League of Arab States
General Secretariat

Arab Convention on Combating Information Technology Offences

League of Arab States
General Secretariat

Arab Convention on Combating Information Technology Offences

Preamble:

The Arab States signatory hereto,

Desiring to enhance cooperation between themselves to combat information technology offences threatening their security, interests and the safety of their communities,

Convinced of the need to adopt a common criminal policy aimed at protecting the Arab society against information technology offences,

Taking into account the high religious and moral principles, especially the ordinances of Islamic Law (Shari'a), as well as the human heritage of the Arab Nation which rejects all forms of crimes, and having regard to public order in every State,

Adhering to the relevant Arab and international treaties and charters on human rights, and guaranteeing, respecting and protecting them,

Have agreed as follows:

Chapter I

General Provisions

Article 1: Purpose of the Convention:

The purpose of this convention is to enhance and strengthen cooperation between the Arab States in the area of combating information technology offences to ward off the threats of such crimes in order to protect the security and interests of the Arab States and the safety of their communities and individuals.

Article 2: Terminology:

For the purpose of this Convention, the following terms shall be ascribed the definition opposite to each of them:

1- **Information technology**: any material or virtual means or group of interconnected means used to store, sort, arrange, retrieve, process, develop and exchange information according to commands and instructions stored therein. This includes all associated inputs and outputs, by means of wires or wirelessly, in a system or network.

2- **Service provider:** any natural or juridical person, common or private, who provides subscribers with the services needed to communicate through information technology, or who processes or stores information on behalf of the communication service or its users.

3- **Data**: All that may be stored, processed, generated and transferred by means of information technology, such as numbers, letters, symbols, etc…

4- **Information programme**: A set of instruction or commands which can be executed by means of information technology and intended to achieve a given task.

5- **Information system**: A set of programmes and tools intended to process and manage data and information.

6- **Information network**: The interconnection between more than one information system to obtain and exchange information.

7- **Site**: A location where information is made available on the information network through a specific address.

8- **Capture**: To view or obtain data or information.

9- **Subscriber's information**: Any information that the service provider has concerning the subscribers to the service, except for information through which the following can be known:
   a- the type of communication service used, the technical requirements and the period of service.
   b- the identity of the subscriber, his postal or geographic address or phone number and the payment information available by virtue of the service agreement or arrangement.
   c- any other information on the installation site of the communication equipment by virtue of the service agreement.

Article 3: Areas of Application of the Convention

Unless otherwise indicated, this convention shall apply to information technology offences with the aim of preventing, investigating and prosecuting them, in the following cases:

1- when committed in more than one State.
2- when committed in a State and prepared, planned, directed or supervised in another State or other States.
3- when committed in a State with the involvement of an organized crime group exercising its activities in more than one State.
4- when committed in a State and had severe consequences in another State or other States.

Article 4: Safeguarding Sovereignty

1- Every State Party shall commit itself, subject to its own statutes or constitutional principles, to the discharge of its obligations stemming from the application of this convention in a manner consistent with the two principles of equality of the regional sovereignty of States and the non interference in the internal affairs of other States.

2- Nothing in this convention shall allow a State Party to exercise in the territory of another State the jurisdiction or functions the exercising of which is the exclusively right of the authorities of that other State by virtue of its domestic law.

Article 5: Criminalization

Every State Party shall commit itself to the criminalization of acts set forth in this chapter, according to its legislations and statutes.

Article 6: Offense of Illicit Access

1- Illicit access to, presence in or contact with part or all of the information technology, or the perpetuation thereof.
2- The punishment shall be increased if this access, presence, contact or perpetuation leads to:

a- the obliteration, modification, distortion, duplication, removal or destruction of saved data, electronic instruments and systems and communication networks, and damages to the users and beneficiaries.

b- the acquirement of secret government information.

Article 7: Offence of Illicit Interception

The deliberate unlawful interception of the movement of data by any technical means, and the disruption of transmission or reception of information technology data.

Article 8: Offence Against the Integrity of Data

1- Deliberate unlawful destruction, obliteration, obstruction, modification or concealment of information technology data.
2- The Party may require that, in order to criminalize acts mentioned in paragraph 1, they must cause severe damage.

Article 9: Offence of Misuse of Information Technology Means

1- The production, sale, purchase, import, distribution or provision of:
   a- any tools or programmes designed or adapted for the purpose of committing the offences indicated in Articles 6 to 8.
   b- the information system password, access code or similar information that allows access to the information system with the aim of using it for any of the offences indicated in Articles 6 to 8.
2- The acquisition of any tools or programmes mentioned in the two paragraphs above with the aim of using them to commit any of the offences indicated in Articles 6 to 8

Article 10: Offence of Forgery

The use of information technology means to alter the truth of data in a manner that causes harm, with the intent of using them as true data.

Article 11: **Offence of Fraud**

Intentionally and unlawfully causing harm to beneficiaries and users with the aim of committing fraud to illicitly realize interests and benefits to the perpetrator or a third party, through:

1- entering, modifying, obliterating or concealing information and data.
2- interfering with the functioning of the operating systems and communication systems, or attempting to disrupt or change them.
3- disrupting electronic instruments, programmes and sites.

Article 12: Offence of Pornography

1- The production, display, distribution, provision, publication, purchase, sale, import of pornographic material or material that constitutes outrage of modesty through information technology.

2- The punishment shall be increased for offences related to children and minors pornography.
3- The increase mentioned in paragraph 2 of this Article covers the acquisition of children and minors pornographic material or children and minors material that constitutes outrage of modesty, through information technology or a storage medium for such technology.

Article 13: Other Offences Related to Pornography

Gambling and sexual exploitation.

Article 14: Offence Against Privacy

Offence against privacy by means of information technology.

Article 15: Offences Related to Terrorism Committed by means of information technology

1- Dissemination and advocacy of the ideas and principles of terrorist groups.
2- Financing of and training for terrorist operations, and facilitating communication between terrorist organizations.
3- Dissemination of methods to make explosives, especially for use in terrorist operations.
4- Spreading religious fanaticism and dissention and attacking religions and beliefs.

Article 16: Offences related to organized crime committed by means of information technology

1- Undertake money-laundering operations, request assistance or disseminate money-laundering methods.
2- Advocate the use of and traffic in drugs and Psychotropic Substances.
3- Traffic in persons.
4- Traffic in human organs

5- Illicit traffic in arms.

Article 17: Offenses Related to Copyright and Adjacent Rights

Violation of copyright as defined according to the law of the State Party, if the act is committed deliberately and for no personal use, and violation of rights adjacent to the relevant copyright as defined according to the law of the State Party, if the act is committed deliberately and for no personal use.

Article 18: Illicit Use of Electronic Payment Tools

1- Any person who forges, manufactures or sets up any instrument or materials that assist in the forgery or imitation of any electronic payment tool by whatever means.
2- Any person who takes possession of the data of an electronic payment tool and uses it, gives it to a third party or facilitates its acquisition by a third party.
3- Any person who uses the information network or an information technology means to unlawfully access the numbers or data of a payment tool.
4- Any person who knowingly accepts a forged payment tool.

Article 19: Attempt at and Participation in the Commission of Offences

1- Participation in the commission of any of the offences set forth in this chapter with the intention to commit the offence in the law of the State Party.
2- Attempt at the commission the offences set forth in Chapter II of this convention.
3- A State Party may reserve the right to not implement the second paragraph of this Article totally or partly.

Article 20: Criminal Responsibility of Natural or Juridical Persons

Every State Party shall commit itself, taking into account its domestic law, to arrange for the penal responsibility of juridical persons for the offences committed by their representatives on their behalf or in their interest, without prejudice to imposing a punishment on the person who committed the offence personally.

Article 21: Increasing Punishment for Traditional Crimes Committed by Means of Information Technology

Every State Party shall commit itself to increasing the punishment for traditional crimes when they are committed by means of information technology

Chapter III

Procedural Provisions

Article 22: Scope of Application of the Procedural Provisions

1- Every State Party shall commit itself to adopting, in its domestic law, the legislations and procedures necessary to specify the powers and procedures set forth in Chapter III of this convention.
2- Taking into account the provisions of Article 29, every State Party shall apply the powers and procedures mentioned in paragraph 1 to:
   a- offences mentioned in Articles 6 to 19 of this Convention.
   b- any other offences committed by means of information technology.
   c- collecting evidence on offences in electronic format.
3- a- A State Party may reserve the right to apply the procedures mentioned in Article 29 only to the offences or types of offences covered by the reservation, provided that the number of these offences shall not exceed the number of offences to which the procedures mentioned in Article

30 apply. Every State Party shall bear in mind the restrictiveness of the reservation in order to allow for the wide application of the procedures mentioned in Article 29.

b- A State Party may also reserve the right not to apply those procedures if, due to limited legislations, it is unable to apply them to communication transmitted by means of information technology by a service provider, provided the technology:

- is operated on behalf of a closed group of users.
- does not use a public communication network and is not connected to another public or private information technology.

Every State Party shall bear in mind the restrictiveness of the reservation in order to allow for the wide application of the procedures mentioned in Articles 29 and 30.

Article 23: Expeditious Custody of Data Stored in Information Technology

1- Every State Party shall adopt the procedures necessary to enable the competent authorities to issue orders or obtain the expeditious custody of information, including information for tracking users, that was stored on an information technology, especially if it is believed that such information could be lost or amended.

2- Every State Party shall commit itself to adopting the procedures necessary as regards paragraph 1, by means of issuing an order to a person to preserve the information technology information in his possession or under his control, in order to require him to preserve and maintain the integrity of such information for a maximum period of 90 days that may be renewed, in order to allow the competent authorities to search and investigate.

3- Every State Party shall commit itself to adopting the procedures necessary to require the person responsible for safeguarding the information technology to maintain the

procedures secrecy throughout the legal period stated in the domestic law.

Article 24: Expeditious Custody and Partial Disclosure of Users Tracking Information

Every State Party shall commit itself to adopting the procedures necessary as regards users tracking information in order to:

1- ensure expeditious custody of users tracking information, regardless of whether such communication is transmitted by one or more service providers.
2- ensure that a sufficient amount of users tracking information is disclosed to the competent authorities of the State Party or to a person appointed by these authorities to allow the State Party to determine the service providers and the transmission path of the communications.

Article 25: Order to Submit Information

Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to issue orders to:

1- Any person in its territory to submit certain information in his possession which is stored on information technology or a medium for storing information.
2- Any service provider offering his services in the territory of the State Party to submit user's information related to that service which is in the possession of the service provider or under his control.

Article 26: Inspecting Stored Information

1- Every State Party shall commit itself to adopting the procedures necessary to enable its competent authorities to inspect or access:
   a- an information technology or part thereof and the information stored therein or thereon.

b- the storage environment or medium in or on which the information may be stored.

2- Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to inspect or access a specific information technology or part thereof in conformity with paragraph 1(a) if it is believed that the required information is stored in another information technology or in part thereof in its territory and such information is legally accessible or available in the first technology, the scope of inspection may be extended and the other technology accessed.

Article 27: Seizure of Stored Information

1- Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to seize and safeguard information technology information accessed according to Article 26, paragraph 1, of this Convention.
These procedures include the authority to:

a- seize and safeguard the information technology or part thereof or the storage medium for the information technology information.

b- make a copy the information technology information and keep it.

c- maintain the integrity of the stored information technology information.

d- remove such accessed information from the information technology or prevent its access.

2- Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to order any person who is acquainted with the functioning of the information technology or the procedures applied to protect the information technology to give the information necessary to complete the procedures mentioned in paragraphs 2 and 3 of Article 26 of this Convention.

Article 28: Expeditious Gathering of Users Tracking Information

1- Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to:
   a- gather or register using technical means in the territory of this State Party.
   b- require the service provider, within his technical competence, to:
      - gather or register using technical means in the territory of this State Party, or
      - cooperate with and help the competent authorities to expeditiously gather and register users tracking information with the relevant communications and which are transmitted by means of the information technology.

2- If, because of the domestic legal system, the State Party is unable to adopt the procedures set forth in paragraph 1(a), it may adopt other procedures in the form necessary to ensure the expeditious gathering and registration of users tracking information corresponding to the relevant communications in its territory using the technical means in that territory.

3- Every State Party shall commit itself to adopting the procedures necessary to require the service provider to maintain the secrecy of any information when exercising the authority set forth in this Article.

Article 29: Interception of Content Information

1- Every State Party shall commit itself to adopting the legislative procedures necessary as regards a series of offences set forth in the domestic law, in order to enable the competent authorities to:
   a. gather or register through technical means in the territory of this State Party, or

b. cooperate with and help the competent authorities to expeditiously gather and register content information of the relevant communications in its territory and which are transmitted by means of the information technology.

2- If, because of the domestic legal system, the State Party is unable to adopt the procedures set forth in paragraph 1(a), it may adopt other procedures in the form necessary to ensure the expeditious gathering and registration of content information corresponding to the relevant communications in its territory using the technical means in that territory.

3- Every State Party shall commit itself to adopting the procedures necessary to require the service provider to maintain the secrecy of any information when exercising the authority set forth in this Article.

Chapter IV

Legal and Judicial Cooperation

Article 30: Competence

1- Every State Party shall commit itself to adopting the procedures necessary to extend its competence to any of the offences set forth in Chapter II of this Convention, if the offence is committed, partly or totally, or was realized:

a- in the territory of the State Party

b- on board a ship raising the flag of the State Party.

c- on board a plane registered under the law of the State Party.

d- by a national of the State Party if the offence is punishable according to the domestic law in the location where it was committed, or if it was committed outside the jurisdiction of any State.

e- if the offence affects an overriding interest of the State.

2- Every State Party shall commit itself to adopting the procedures necessary to extend the competence covering the offences set forth in Article 31, paragraph 1, of this Convention in the cases in which the alleged offender is present in the territory of that State Party and shall not extradite him to another Party according to his nationality following the extradition request.

3- If more than one State Party claim to have jurisdiction over an offence set forth in this Convention, priority shall be accorded to the request of the State whose security or interests were disrupted by the offence, followed by the State in whose territory the offence was committed, and then by the State of which the wanted person is a national. In case of similar circumstances, priority shall be accorded to the first State that requests the extradition.

Article 31: Extradition

1- a- This Article applies to the exchange of offenders between State Parties for offences set forth in Chapter II of this Convention, provided that such offences shall be punishable under the laws of the concerned State Parties by deprivation of freedom for a minimum period of one year or a more severe penalty.
b- If a different, less severe, penalty is applicable by virtue of an agreed arrangement or by virtue of the extradition treaty, then the less severe penalty shall apply.

2- Offences set forth in paragraph 1 of this article shall be deemed offences whose perpetrators are extraditable under any extradition treaty between State Parties.

3- If a State Party makes extradition conditional on the existence of a treaty, and it receives an extradition request from a State Party that has no extradition treaty, this Convention may be considered as a legal basis for extradition as regards offences set forth in paragraph 1 of this Article.

4- State Parties that do not require the existence of an extradition treaty shall consider that the offences set forth in paragraph 1 of

this Article are offences whose perpetrators are extraditable among such States.

5- Extradition shall be subject to the requirements set forth in the law of the State Party to which the request is submitted or to the applicable extradition treaties, including the grounds on which the State Party can rely to refuse extradition.

6- A contracting State Party may refuse to extradite its nationals and undertake, within the limits of its jurisdiction, to prosecute those of whom who commit in any other State Party offences punishable under the law in both countries by deprivation of freedom for a period of one year or a more severe penalty in any of the two contracting Parties, provided the other State Party addresses to it a prosecution request together with the files, documents, objects and information that it has in its possession. The requesting State Party shall be informed of what is being done regarding its request. Nationality shall be determined at the date the offence happened for which extradition is requested.

7- a- Every State Party shall commit itself to communicate, at the time of signature or deposit of the instrument of ratification or acceptance, the name and address of the authority responsible for extradition or procedural arrest, in the absence of a treaty, to the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers.

b- The General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers shall establish and update the registry of concerned authorities in the State Parties. Every State Party shall insure that the registry's details are correct at all times.

Article 32: Mutual Assistance

1- All State Party shall lend assistance to each other to the fullest extent for the purposes of investigation, procedures related to information and information technology offences or to gather electronic evidence in offences.

2- Every State Party shall commit itself to adopting the procedures necessary to fulfill the obligations set forth in Articles 34 to 42.

3- Requests for bilateral assistance and related communications shall be submitted in writing. In case of emergency, a State Party may submit such request in an expeditious manner, including by fax or email, provided such communication ensures a reasonable degree of security and reference (including by using coding) and confirmation of dispatch as required by the State Party. The State Party from which assistance is requested shall respond to the request through a fast means of communication.

4- Except as otherwise stated in this chapter, bilateral assistance shall be subject to the requirements set forth in the law of the State Party from which assistance is requested or in mutual assistance treaties, including the grounds on which the State Party can rely to refuse cooperation. The State Party from which assistance is requested may not exercise its right to refuse assistance with respect to offenses set forth in Chapter II only on the basis that the request relates to an offence that it considers as a financial offence.

5- Whenever the State Party from which assistance is requested may provide such assistance only in the presence of dual criminality, this condition shall be considered fulfilled regardless of whether the laws of the State Party classify the offence in the same category as those of the requesting State Party, provided that the act leading to the offence in respect of which assistance is requested is considered an offence according to the laws of the State Party.

Article 33 Circumstantial Information

1- A State Party may – within the confines of its domestic law – and without prior request, give another State information it obtained through its investigations if it considers that the disclosure of such information could help the receiving State

Party in investigating offences set forth in this convention or could lead to a request for cooperation from that State Party.

2- Before giving such information, the State Party providing it may request that the confidentiality of the information be kept; if the receiving State Party cannot abide by this request, it shall so inform the State Party providing the information which will then decide about the possibility of providing the information. If the receiving State Party accepts the information on condition of confidentiality, the information shall remain between the two sides.

Article 34: Procedures for Cooperation and Mutual Assistance Requests

1- The provisions of paragraphs 2-9 of this Article shall apply in case no cooperation and mutual assistance treaty or convention exists on the basis of the applicable legislation between the State Parties requesting assistance and those from which assistance is requested. If such a treaty or convention exists, the mentioned paragraphs shall not apply, unless the concerned parties agree to apply them in full or in part.

2- a- Every State Party shall designate a central authority responsible for sending and responding to mutual assistance requests and for their implementation and referral to the relevant authorities for implementation.

b- Central authorities shall communicate directly among themselves.

c- Every State Party shall, at the time of signature or deposit of the instrument of ratification, acceptance or agreement, contact the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers and communicate to them the names and addresses of the authorities specifically designated for the purposes of this paragraph.

d- The General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers shall establish and update a registry of concerned

central authorities appointed by the State Parties. Every State Party shall insure that the registry's details are correct at all times

3- Mutual assistance requests in this Article shall be implemented according to procedures specified by the requesting State Party, except in the case of non conformity with the law of the State Party from which assistance is requested.

4- The State Party from which assistance is requested may postpone taking action on the request if such action shall affect criminal investigations conducted by its authorities.

5- Prior to refusing or postponing assistance, the State Party from which assistance is requested shall decide, after consulting with the requesting State Party, whether the request shall be partially fulfilled or be subject to whatever conditions it may deem necessary.

6- The State Party from which assistance is requested shall commit itself to inform the requesting State Party of the result of the implementation of the request. If the request is refused or postponed, the reasons of such refusal or postponement shall be given. The State Party from which assistance is requested shall inform the requesting State Party of the reasons that prevent the complete fulfillment of the request or the reasons for its considerable postponement.

7- The State Party requesting assistance may request the State Party from which assistance is requested to maintain the confidentiality of the nature and content of any request covered by this chapter, except in as far as necessary to implement the request. If the State Party from which assistance is requested cannot abide by this request concerning confidentiality, it shall so inform the requesting State Party which will then decide about the possibility of implementing the request.

8- a- In case of emergency, mutual assistance requests may be sent directly to the judicial authorities in the State Party from which assistance is requested from their counterparts in the requesting State Party. In such case, a copy shall be sent

concurrently from the central authority in the requesting State Party to its counterpart in the State Party from which assistance is requested.

b- Communications can be made and requests submitted pursuant to this paragraph through INTERPOL.

c- Whenever, according to paragraph a, a request is submitted to an authority, but that authority is not competent to deal with that request, it shall refer the request to the competent authority and directly inform the requesting State Party accordingly.

d- Communications and requests carried out according to this paragraph and not concerning compulsory procedures may be transmitted directly by the competent authorities in the requesting State Party to their counterpart in the State Party from which assistance is requested.

e- Every State Party may, at the time of signature, ratification, acceptance or adoption, inform the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers that requests according to this paragraph must be submitted to the central authority for reasons of efficiency.

Article 35: Refusal of Assistance

In addition to the grounds for refusal set forth in Article 32, paragraph 4, the State Party from which assistance is requested may refuse assistance if:

1- the request relates to an offence that the law of the State Party from which assistance is requested considers as a political offence.

2- It considers that implementing the request could constitute a violation of its sovereignty, security, order or basic interests.

Article 36: Confidentiality and Limits of Utilization

1- In case no mutual assistance treaty or agreement exists on the basis of the applicable legislation between the State Parties

requesting assistance and those from which assistance is requested, the provisions of this Article shall apply. These provisions shall not apply if such a convention or treaty exists unless the concerned State Parties agree to apply any of the paragraphs of this Article or the whole Article.

2- The State Party from which assistance is requested may provide information or material contained in the request, provided:
   a- The element of confidentiality is maintained for the State Party requesting assistance; there shall be no compliance with the request in the absence of this element.
   b- The information is not used in investigations other than those contained in the request.

3- If the State Party requesting assistance cannot abide by the requirement set forth in paragraph 2, it shall so inform the other State Party which will then decide about the possibility of providing the information. If the requesting State Party accepts this requirement, it shall abide by it.

4- A State Party providing information or material according to the requirement in paragraph 2 concerning the provision of information may request the other State Party to justify the use of the information or material.

Article 37: Expeditious Safeguarding of Information Stored on Information Systems

1- A State Party may request another State Party to obtain the expeditious safeguarding of information stored on an information technology located within its territory regarding matters about which the State Party requesting assistance is submitting a request for mutual assistance in order to investigate, seize secure and disclose information.

2- A safeguarding request according to paragraph 1 shall specify the following:
   a- the authority requesting the safeguarding.
   b- the offence that is the subject of the investigation and a summary of the facts.

c- the information technology information to be safeguarded and its relation to the crime.
d- any available information that determines the person responsible for the stored information or the location of the information technology.
e- the reasons for the safeguarding request.
f- the desire of the State Party submitting the request for bilateral assistance to investigate, access, seize, secure or disclose the stored information technology information.

3- When a State Party receives a request from another State Party, it shall take all appropriate actions to safeguard the specified information in an expeditious manner according to its domestic law. For the purpose of responding to the request, safeguarding shall not be conditional on the existence of dual criminality.

4- A State Party that stipulates the existence of dual criminality to respond to the assistance request may, except in cases of crimes set forth in Chapter II of this Convention, reserve its right to refuse the safeguarding request according to this Article if there is reason to believe that the dual criminality requirement shall not be fulfilled at the time of disclosure.

5- Additionally, a safeguarding request may be refused if:
a- the request relates to an offence that the State Party from which assistance is requested considers as a political offence.
b- the State Party from which assistance is requested considers that implementing the request could threaten its sovereignty, security, order or interests.

6- Whenever the State Party from which assistance is requested believes that safeguarding will not guarantee the future availability of information or will jeopardize the confidentiality of the investigations of the requesting State Party or their integrity, it shall inform the requesting State Party accordingly so that it may subsequently determine the possibility of implementing the request.

7- A safeguarding that results from a response to the request mentioned in paragraph 1 shall be for a period of no less than

60 days in order to allow the requesting State Party to submit the request for searching, accessing, seizing, securing or disclosing information. After receipt of such a request, safeguarding of information shall be maintained according to the decision related to the request.

Article 38: Expeditious Disclosure of Safeguarded Users Tracking Information

1- Whenever the State Party from which assistance is requested determines – in the context of implementing, according to Article 37, a request to safeguard users tracking information related to specific communications - that a service provider in another state has participated in the transmission of the communication, the State Party from which assistance is requested shall disclose to the State Party requesting assistance a sufficient amount of users tracking information in order to determine the service provider and the transmission path of the communications.

2- The disclosure of users tracking information according to paragraph 1 may be suspended if:
   a- the request relates to an offence that the State Party from which assistance is requested considers as a political offence.
   b- the State Party from which assistance is requested considers that implementing the request could threaten its safety, security, order or interests

Article 39: Cooperation and Bilateral Assistance Regarding Access to Stored Information Technology Information

1- A State Party may request another State Party to investigate, access, seize, secure or disclose the stored information technology information located within the territory of the State Party from which assistance is requested, including information that has been safeguarded according to Article 37.

2- The State Party from which assistance is requested shall commit itself to respond to the State Party requesting assistance according to the provisions of this convention.
3- The response to the request shall be prompt if the relevant information may be lost or amended.

Article 40: Access to Information Technology Information Across Borders

A State Party may, without obtaining an authorization from another State Party:

1- Access information technology information available to the public (open source), regardless of the geographical location of the information.
2- Access or receive – through information technology in its territory – information technology information found in the other State Party, provided it has obtained the voluntary and legal agreement of the person having the legal authority to disclose information to that State Party by means of the said information technology.

Article 41: Cooperation and Bilateral Assistance Regarding the Expeditious Gathering of Users Tracking Information

1- State Parties shall lend bilateral assistance to each other regarding the expeditious gathering of users tracking information associated with specific communications in their territories and transmitted through the information technology.
2- Every State Party shall provide such assistance at least with respect to offences for which similar domestic cases involve the expeditious gathering of users tracking information.

Article 42: Cooperation and Bilateral Assistance Regarding Information Related to Content

State Parties shall commit themselves to provide bilateral assistance to each other regarding the expeditious gathering of content

information for specific communications transmitted by means of the information technology up to the limit allowed according to applicable treaties and local laws.

Article 43: Specialized Body

1- Every State Party shall guarantee, according to the basic principles of its legal system, the presence of a specialized body dedicated 24 hours a day to ensure the provision of prompt assistance for the purposes of investigation, procedures related to information technology offences or gather evidence in electronic form regarding a specific offence. Such assistance shall involve facilitating or implementing:

a- provision of technical advice.

b- safeguarding information based on Articles 37 and 38.

c collecting evidence, provide legal information and locate suspects.

2- a- In all State Parties, such a body shall be able to communicate promptly with the corresponding body in any other State Party

b- If the said body, designated by a State Party, is not part of the authorities of that State Party responsible for international bilateral assistance, that body shall ensure its ability to promptly coordinate with those authorities.

3- Every State Party shall ensure the availability of capable human resources to facilitate the work of the above mentioned body.

Chapter V

Final Provisions

1- Competent authorities in State Parties shall take the domestic procedures necessary to implement this convention.

2- This Convention is subject to ratification, acceptance or adoption by signatory States. The documents of ratification, acceptance or adoption shall be deposited with the General

Secretariat of the League of Arab States no later than thirty days following the date of ratification, acceptance or adoption. The General Secretariat shall inform all State Parties and the General Secretariat of the Council of Arab Interior Ministers of every deposit of such document and its date.

3- This Convention shall enter into force thirty days after the date of deposit of ratification, acceptance or adoption documents by seven Arab States.

4- Any State of the League of Arab States that has not signed this Convention may accede to it. Such State shall be considered a Party to this convention as soon as it has deposited the ratification, acceptance, adoption or accession document with the General Secretariat of the League of Arab States and thirty days have elapsed following the date of deposit.

5- Taking into account what is stated in paragraph 3 of Article 19, if the provisions of this Convention are incompatible with the provisions of any previous special convention, the text that is more appropriate to combat information technology offences shall apply.

6- No State Party may express a reservation involving a violation of the texts of this convention or a departure from its objectives.

7- A State Party may propose the amendment of any of the texts of this Convention and refer it to the Secretary General of the League of Arab States who shall transmit it to the State Parties of the Convention to decide on its adoption with a two third majority of State Parties. This amendment shall enter into force thirty days after the date of deposit of ratification, acceptance or adoption documents with the General Secretariat of the League of Arab States by seven Arab States.

8- A State Party may withdraw from this Convention upon submission of a written request to be sent to the Secretary General of the League of Arab States.

A withdrawal shall take effect six month after the date the request was sent to the Secretary General of the League of Arab States.

Done at Cairo, the Arab Republic of Egypt, on 15/1/1432 (H), 21/12/2010, in Arabic, in a single original deposited with the General Secretariat of the League of Arab States (the Technical Secretariat of the Arab Justice Ministers), and an exact copy being provided to the General Secretariat of the Council of Arab Interior Ministers. An exact copy is also provided to each State Party .

In witness whereof the Arab ministers of interior and Justice have signed this Convention on behalf of their States..

State	Ministers of Interior	Ministers of Justice
The Hashemite Kingdom of Jordan	(for) His Excellency Mr. Hisham Altal	His Excellency Mr. Hisham Altal
The United Arab Emirates	(for) His Excellency Dr. Hadif Ben Jaoan Alzaheri	His Excellency Dr. Hadif Ben Jaoan Alzaheri
The Kingdom of Bahrain	His Excellency General Sheikh Rashed Ben Abdallah Al Khalifa	His Excellency Sheikh Khaled Ben Ali Al Khalifa
The Republic of Tunisia	Signature illegible	His Excellency Mr. Alazhar Boaoni
The People's Democratic Republic of Algeria	His Excellency Mr. Daho Weld Kabliah	His Excellency Mr. Altayeb Beliz
The Republic of Djibouti		
The Kingdom of Saudi Arabia	His Royal Highness Prince Naif Ben Abdelaziz	His Excellency Dr. Mohamed Ben Abdelkerim Abdelaziz Alissa
The Republic of Sudan	His Excellency Engineer Ibrahim Mahmood Hamed	His Excellency Mr. Mohamed Bishara Dousa
The Syrian Arab Republic	His Excellency General Said Samoor	His Excellency Judge Ahmed Hamoud

		Younes
The Republic of Somalia		
The Republic of Iraq	His Excellency Mr. Jawad Kazem Albolani	His Excellency Mr. Dara Noureddin Bahaeddin
The Sultanate of Oman	His Excellency Mr. Saoud Ben Ibrahim Ben Saoud Alborsaidi	His Excellency Sheikh Mohamed ben Abdallah ben Zaher Alhanai.
The State of Palestine	His Excellency Dr. Said Abdelrahman Ahmad Aboaly	His Excellency Dr. Aly Khashan
The State of Qatar	His Excellency Sheikh Abdallah Ben Nasser Ben Khalifa Al thani	His Excellency Mr. Hassan Ben Abdallah Alghanem
The United Republic of Comoros		
The State of Kuwait	His Excellency Sheikh General Jaber Khaled Alsabah	His Excellency Counsellor Rashed Abdelmohsen Alhamad
The Lebanese Republic		
The Socialist People's Libyan Arab Jamahiriya	His Excellency General Abdelfattah Younes Alobidi	His Excellency Judge Mostafa Mohamed Abdelgilil
The Arab Republic of Egypt	His Excellency Mr. Habib Ibrahim Eladly	His Excellency Counsellor Mamdouh Mohidin Marey
The Kingdom of Morocco	His Excellency Mr. Altayeb Alsharquawi	His Excellency Mr. Mohamed Alnasseri
The Islamic Republic of Mauritania	Signature illegible	His Excellency Mr. Abdin Weldelkheir
The Republic of Yemen	His Excellency General Mothar	His Excellency Dr. Ghazi Shaef

	Rashad Almasry	Alaghbari