Authority as special structure, which continuously follows the process of declaration of private interests and conflict of interest, for all officials of the public institution, maintaining constant contacts with ILDKPKI.

KREU V

FINAL PROVISIONS
Article 24
The right to information

1. AKCESK shows special care regarding the implementation of law no. 119/2014 "On the right to information" and pursuant to this law, the General Director appoints by order one of the officials as Coordinator for the Right to Information, in order to coordinate the work to guarantee the right to information.
2. The Information Rights Coordinator exercises the powers set out in the Article 10, of law no. 119/2014 "On the right to information" and ensures the implementation of the law in AKCESK.

Article 25
Rules for maintenance and safety

1. AKCESK employees are prohibited from taking out of the premises where they work any kind of documentation related to the work of the institution, in written form, electronic verbal, or in any other form.
2. AKCESK employees are obliged to maintain all the equipment they have in use while performing their duties. It is forbidden to keep near any kind of material that may cause partial or complete damage to these devices.

Article 26
Gender equality and non-discrimination

1. AKCESK applies with special care the provisions of the legislation on gender equality in society and pays special attention to the basic issues of gender equality in public life, protection and equal treatment of women and men at work, equal opportunities and opportunities. for the exercise of human rights. In this context, AKCESK provides effective protection against discrimination based on gender, race, color, ethnicity, language, gender identity, sexual orientation, political, religious or philosophical beliefs, economic, educational or social status, pregnancy, parental affiliation, parental responsibility. , age, marital or marital status, marital status and any form of conduct that promotes discrimination.
2. During the recruitment process, AKCESK is committed to maximizing the inclusion of elements of gender discrimination in the announcement of vacancies and ensures equal opportunities for women and men to apply for vacancies. AKCESK can not disadvantage a jobseeker by establishing rules, criteria or procedural methods, which are seemingly neutral, but in practice are less favorable to persons of the opposite sex, except for objective and reasonable reasons.

Article 27
Disciplinary responsibility and job descriptions

1. AKCESK directorates take all necessary measures for the drafting of job descriptions for each position in accordance with the provisions of the civil service legislation.
2. AKCESK personnel must implement the provisions of this regulation.
3. Non-compliance with this regulation constitutes a reason for initiating disciplinary proceedings, according to special legislation regulating the employment relationship..

NR.PROT. 3264/1
DATË 2. 7. 2020

AUTORITETIT KOMBËTAR PËR CERTIFIKIMIN
ELEKTRONIK DHE SIGURINË KIBERNETIKE

Sekretari i Përgjithshëm

Engjëll AGAÇI

REPUBLIKA E SHQIPËRISË - KËSHILLI I MINISTRAVE