Law by Decree No. 16 of 2017 on Cybercrime

The President of the State of Palestine
The Chairman of the Executive Committee of the Palestine Liberation Organisation

In reference of the provisions of the Amended Basic Law of 2003, as amended, particularly the provisions of Article 43 thereunder,
Having reviewed the Palestinian Penal Law No. 74 of 1936, as amended, in force in the Southern Governorates,
The provisions of the Jordanian Penal Law No. 16 of 1960, as amended, in force in the Northern Governorates,
The Law No. 3 of 1996 Concerning Wired and Wireless Communications,
The Law of Penal Procedure No. 3 of 2001, as amended,
The Law by Decree No. 18 of 2015 Concerning the Combating of Drugs and Psychotropic Substances,
The Law by Decree No. 20 of 2015 Concerning the Combating of Money Laundering and Financing of Terrorism, as amended,
Based upon the recommendation of the Council of Ministers, dated June 20th, 2017,
Based upon the powers bestowed upon me,
In accomplishment of the public interest, and
In the name of the Arab Palestinian people,

I hereby promulgate the following Law by Decree:

Article 1

The following words and expressions mentioned in this Law by Decree shall have the meanings designated thereto hereunder, unless the context determines otherwise:

Ministry:	The Ministry of Telecommunications and Information Technology.
Minister:	The Minister of Telecommunications and Information Technology.
Data processing:	Conducting or applying a process or a set of processes to data, whether in relation to individuals or otherwise, including the collection, receipt, recording, storing, modification, transmission, retrieval, erasure, publication, republication, or blocking of access to such data, or the disruption or elimination of the operation of devices or modification of its content.
Information technology:	Any electronic, magnetic, optical or electrochemical means or any other means, either tangible or intangible, or a set of connected or unconnected means, which is used to process data, perform logic and arithmetic or storing functions, and includes any capacity to store data or communications which relate to or operate in conjunction with such a means.
Electronic data:	All that can be stored, processed, developed or transmitted by means of information technology, particularly inscription, images, sound, figures, letters, symbols, signs, and so forth.
Electronic information:	Any information that can be stored, processed, imported or transmitted by means of information technology, particularly inscription, images, sound, figures, letters, symbols, signs, and so forth.

DCAF Geneva Centre for Security Sector Governance

Electronic network:	A connection between more than one means of information technology to access and share information, including private and public networks or the world wide web (internet).
Electronic record:	A set of information, which in its entirety constitute a description of a case relating to a person or some object. It is developed, sent, received, or stored through electronic means.
Electronic document:	The electronic record which is released using any means of information technology. It is developed, stored, extracted, copied, sent, notified or received through a means of information technology on a tangible medium or on any other electronic medium. It is retrievable in a manner that is comprehensible.
Electronic website:	The place where information or services are made available on the electronic network through a particular address.
Person:	The natural or juridical person.
Electronic application:	An electronic programme designed to perform a particular task directly for the user or another electronic programme. It is used through the means of information technology or those alike.
Traffic data:	Any electronic data or information developed by means of information technology, showing the source of transmission, the destination where it is transmitted, its route, time, date, volume, and the duration and type of communications service.
Password:	All that is used to access information technology systems and those alike to verify the user's identity. It is part of the traffic data and includes codes, retinal scan, facial scan, fingerprint scan, or those alike.
Electronic transaction device:	The electronic card which contains a magnetic strip, a smart chip or another means of information technology, or an electronic application, which contains electronic data or information and is issued by licenced authorities.
Government data:	Includes the data of the State, entities and public institutions, or the companies belonging thereto.
Encryption:	The process of transforming electronic data into a form with which it is impossible to read and comprehend without restoration to its original format.
Code:	A secret and private key(s) that belongs to a person or a particular entity and is used for encrypting computer data by means of figures, letters, symbols, or those alike.
Reception:	Viewing of or access to data or information.
Breach:	Unauthorised or unlawful access to information technology systems or the electronic network.
Electronic signature:	Electronic data supplemented, attached to or connected with an electronic transaction, and has a feature that allows to determine the identity of the person who signed it and to distinguish him from others for the purposes of approval of the content of the transaction.
Signature device:	A programme used to create an electronic signature on a transaction.
Certificate:	The electronic certificate issued forth by the Ministry or the body authorised thereby to prove the relation and connection

DCAF | Geneva Centre for Security Sector Governance

	between the website and electronic signature data.
Service provider:	Any person who provides the users of his service with the capability of communication by means of information technology, or any person who processes, stores or hosts computer data on behalf of any information service provider or the users of such service.
Damage:	The destruction of electronic programmes, either wholly or partly, or damage of the same in a manner that renders them unusable.
Subscriber's information:	Any information that is available with the service provider and pertains to the service subscribers, including:
	− The type of communications service used, technical requirements and duration of the service.
	− Identity, postal or geographical address or telephone of the subscriber and payment information available on the basis of the service agreement or installation.
	− Any other information on the site of the installation of the communication equipment based upon the service agreement.
Employee:	Each person who works in the public sector, private sector, private institutions, local government units, civil society organisations, associations, or private companies, in which the State is a shareholder, and all those of similar standing.

Article 2

1. The provisions of this Law by Decree shall be applicable to any of the crimes provided for thereunder in the event they are perpetrated either wholly or partly inside or outside Palestine or their impact extends inside Palestine, and regardless of whether the perpetrator is original, accomplice, abettor or accessory, on condition that the crimes are punishable outside Palestine and subject to the general principles provided for under the Penal Law in force.

2. Each person who perpetrates outside Palestine one of the crimes provided for under this Law by Decree may be prosecuted in any of the following cases:
   a. If it is perpetrated by a Palestinian citizen.
   b. If is perpetrated against Palestinian parties or interests.
   c. If it is perpetrated against foreign parties or interests by a foreign national or a stateless person, whose habitual place of residence is within Palestine, or by a foreign national or a stateless person who is present in the Palestinian territory, but concerning whom the legal conditions of extradition are not fulfilled.

Article 3

1. A specialised cybercrime unit shall be established within the police agencies and security forces, provided that it enjoys the capacity of the judicial police. The Public Prosecution shall be responsible for supervising the officers vested with the judicial duties, each in the area of his jurisdiction.

2. Regular courts and the Public Prosecution, in accordance with their jurisdictions, shall hear cybercrime cases.

This document constitutes an un-official transcription/translation. DCAF cannot be held responsible for damages that may arise from its use. For official reference, please refer to the original text as published by the Palestinian Authorities.
DCAF's Assistance Programme for the Palestinian Security and Justice Sector
is supported by the German Federal Foreign Office.

DCAF Geneva Centre for Security Sector Governance

Page **3** of **15**

Article 4

1. Each person who deliberately and illegally accesses, by any means, an electronic website, system, electronic network or a means of information technology, or a part thereof, or exceeds the authorised access, or continues to be present therein after he becomes aware of his access, shall be punished by either or both confinement and a fine of not less than two hundred Jordanian dinars and not more than one thousand Jordanian dinars.

2. In the event the act provided for under Paragraph 1 of this Article is committed against government data, the penalty shall be either or both confinement for a term of not less than six months and a fine of not less than two hundred Jordanian dinars and not more than one thousand Jordanian dinars.

3. In the event the access results in cancelling, deleting, adding, disclosing, damaging, destroying, altering, transmitting, receiving, copying, publishing or republishing electronic data or information, which is stored in the information system, or causing damage to users or beneficiaries, or altering, eliminating, or modifying the contents of the electronic website, occupying its address, its designs or method of its use, or impersonating its owner or manager, the penalty shall be either or both temporary hard labour for a term that does not exceed five years and a fine of not less than one thousand Jordanian dinars and not more than five thousand Jordanian dinars or its equivalent in the legal currency of circulation.

4. In the event the act provided for under Paragraph 3 of this Article is committed against government data, the either penalty shall be or both temporary hard labour for a term that is not less than five years and a fine of not less than five thousand Jordanian dinars and not more than ten thousand Jordanian dinars or its equivalent in the legal currency of circulation.

Article 5

Each person who obstructs or disrupts, by any means, access to the service or access to devices, programmes or sources of data or information through the electronic network or a means of information technology shall be punished by either or both confinement and a fine of not less than two hundred Jordanian dinars and not more than one thousand Jordanian dinars or its equivalent in the legal currency of circulation.

Article 6

Each person who produces or introduces through the electronic network or a means of information technology any item that may suspend or disrupt its operation, or destroy, delete, damage or modify the programmes shall be punished by temporary hard labour and a fine of not less than five thousand Jordanian dinars and not more than ten thousand Jordanian dinars or its equivalent in the legal currency of circulation.

Article 7

Each person who receives, records, intercepts or wiretaps, on purpose and illegally, any data sent through the network or a means of information technology, shall be punished by either or both confinement and a fine of not less than one thousand dinars and not more than three thousand Jordanian dinars.

Article 8

1. Each person who decodes encrypted data in circumstances other than those permitted by law shall be punished by either or both confinement and a fine of not less than one thousand Jordanian dinars and not more than five thousand Jordanian dinars.

2. Each person who unlawfully uses personal encryption elements or an electronic signature creation device of another person shall be punished by either or both confinement and a fine of not less than two thousand Jordanian dinars and not more than five thousand Jordanian dinars.

3. Each person who commits a crime using any of the devices provided for under Paragraph 2 of this Article shall be punished by temporary hard labour and a fine of not less than two thousand Jordanian dinars or its equivalent in the legal currency of circulation.

Article 9

1. Each person who benefits illegally from communication services through a means of information technology or those alike shall be punished by either or both confinement for a term of not less than six months and a fine of not less than five hundred Jordanian dinars and not more than three thousand Jordanian dinars.

2. In case the benefit provided for under Paragraph 1 of this Article is intended for profit, the penalty shall be either or both confinement for a term of not less than one year and a fine of not less than one thousand Jordanian dinars and not more than five thousand Jordanian dinars.

Article 10

Each person who deliberately creates or publishes a false certificate, or presents false data about his identity to the competent authorities under the laws on the issuance of certificates for the purposes of applying for, cancelling or suspending a certificate, shall be punished by confinement and a fine of not less than two hundred Jordanian dinars and not more than one thousand Jordanian dinars or its equivalent in the legal currency of circulation.

Article 11

1. Each person who forges an official electronic document of the State or public entities or institutions, which is legally recognised within an information system, shall be punished by temporary hard labour for a term of not less than five years and a fine of not less than five thousand Jordanian dinars and not more than ten thousand Jordanian dinars or its equivalent in the legal currency of circulation.

2. In the event the forgery affects other documents and it may cause damage, the penalty shall be either or both confinement and a fine of not less than five hundred Jordanian dinars and not more than three thousand Jordanian dinars.

3. Each person who uses the forged document, knowing that it is forged, shall be liable to the penalty prescribed for the crime of forgery in due form.

4. Each person who forges or manipulates an official electronic signature or electronic signature device or systems, either by manufacturing, damaging, fault-finding, modifying, or transforming it or by any other means that leads to the alteration of the truth in its data or information, shall be punished by temporary hard labour for a term of not less than five years and a fine of not less than five thousand Jordanian dinars and not more than ten thousand Jordanian dinars or its equivalent in the legal currency of circulation.

5. In the event the forgery or manipulation affects other electronic signatures under Paragraph 4 of this Article, the penalty shall be either or both confinement and a fine of not less than five hundred Jordanian dinars and not more than three thousand Jordanian dinars.

6. Each person who develops data of an official electronic signature or device of an electronic signature system, or one that belongs to public entities or institutions shall not have the right to access it, using false or erroneous information or data, or collude with others to develop the same. [If he does so], he shall be punished by temporary hard labour

DCAF | Geneva Centre for Security Sector Governance

for a term of not less than five years and a fine of not less than five thousand Jordanian dinars and not more than ten thousand Jordanian dinars or its equivalent in the legal currency of circulation.

7. In the event other electronic signatures under Paragraph 4 of this Article are developed, the penalty shall be either or both confinement or a fine of not less than five hundred Jordanian dinars and not more than three thousand Jordanian dinars.

Article 12

1. Each person who uses the electronic network or a means of information technology in order to illegally access or manipulate numbers or data of an electronic transaction device, shall be punished by either or both confinement for a term of not less than six months and a fine of not less than five hundred Jordanian dinars and not more than three thousand Jordanian dinars.

2. Each person who forges an electronic transaction device by any means whatsoever, or manufactures or possesses without a licence devices or materials used in the issuance or forgery of an electronic transaction card shall be punished by the same penalty prescribed under Paragraph 1 of this Article.

3. Each person who knowingly uses or facilitates the use of a forged electronic transaction device, or knowingly accepts an invalid, forged or stolen electronic transaction device shall be punished by the same penalty prescribed under Paragraph 1 of this Article.

4. In case [such person] intends to use it to access funds and data of a third person, or the services made available through it, he shall be punished by either or both confinement for a term of not less than one year and a fine of not less than one thousand Jordanian dinars and not more than five thousand Jordanian dinars.

5. In case [such person] manages thereby to usurp for himself or for a third person the property of a third party, he shall be punished by either or both confinement for a term of not less than two years and a fine of not less than one thousand Jordanian dinars and not more than five thousand Jordanian dinars.

Article 13

Each person who uses the electronic network or a means of information technology to steal or extort funds shall be punished by either or both temporary hard labour and a fine of not less than two thousand Jordanian dinars and not more than five thousand Jordanian dinars.

Article 14

Each person who manages, through the electronic network or a means of information technology, to usurp for himself or for a third party a movable property, an electronic document, an electronic signature, or data for the creation of an electronic signature or electronic signature creation system, through the use of fraudulent means, or taking a false name or impersonating a false identity in a manner that may deceive the victim, shall be punished by either or both confinement for a term of not less than one year and a fine of not less than two thousand Jordanian dinars and not more than five thousand Jordanian dinars.

Article 15

1. Each person who uses the electronic network or a means of information technology to threaten or extort another person in order to compel him to perform an act or omission, even if such act or omission is lawful, shall be punished by either or both confinement and a fine of not less than two thousand Jordanian dinars and not more than five thousand Jordanian dinars.

This document constitutes an un-official transcription/translation. DCAF cannot be held responsible for damages that may arise from its use. For official reference, please refer to the original text as published by the Palestinian Authorities.
DCAF's Assistance Programme for the Palestinian Security and Justice Sector
is supported by the German Federal Foreign Office.
Page **6** of **15**

DCAF Geneva Centre for Security Sector Governance

2. In the event the threat entails the perpetration of a crime or the imputation of matters that are offensive to the honour or dignity, the penalty shall be temporary hard labour and a fine of not less than two thousand Jordanian dinars and not more than five thousand Jordanian dinars or its equivalent in the legal currency of circulation.

Article 16

1. Each person who produces, develops, prepares, sends or stores with the intention of exploiting, distributing or displaying to a third party through the electronic network, a means of information technology or animation, any matter that may violate public morals, shall be punished by either or both confinement for a term of not less than one year and a fine of not less than one thousand Jordanian dinars and not more than five thousand Jordanian dinars.
2. Each person who develops an electronic website, application or account, or publishes information on the electronic network or a means of information technology, calling for facilitating programmes and ideas that promote the violation of public morals shall be punished by either or both confinement for a term of not less than one year and a fine of not less than one thousand Jordanian dinars and not more than five thousand Jordanian dinars.
3. In case the act provided for under Paragraphs 1 and 2 of this Article targets a child, the penalty shall be temporary hard labour for a term of not less than seven years and a fine of not less than five thousand Jordanian dinars and not more than ten thousand Jordanian dinars or its equivalent in the legal currency of circulation.
4. In the event the content of the act provided for under Paragraph 1 of this Article is a child, appearance of a child, or simulated images of a child, the penalty shall be temporary hard labour for a term of not less than seven years and a fine of not less than five thousand Jordanian dinars and not more than ten thousand Jordanian dinars or its equivalent in the legal currency of circulation.

Article 17

Each person who creates an electronic website, application or account or disseminates information on the electronic network or a means of information technology with the intention of human trafficking and human organ trafficking or facilitates dealing in the same shall be punished by temporary hard labour for a term of not less than ten years and a fine of not less than ten thousand Jordanian dinars and not more than twenty thousand Jordanian dinars or its equivalent in the legal currency of circulation.

Article 18

Without prejudice to the provisions of the Law on the Combating of Money Laundering and the Financing of Terrorism, each person who creates an electronic website, application or account or disseminates information on the electronic network or a means of information technology with the intention of committing the crime of money laundering and financing of terrorism shall be punished by temporary hard labour for a term of not less than ten years and a fine of not less than ten thousand Jordanian dinars and not more than twenty thousand Jordanian dinars or its equivalent in the legal currency of circulation.

Article 19

Each person who creates or releases a website on the electronic network or a means of information technology with the intention of trafficking or smuggling narcotic drugs and psychotropic substances or those alike, or facilitates dealing in, sells, explains or displays the methods of producing narcotic drugs shall be punished by confinement for a term of not less

than ten years and a fine of not less not ten thousand Jordanian dinars and not more than twenty thousand Jordanian dinars or its equivalent in the legal currency of circulation.

Article 20

1. Each person who creates or manages an electronic website through the electronic network or a means of information technology to disseminate news that may put the State integrity, its public order or its internal or external security at risk, shall be punished by either or both confinement for a term of not less than one year and a fine of not less than one thousand dinars and not more than five thousand Jordanian dinars.
2. Each person who promotes, broadcasts or publishes, by any means, such news with the same intention, shall be punished by either or both confinement for a term of not more than one year and a fine of not less than two hundred Jordanian dinars and not more than one thousand Jordanian dinars.
3. In the event the act provided for under Paragraphs 1 and 2 of this Article occurs during the state of emergency, the penalty prescribed thereto shall be doubled.

Article 21

Each person who creates an electronic website, application or account or disseminates information on the electronic network or a means of information technology with the intention of abusing or cursing a holy shrine, rituals of religions or a religious belief shall be punished by either or both confinement for a term that is not less than one year and a fine of not less than two thousand Jordanian dinars and not more than five thousand Jordanian dinars.

Article 22

Each person who creates an electronic website, application or account or disseminates information on the electronic network or a means of information technology with the intention of encroaching on any family principles or values by releasing live or recorded news, images, audio or visual recordings relating to the sanctity of the private or family life of individuals – even if they were true, or attacks a third party by means of libel, slander or contempt, or defames and causes damage to others, shall be punished by either or both confinement for a term of not less than two years and a fine of not less than three thousand Jordanian dinars and not more than five thousand Jordanian dinars.

Article 23

Each person who creates an electronic website, application or account or disseminates information on the electronic network or a means of information technology with the intention of managing, facilitating, encouraging or promoting a gambling project or presents gambling games shall be punished by either or both confinement for a period of not less than six months and a fine of not less than one thousand Jordanian dinars and not more than five thousand dinars.

Article 24

Each person who creates an electronic website, application or account or disseminates information on the electronic network or a means of information technology with the intention of publishing and disseminating information that gives rise to racist discord and aims at the racial discrimination against a particular group, or threatens, disdains or encroaches on a person by reason of his race, sectarian affiliation colour, appearance or disability, shall be punished by temporary hard labour and a fine of not less than five thousand Jordanian dinars and not more than ten thousand Jordanian dinars or its equivalent in the legal currency of circulation.

This document constitutes an un-official transcription/translation. DCAF cannot be held responsible for damages that may arise from its use. For official reference, please refer to the original text as published by the Palestinian Authorities.
DCAF's Assistance Programme for the Palestinian Security and Justice Sector
is supported by the German Federal Foreign Office.
Page **8** of **15**

Article 25

Each person who creates an electronic website, application or account or disseminates information on the electronic network or a means of information technology with the intention of misrepresenting and justifying acts of genocide or crimes against humanity, which are prohibited by international conventions and laws, or deliberately assists or incites the perpetration of crimes against humanity, shall be punished by hard labour for life or temporary hard labour for a term that is not less than ten years.

Article 26

Each person who possesses, presents, produces, distributes, imports, exports or promotes a device for the purpose of use, or a programme or any ready-made electronic data, a password, or access codes for the purposes of perpetrating any of the crimes provided for under this Law by Decree, shall be punished by temporary hard labour for a term of not more than five years and a fine of not less than five thousand Jordanian dinars and not more than ten thousand Jordanian dinars or its equivalent in the legal currency of circulation.

Article 27

1. Each employee who commits any of the crimes provided for under this Law by Decree, exploiting his powers and authorities during or by virtue of the performance of their work, or facilitates the same for a third party, shall be punished by either or both confinement for a term of not less than one year and a fine of not less than five thousand Jordanian dinars and not more than ten thousand Jordanian dinars.
2. Each employee of service providers who commits any of the crimes provided for under this Law by Decree, exploiting his powers and authorities during or by virtue of the performance of their work, or facilitates the same for a third party, shall be punished by either or both confinement for a term of not less than three years and a fine of not less than ten thousand Jordanian dinars and not more than twenty thousand Jordanian dinars.

Article 28

Each person who creates an electronic website, application or account or disseminates information on the electronic network or a means of information technology with the intention of committing any crime that is punishable under any piece of legislation in force, or takes part in or incites its commission shall be punished by double the penalty prescribed by such legislation.

Article 29

1. Each person who incites, assists, or agrees with a third party to perpetrate a crime of those provided for by the provisions of the Law by Decree through any electronic means, and such a crime occurs on grounds of such incitement, assistance or agreement, shall be punished by two thirds of the maximum penalty prescribed for its culprit.
2. In the event the victim is a child in Paragraph 1 of this Article, the culprit shall be punished by temporary hard labour for a term of not less than five years and a fine of not less than two thousand Jordanian dinars and not more than five thousand Jordanian dinars or its equivalent in the legal currency of circulation, even if the crime does not actually occur.

Article 30

In the event a crime provided for under this Law by Decree is committed in its name or on its behalf, the juridical person shall be punished by a fine of not less than five thousand dinars

DCAF Geneva Centre for Security Sector Governance

and not more than ten thousand Jordanian dinars. The court shall be entitled to deprive the juridical person of performing its activity for a maximum period of five years or to rule for its dissolution, without prejudice to the criminal liability of the natural person affiliated therewith.

Article 31

Each person who uses electronic systems, an electronic website or an electronic application to bypass the block imposed in accordance with the provisions of this Law by Decree shall be punished by confinement for a term of not less than three months and a fine of not less than five hundred Jordanian dinars and not more than one thousand Jordanian dinars.

Article 32

In pursuance of the prescribed legal procedures, the service provider shall adhere to the following:
1. Provide the competent authorities with all necessary data and information which help to uncover the truth, at the request of the Public Prosecution or the competent court.
2. Block the link or content or application on the electronic network, based on the orders issued forth thereto from judicial authorities, taking account of the procedures provided for under Article 40 of this Law by Decree.
3. Keep the subscriber's information for a period of not less than three years.
4. Cooperate with and assist the competent authorities in the collection or recording of electronic information or data and keep them temporarily, based on a decision from the judge of the competent court.

Article 33

1. The Public Prosecution or the officers tasked with judicial duties, whom it delegates, shall be entitled to search persons, places and information technology systems relating to crime.
2. The search warrant must be reasoned and specific. It may be renewed more than once as long as the justifications of such procedure still exist.
3. In the event the search provided for under Paragraph 2 of this Article leads to seizing devices, tools or means relating to the crime, the officers vested with judicial duties must compile a report of the seized items and present them to the Public Prosecution in order to take necessary measures thereon.
4. The prosecutor shall be entitled to permit direct access for the officers vested with judicial duties, or to seek assistance from the experts whom they deem fit, to access and search any information technology system with the intention of accessing data or information.
5. The officer vested with judicial duties shall be required to be qualified to deal with the special nature of cybercrime.

Article 34

1. The Public Prosecution shall be entitled to obtain the electronic devices, tools, means, data, information, traffic data, data relating to communication traffic or their users, or relevant content information with relevance to cybercrime.
2. The Public Prosecution shall be entitled to permit the seizure and restraint of the information system either wholly or partly or any means of information technology, which may help to uncover the truth.
3. In case seizure and restraint of the information system is not necessary or impossible to perform, the data or information relating to the crime as well as the data which secures its reading and comprehension shall be copied on a means of information technology.

4. In case it is impossible to perform the seizure and restraint in actuality, to preserve evidence of the crime, all appropriate means must be used to prevent access to the data stored in the information system.
5. Necessary precautions shall be taken to maintain the integrity of the seized items, including technical tools to protect their content.
6. As much as possible, a list of the seized and restrained items shall be compiled in the presence of the accused or the person in whose custody the seized and restrained items were located. A report shall be drawn up to that effect. The seized items shall be kept, as the occasion may be, in a container or a sealed envelope, on which a paper, stating in writing the date and time of seizure, number of reports and the case.

Article 35

1. The competent judge of the Court of Conciliation shall be entitled to permit the Public Prosecution to conduct surveillance of, and deal with, communications and electronic conversations in order to search for the evidence relating to the crime for a period of fifteen days that is renewable once, based on the availability of new evidence. The person who conducts the search, surveillance or recoding must compile a report thereon and submit it to the Public Prosecution.
2. The Public Prosecution shall be entitled to issue an order to immediately collect and provide any data, including communication traffic, electronic information, traffic data or content information which it deems necessary for the benefit of the investigations, using the proper technical tools and, where applicable, to seek assistance from service providers depending on the type of the service they deliver.

Article 36

The competent authorities must take the measures and procedures to ensure the preservation of the integrity and privacy of the devices, tools, means of information technology, information systems or electronic information, which are the subject of seizure, until such time a relevant decision is rendered by the judicial authorities.

Article 37

1. The competent court shall be entitled to permit the immediate interception, recording or copying of the content of communications at the behest of the Attorney General or one of his assistants. The court decision shall include all the elements which may identify the communications, the subject matter of the application for interception, as well as the acts which necessitate it and its duration.
2. The duration of interception provided for under Paragraph 1 of this Article shall last for three months, starting from the date of its actual commencement. It shall be renewable only once.
3. The authority assigned to implement the permission of interception must notify the Public Prosecution of the actual date of launching the interception process and coordinate with it in regard of taking the necessary measures to ensure its smooth progress.

Article 38

Any piece of evidence that results from a means of information technology, information systems, information networks, electronic websites, or electronic data and information may not be excluded by reason of the nature of such evidence.

This document constitutes an un-official transcription/translation. DCAF cannot be held responsible for damages that may arise from its use. For official reference, please refer to the original text as published by the Palestinian Authorities.
DCAF's Assistance Programme for the Palestinian Security and Justice Sector
is supported by the German Federal Foreign Office.
Page **11** of 15

DCAF | Geneva Centre for Security Sector Governance

Article 39

Any piece of evidence that is obtained by the competent authority or investigation authorities from other states may not be excluded merely for such a reason, as long as it has been obtained in accordance with the legal and judicial procedures of international cooperation.

Article 40

1. The competent authorities of investigation and seizure, in the event they monitor hosted electronic websites, which broadcast either inside or outside Palestine, posting any expressions, figures, images, films, propaganda materials or others which may threaten national security, community safety, public order or public morals, shall be entitled to submit a report thereon to the Attorney General or one of his assistants and request permission to block the broadcast of the website(s) or block some of their links.
2. The Attorney General or one of his assistants shall submit the application for a permission to the Court of Conciliation within 24 hours, enclosed with a notice of his opinion. The Court shall render its decision on the application on the same day it is brought before it, stating either acceptance or rejection.

Article 41

Apart from the professional obligations provided for under this Law, professional secrets or relevant requirements may not be invoked to refrain from the submission of information or documents, which are requested in accordance with the provisions of the Law.

Article 42

The State agencies, institutions, entities and the bodies and companies affiliated therewith shall abide by the following:

1. Take the preventative security measures necessary to protect their own information systems, electronic websites, information networks and electronic data and information.
2. Promptly notify the competent authority of any crime provided for under the Law by Decree as soon as it is detected or any attempt of unlawful reception, interception or wiretapping is detected, and provide the competent authority with all relevant information to uncover the truth.
3. Keep information technology data and subscriber's information for a period of not less than 120 days and provide the competent authority with such data.
4. Cooperate with the competent authority to implement their powers.

Article 43

1. The competent authorities shall work towards facilitating cooperation with their counterparts in foreign countries within the framework of approved international, regional and bilateral agreements or in conformity with the principle of reciprocity with a view to expediting information exchange, ensuring the early warning of cybercrime and communications offences, avoiding their perpetration, and helping to investigate them and prosecute their perpetrators.
2. The cooperation referred to under Paragraph 1 of this Article shall depend on the concerned foreign state's commitment to keep secret the information transferred thereto and its commitment not to transfer it to a third party or exploit it for other purposes than the combating of the crimes specified under this Law by Decree.

Article 44

1. The competent authorities must provide assistance to counterpart agencies in other states, for the purposes of offering mutual legal aid and extraditing criminals in the investigations

This document constitutes an un-official transcription/translation. DCAF cannot be held responsible for damages that may arise from its use. For official reference, please refer to the original text as published by the Palestinian Authorities.
DCAF's Assistance Programme for the Palestinian Security and Justice Sector
is supported by the German Federal Foreign Office.
Page **12** of **15**

DCAF Geneva Centre for Security Sector Governance

and criminal proceedings associated with the crimes provided for under this Law by Decree, in accordance with the rules which are prescribed by the Penal Procedure Law, bilateral or multilateral agreements to which the State is a party or the principle of reciprocity, without prejudice to the provisions of this Law by Decree or any other law.

2. The application for legal aid or application for the extradition of criminals, in reference of the provisions of this Law by Decree, shall only be executed in the event the laws of the applicant state and laws of the State penalise the crime the subject matter of the application or a similar crime. Dual criminality shall be deemed to be fulfilled in disregard of whether the laws of the applicant state include the crime within the category of the same crimes or uses in the designation of the crime the same term used in the State, on condition that the act the subject matter of the application is incriminated in pursuance of the laws of the applicant state.

Article 45
Without prejudice to any more aggravated penalty provided for by the Penal Law in force or any other law, the perpetrators of the crimes punishable in accordance with the provisions of this Law by Decree shall be liable to the penalties prescribed thereunder.

Article 46
Each person who perpetrates an act that constitutes a crime under any effective piece of legislation using the electronic network or a means of information technology, or is involved as an accomplice, abettor or accessory to its perpetration, shall be liable to the same penalty which is prescribed for such crime under that piece of legislation.

Article 47
Each person who creates a website on the electronic network with the aim of promoting the perpetration of any crime provided for under the Penal Law or any special law shall be punished by temporary confinement and a fine of not less than five thousand Jordanian dinars and not more than ten thousand Jordanian dinars.

Article 48
Each person who discloses the confidentiality of the procedures provided for under this Law by Decree in cases other than those legally authorised, shall be punished by either or both confinement and a fine of not less than five hundred Jordanian dinars and not more than three thousand Jordanian dinars.

Article 49
Each person who violates, damages, conceals, modifies or erases judicial information evidence, shall be punished by confinement for a term of not less than one year and a fine of not less than one thousand Jordanian dinars and not more than five thousand Jordanian dinars or its equivalent in the legal currency of circulation.

Article 50
Each person who deliberately refrains from reporting or falsely reports on purpose cybercrimes, shall be punished by either or both confinement for a term of not less than six months and a fine of not less than two hundred Jordanian dinars and not more than one thousand Jordanian dinars.

This document constitutes an un-official transcription/translation. DCAF cannot be held responsible for damages that may arise from its use. For official reference, please refer to the original text as published by the Palestinian Authorities.
DCAF's Assistance Programme for the Palestinian Security and Justice Sector
is supported by the German Federal Foreign Office.
Page **13** of **15**

DCAF | Geneva Centre for Security Sector Governance

Article 51

In the event any crime provided for under this Law by Decree is perpetrated for the purpose of violating public order, endangering the society's integrity and security, putting the lives of citizens at risk, preventing or obstructing the public authorities from exercising their functions, disrupting the provisions of the Constitution, Basic Law, laws or bylaws, or with the intention of undermining national unity and community safety, showing contempt at religions, or encroaching on the rights and freedoms enshrined in the Constitution or Basic Law, the penalty shall be hard labour for life or temporary hard labour.

Article 52

Whoever takes part by means of an agreement, incitement, assistance or intervention in the perpetration of a crime or a misdemeanour that is punishable in accordance with the provisions of this Law by Decree shall be liable to the same penalties which are prescribed for the original perpetrator. In case the crime has not occurred, they shall be liable to half of the penalty prescribed thereto.

Article 53

Each person who attempts to perpetrate a crime or misdemeanour of those provided for under this Law by Decree shall be deemed to be a perpetrator of a crime and shall be liable to half of the penalty prescribed thereto.

Article 54

1. Without prejudice to the penalties prescribed under this Law by Decree, as well as the rights of a *bona fide* third party, the Court shall render a decision to confiscate the devices, programmes or means used in the perpetration of any of the crimes prescribed under this Law by Decree or the funds obtained therefrom, provided that the violation is removed at the expense of the perpetrator.
2. The Court shall render a decision, stating the duration of the closure of the premise or blocking of the electronic website, in or by means of which such crimes were perpetrated, as the occasion may be.

Article 55

The penalty provided for under this Law by Decree shall be doubled in the event the culprit repeats any of the prescribed crimes, regardless of whether they are perpetrated inside or outside Palestine. Foreign judgements shall be deemed to be a precedent in recidivism against the culprit.

Article 56

The penalty prescribed for the crimes which are punishable in accordance with the provisions of this Law by Decree shall be doubled in any of the following cases:
1. In case an employee at a private institution or a public servant or those of similar standing perpetrates them or facilitates their perpetration, exploiting their powers and authorities to that effect. A judgement shall also be rendered to dismiss the public servant from public service in the event of conviction.
2. In case the crime is committed against a website, information system, data, figures, letters, codes or images that are managed by the State, a public juridical person, or [an entity] owned by or belonging to it, including local government units.
3. In case the culprit perpetrates the crime through an organised gang.
4. In case children and those alike are misled and exploited.

DCAF | Geneva Centre for Security Sector Governance

5. In case the crime is perpetrated against an information system, electronic website or information network and relates to the transfer of funds, provision of payment services, clearance, reconciliations or any banking services delivered by banks and financial institutions.

Article 57

Each culprit who takes the initiative to notify the competent authorities of any information on the crime and the accomplices therein before the authorities are aware of it and before damage is caused shall be exempted from the penalties provided for under this Law by Decree. The court may rule for the stay of execution of the penalty in the event the notification takes place after the competent authorities are aware [of the crime], whereby it leads to the arrest of the rest of the culprits.

Article 58

The Ministry shall, in accordance with its jurisdiction, provide support and technical assistance to the law enforcement agencies. The Ministry staff, who are appointed by the Minister, shall be deemed to be officers vested with judicial duties for the purposes of the enforcement of the provisions of this Law by Decree.

Article 59

All provisions that contradict the provisions of this Law by Decree shall be repealed

Article 60

This Law by Decree shall be presented to the Legislative Council in the first session it convenes for approval.

Article 61

All the competent authorities, each one within its sphere of jurisdiction, shall implement the provisions of this Law by Decree, which shall enter into force as of the date of its publication in the Official Gazette.

Issued in the city of Ramallah on June 24th, 2017 *Anno Domini*,
Corresponding to Ramadan 29th, 1439 *Anno Hegira*.

Mahmoud Abbas
President of the State of Palestine
Chairman of the Executive Committee of the Palestine Liberation Organisation

This document constitutes an un-official transcription/translation. DCAF cannot be held responsible for damages that may arise from its use. For official reference, please refer to the original text as published by the Palestinian Authorities.
DCAF's Assistance Programme for the Palestinian Security and Justice Sector
is supported by the German Federal Foreign Office.
Page **15** of **15**

DCAF Geneva Centre for Security Sector Governance