REGULATION
"ON THE USE OF INFORMATION TECHNOLOGY AT THE APPEAL CHAMBER"

Approved as per Decision No. 110 dated 21.12.2022 of the Meeting of Judges

Article 1
Purpose and scope

1. This regulation aims to determine the rules for the organization and functioning of the information technology systems at the Appeal Chamber, in accordance with Law no. 84/2016 "On the transitional re-evaluation of judges and prosecutors in the Republic of Albania", regulation "On the activity of the Appeal Chamber of the Constitutional Court", as amended, as well as other regulations in force.
2. The definitions of the rules, as well as their implementation, aims to reduce the operational risk that may be caused by the misuse of ICT systems, as well as to maintain the integrity of these systems in supporting the activity of users.
3. This regulation applies to all users of information technology at the Appeal Chamber. This regulation applies to all users of information technology and to all computer and electronic equipment owned by the Special Appeal Chamber.

Article 2
Legal basis

These rules are issued pursuant to:

- Law no. 84/2016 "On the transitional re-evaluation of judges and prosecutors in the Republic of Albania";
- Law no. 9887, dated 10.3.2008, "On the protection of personal data", as amended;
- Law no. 10273, dated 29.4.2010, "On the electronic document";
- Law no. 9918, dated 19.5.2008, "On electronic communications in the Republic of Albania", as amended;
- Regulation "On the activity of the Appeal Chamber of the Constitutional Court";
- Regulation "On the organization and functioning of the personnel and the administration of the documentation of the Appeal Chamber";
- Regulation "On the protection, processing, storage and security of personal data";
- Regulation "On the use of electronic mail in the Public Administration".

Article 3
Users

Users of information technology at the Appeal Chamber are:

1. Internal users:
   a) Judges of the Appeal Chamber;
   b) The advisors of the Legal Service Unit;

c) Administrative staff of the Appeal Chamber;
ç) IMO representatives.

2. External users, shall mean any person authorized as a user for work related purposes.

Article 4
Definitions

1. **Information and Communication Technologies** are *hardware* and *software* (computers, mobile phones, internet, operating system, computer programs, mobile applications, etc.) that enable the collection, storage, use and transmission of data.
2. **ICT capacities** are skills that enable the effective use of common or advanced software means (computers, software, and internet).
3. **ICT (or IT) specialists** are the officials whose main job is ICT development, operation or maintenance of ICT systems or applications.
4. **Computer** includes personal computers, tablets or other portable devices, such as: *Smartphones* or *Personal Digital Assistants* (PDAs).
5. **Internet access** refers to an external Internet connection through a company that operates as an Internet Service Provider (ISP).
6. ***Broadband*** are technologies or connections that enable the rapid transmission of data, that maybe: documents, audio/video recordings, movies, games, video-conferences through an Internet network (for example: ADSL, cable connection, UMTS, optical connection, VDSL, optical fiber, etc.).
7. ***Website*** is the internet interface, a document in *HyperText*, which may contain text, links, videos, photos, and other materials of electronic documents.
8. **Server** is the computer with specific physical parameters, which serves to store data, install various applications, as well as to establish, through it, the sharing of privileges for users.
9. ***Firewall*** is a device or computer program that is configured to control the traffic passing through the network, allowing or blocking it, based on a set of rules.
10. **IM** (*Instant Messaging*) are technologies that provide the possibility of real-time text communication between two or more interlocutors on a closed network or Internet.
11. **UserID/Username** is a string of characters that uniquely identifies a user on a computer system or network.
12. **Password** is a string of characters, a secret code of a user, which should not be known by other users, and which, used together with *UserID*, allows access to a computer system.
13. **Logging** is the process through which a user gains access to a computer system or network, which usually means entering a *UserID* (*username*) and a password.
14. **Electronic mail** is considered any message in the form of text, sound or image sent via a public communications network, which may be stored on the network or on the recipient's terminal device until the recipient receives it.
15. ***Domain Name*** is the part of the text that comes after the "**@**" sign in an *e-mail* address. Given that the Internet functions on the basis of IP addresses (of four digits), each *domain name* has a unique respective digit.
16. **Mail Client** is a program on users' computers that makes possible the sending, receiving and organization of the *e-mail*.

17. ***Reply to all*** is the option provided by the mail client to reply via e-mail not only to the sender, but to all users of the e-mail addresses included in the sender's initial e-mail, in "To" or "CC" sections.
18. ***Recall*** is the possibility provided by the mail client to withdraw back a sent *e-mail*.
19. ***Antivirus/Antispyware*** are programs that make possible the control, identification, and elimination of harmful computer programs installed on computers (viruses, Trojans, etc.).
20. ***Spam*** are electronic messages, *e-mails*, with unofficial commercial or informative content, usually sent automatically by software.
21. ***Attachment*** is a file on the computer that is sent via e-mail, that may be a document (PDF, Word, Excel, Access, etc.), audio file (FTR format, MP3, etc.), photo file (jpeg, img., etc.), a series of other e-mails, videos or any type of electronic element.
22. ***Chat*** is a program that allows real-time communication between two or more users on the Internet.
23. **Personal data** is any information related to the staff of the public administration, identified or identifiable, directly or indirectly, in particular referring to an identification number or one or more specific features for his physical, physiological, mental, economic, cultural or social identity.

Article 5
Administration of electronic devices and computer programs

1. The administration of electronic devices and computer programs, which are owned by the Special Appeal Chamber, is carried out in the same way as that of other assets, in accordance with the legislation in force for the management of assets and with regulations adopted by the Appeal Chamber.
2. The use of the network and computer equipment is managed by the Information and Communication Technology Specialists (hereinafter "IT specialist"), under the Economic and Support Services Directorate.
3. The Economic and Support Services Directorate is responsible for the care, safety and maintenance of information technology equipment, hardware, software and ICT platforms, except for cases where damage is caused by the official who uses them or an individual not authorized to use such devices.

Article 6
Provision with IT means

1. The internal user has the right to be provided with information technology means to perform his duties.
2. The internal user uses all information sources through IT techniques and methods, according to the task he/she carries out.
3. As regards the delivery of electronic devices and computer programs, as well as their collection, in the event a person leaves the office, IT specialists are provided with a request from the human resources specialist specifying:
   a) Individual's data;

b) The office designated to carry out the task;
c) Specific need.

4. In case of a relevant official is dismissed, the rules defined in the regulations in force on the handover of the task shall be applied also for the handover of computer equipment.

Article 7
Rules on use of electronic devices for users

1. The user shall use the electronic devices only for the performance of the tasks defined in the regulations in force, adopted by the Appeal Chamber.
2. The user of the electronic system must possess the necessary knowledge and have sufficient technical skills for the use of IT equipment to the extent that serves the exercise of the task.
3. In no case, the user shall interfere physically in the IT tools, with/without his initiative. If during their use, the user has encountered problems of a technical nature, he/she shall immediately notify the IT specialists for technical assistance.
4. In no case, the user should keep on the monitor functional data of his task in the presence of an unauthorized person, inside and outside the institution premises.
5. To no user is allowed to open or download from any USB, diskette, CD or DVD various materials without first checking these devices for viruses.
6. The user is responsible for protecting the information at his disposal from misuse, unauthorized access or intentional damage during the work process.
7. The user must not, in any possible case, download computer programs from the Internet or any other source to the computer(s) he/she is using, without the prior approval of IT specialists.
8. In the event that the user finds that there has been a breach of the security of the IT system, of the computer, or the computer is infected with a virus or other programs that compromise the integrity of the system, he must immediately notify the IT specialists.
9. The user must not create, save, transmit by IT means, or through them, materials that are offensive, defamatory, racist, discriminatory, denigrating, sexual, and pornographic or that may constitute a criminal offense. The user who comes into contact with or receives such materials must immediately notify the IT specialists.
10. The use of IT means owned by the Appeal Chamber are not allowed for personal and profit reasons.
11. External users shall be supervised by the IT specialist to guarantee the implementation of this regulation.
12. At the end of the work, all users must turn off the electronic devices they are using.
13. The user must carry out the login procedure using the personal password at the beginning of his access. Passwords are changed periodically (*every three months*).
14. Passwords must not be shared with other persons inside or outside the AC.
15. Passwords must observe the security criteria as appropriate (*number of characters, type of strings or set word*).
16. In a computer system, property of the Appeal Chamber, only those programs that the user needs to perform the functional task will be installed. The operating system and the Office

package are installed on each computer. Any additional software must be approved by the President of the Chamber/ Secretary General and maintained by IT specialists.

17. The computer programs used in the AC must be provided with licenses that allows their installation and use.

Article 8
Use of e-mail

1. The official e-mail address and electronic messages are not the individual property of internal users. It is forbidden to use the official e-mail address for private purposes.
2. The administration of official e-mail is carried out in accordance with the standards established by the National Agency for Information Service (AKSHI), in accordance with the legislation in force on information technology and the organization and functioning of this agency.
3. Each internal user is assigned an email address to be used exclusively for work related purposes. The address is individual and its use is protected with a password owned only by the official. Provided as a security protocol from AKSHI, the e-mail password expires automatically every 90 days.
4. The e-mail may also be used via mobile phones, after its installation by the IT specialists.
5. The employees are prohibited from automatically forwarding electronic messages received through the institution's network to private e-mail addresses.
6. The institution reserves the right to monitor, review, interrupt or publish any message created, sent or received via the network. Monitoring, reviewing and intercepting messages may be carried out by the IT specialist with the assistance of content filtering software.
7. The institution reserves the right to change the route, destination or suspend the sending of messages depending on the circumstances, notifying immediately the sender. This includes, but is not limited to:
   a) preventing the sending, alternation, archiving or deletion of attached documents (attachments) or the message code when it is suspected that it poses a risk to the operation of the computer system;
   b) deletion of additional contents in messages (e.g., music files), which are considered of no value to the institution and take up space in the memory;
   c) preventing the sending or archiving of messages with suspicious content, messages containing attached documents with suspicious names and suffixes;
   ç) preventing the sending or archiving of messages formulated in offensive language;
   d) preventing the sending or archiving of messages that are considered unofficial or commercial advertisements (*spam*).
8. In case an employee leaves the position:
   a) When an employee leaves the job or his term of employment ends for any reason, the human resources specialist shall inform the IT specialist accordingly. The IT specialist shall archive the account's electronic correspondence and shall remove the access rights to the ICT infrastructure before the employee physically leaves the work premises;

b) if requested by the employee's direct superior, an automatic message (*Out of Office*) is activated to notify all senders of the impossibility of further communication as a result of leaving the job;
c) The final deletion of the official e-mail address is made following the end of a 3-month period from the leaving date.

Article 9
Rules on the use of the Internet service

1. In the exercise of his/her tasks, the IT specialist:
   a) ensures that each computer connected to the Internet shall be provided with a firewall and access security controls are configured in such a way that no internal application opens alternative communication ports with the Internet;
   b) shall provide Internet access and provide passwords to all individual employee;
   c) shall configure the system and local computer options so that users do not have full rights to security software and antivirus.
2. The internal users should exercise caution when accessing online services, aiming:
   a) the proper use of Internet resources;
   b) minimization of unauthorized search by the direct superior, on the Internet;
   c) maintaining the integrity of the information on the Internet;
   ç) to not disable antivirus options for materials downloaded from the Internet.
3. The AC President may authorize:
   a) blocking certain websites that are considered inappropriate for work purposes (e.g., containing illegal, discriminatory or pornographic content);
   b) monitoring websites and their list, opened chronologically by the employee;
   c) downloading software from the Internet;
   ç) use of paid sites for information due for work-related purposes.

Article 10
Guaranteeing security conditions for information technology

1. The IT specialist must be notified of all incidents affecting the reliability, integrity or access of data or information technology equipment owned by the Appeal Chamber.
2. Theft, unauthorized entry, infection by viruses are cases for which the legislation in force provides disciplinary measures. In case it is found that the information technology equipment has been damaged in any way, the IT specialist shall keep a record that shall contain:
   a) data of the person in charge of the device/equipment;
   b) the date, time and place of finding the damage, malfunction, flaw;
   c) the type, specifics, causes of the problem;
   ç) opinion how to proceed further;
   d) the names and signatures of the specialists who examined the case;
   dh) the name and signature of the person in charge of the device/equipment.

3. In the event a problem found cannot be repaired, the electronic devices shall be returned to the IT specialist office, to be disposed of in accordance with the legislation in force. New equipment cannot be issued unless damaged equipment is returned.
4. To create optimal security conditions, the IT specialist processes the password system for:
   a) *e-albania outlook* platform;
   b) *sharefolder* system;
   c) computers in use;
   ç) *wireless* system;
5. For security reasons, the IT specialist cannot transmit and receive over the phone passwords for all information technology services that require the use of a password. The IT specialist provides all employees with an initial password, which users shall obligatorily change at the first login.
6. The password for logging into the institution's servers is administered only by the institution's IT specialists.
7. Logging into the server shall be carried out only for work purposes and in any case, at the end of the work process, the IT specialist shall report via e-mail to the Secretary General and direct superior on the reason for logging into the server. In case the logging is carried out for the needs of a certain employee, the relevant employee is notified in the reporting e-mail.
8. Information technology employees shall apply network firewall security policies.
9. The premises where personal electronic data shall be processed must be protected by organizational, physical and technical measures to prevent access by unauthorized persons.
10. In the premises where personal data is processed, these security measures are applied:
    a) Entry of unauthorized persons is prohibited.
    b) Persons entering these premises must be provided with the relevant authorization, accompanied by a security officer.
    c) The entry-exit premises shall be monitored via CCTV during 24 hours.
    ç) Electronic security devices and systems installed (alarm systems, cameras, smoke, humidity and temperature sensors in the relevant premises, etc.), as well as alarms in cases a change in the defined reference parameters is detected.
11. In the exercise of his/her duty, the IT specialist:
    a) shall apply the legislation in force for the protection of personal data and any other legislation necessary for the performance of his duties;
    b) shall ensure that the configuration of all security devices is confidential for the technical personnel alone. The same rule applies when the technical staff is external;
    c) shall undertake counseling, which may include intensive training on the use of the equipment.

Article 11
Updating of the Appeal Chamber official website

1. The official website shall be updated by the IT specialist whenever requested by the AC President, the Secretary General, the Director of the Case Management and Media and

Public Relations, the Director of the Economic Directorate and Support Services, and by the Media and Foreign Relations Coordinator.

2. The communication about updating the site shall be carried out via e-mail.
3. The update of the Transparency Program on the official website takes 2-5 working days.
4. Due to the needs of updating the official website, the IT specialist:
   a) shall maintain constant contact with the site maintenance company and reports continuously, in accordance with the provisions of the contract;
   b) shall maintain continuous communication with AKSHI for the purpose of informing and monitoring the host server located at AKSHI data center;
   c) for security reasons, he shall carry out every Friday a full back-up of the website on an external HDD.

Article 12
The use of ICT in the courtroom

1. The electronic audio-video system in the Appeal Chamber is used only to perform the function defined in this regulation. This system is used only by the IT specialist. In case of need, for maintenance or repair purposes, the system will also be accessed by specialized third parties, under the supervision of the institution's personnel. The system is used only for court hearings, for recording, archiving, as well as for monitoring hearings for security purposes and cannot be used for any other purpose.
2. The IT specialist records and documents, by keeping a minutes, any necessary modifications in case of error, flaw or incident in the audio-video system.
3. The use of the system is carried out by the IT specialist according to the tasks defined in the job description, in accordance with the regulation "On the organization and functioning of the personnel and the administration of the documentation of the Appeal Chamber".
4. The authorized IT personnel shall maintain the system infrastructure and perform the necessary technical checks. For any error, flaw or incident of the electronic audio-video system, qualified and authorized personnel are notified, who carry out the relevant identification and repair.
5. When the IT specialist in charge of using the audio-video system changes the workplace or leaves the job, he loses the right of access related to the previous task.
6. The IT specialist shall activate the FTR system according to the calendar of court hearings, to operate in parallel with the "audio-video" system. The electronic "audio-video" system shall be operated according to the calendar of court hearings.
7. The responsible persons (IT specialist and court secretary) who carry out the recording of the court hearings, shall stop the recording when the hearing ends, it is interrupted, or when requested by the trial panel.
8. At the request of the court secretariat, IT specialist extracts copies from the archive of court hearings in "audio" format, with the acknowledgement of the direct superior and Secretary General.
9. The copies from the archive of court hearing in the "video" format shall be extracted by the IT specialist only upon order of the AC President.

Article 13
Server room

1. Only the access of the IT specialist is allowed in the premises the servers are located.
2. In case of need of an external personnel, due to maintenance of the electronic system, he/she shall be allowed to enter these premises accompanied by the IT specialist and shall fill in the relevant form at the end of the process, the final form is part of Annex A.
   This form shall contain:
   - person's data;
   - time: date, entry time, exit time;
   - data on the reason and the actions that were performed;
   - signatures of the parties.
3. Smoking is prohibited.
4. The use of heating means is prohibited.
5. The fire protection equipment must always be in working conditions and in visible places.

Article 14
Data *Backup*

1. The IT specialist shall carry out the backup procedure of the institution's servers. The data and programs on the servers must be backed up periodically, in accordance with common practices.
2. The Information and Communication Technology Specialist must have a copy and a duplicate copy of all data and software maintained or stored on the central computer (Server 1). The duplicate copy shall be stored at the secondary computer (Server 2), in the server room.
3. Copies (backups) of data must be stored in places protected from fire and outside the premises the servers are kept.
4. Data copies should be tested regularly to ensure that they can be used in cases of need. Data recovery procedures should be tested regularly to ensure that they are effective and can be executed within the allowed time.
5. Every employee who creates/produces documents electronically at the devices at his disposal, in meeting his/her duties, or when receives them from any other source (e-mail, USB, HDD, CD/DVD, etc.), for work-related purposes, must duplicate (copy) them at least once in three months, with the assistance of the IT specialist.
6. The responsibility for carrying out these duplications in order to protect the data from loss, lies with each employee.

Article 15
Privacy protection

To the purpose of protecting the privacy of the data of the internal users of the Appeal Chamber, the provisions of the legislation in force for the protection of personal data, for the electronic

document, as well as for electronic communications, as well as the regulations in force adopted by the Appeal Chamber shall apply.

Article 16
Sanctions

Any action or omission contrary to this regulation shall constitute a violation and shall be followed up according to the rules defined in the legislation in force.

Article 17
Entry into force

This regulation shall enter into force immediately upon its adoption by the Meeting of Judges.