

No. of year

Jordanian Legislation

Law Number Year

Legislation and
Opinion Bureau

Cybersecurity law

Published on page 5143 of Official Gazette number 5595 dated 09/16/2019

Article 1

This law is called (Cyber Security Law of 2019) and it shall be enforced from the .date of its publication in the Official Gazette

Article 2

The following words and expressions, wherever mentioned in this law, shall have :the meanings assigned to them below, unless the context indicates otherwise

An environment consisting of the interaction of people, data and information, the information system and programs on information: Cyber space .networks, communication systems and related infrastructure

The measures taken to protect critical systems, information networks and infrastructure from cyber security incidents and the ability to restore their work and continuity, whether access to them without permission or misuse or as a result of failure to follow security measures: .or exposure to deception that leads to this

Cyber
security

The permission granted by the person concerned to one or more persons or the public to enter or use the information system or the information network with the intention of viewing, canceling, deleting, adding, changing, or republishing data or information, withholding access to it, stopping the work of the devices, changing a website .or Cancellation or modification of its contents

The
declaration



Figures, letters, symbols, shapes, sounds, pictures or drawings that are not significant in themselves ;	data
The data that has been processed has become significant:	the information
The set of programs and tools designed to create data or information electronically, to send: receive, process, store, manage or display it by electronic means ,	Information system
A link between more than one information system to make data and information available and obtain it	Informational networks
The set of systems, electronic networks, tangible and intangible assets or cyber assets and systems whose continuous operation is necessary to ensure the security of the state, its economy, and the safety of society	Critical infrastructure
A set of orders and technical instructions intended to accomplish a task that can be implemented using information systems	Programs
An action or attack that poses a threat to data, information, information systems, the information network, or related infrastructure and requires a response to stop it or to mitigate its consequences or effects	Cyber security incident
A set of procedures related to managing, monitoring and detecting cyber security incidents and threats that fall within the cyberspace: space, developing response plans and implementing them	Cyber security operations
Technical, administrative, and consulting activities in the field of cybersecurity, including security assessment, monitoring, auditing: and consulting services	Cyber security services

Article 3

- A- A council called (the National Council for Cyber Security) shall be formed in the Kingdom, consisting of a president appointed by a high royal will and a number of members representing the following bodies
- 1 The Ministry of Digital Economy and Entrepreneurship
 - 2 The Central Bank of Jordan
 - 3 Jordanian Armed Forces - Arab Army
 - 4 General Intelligence Department
 - 5 General Security Directorate
 - 6 The National Center for Security and Crisis Management
 - 7 Three members appointed by the Council of Ministers upon the recommendation of the Speaker for a period of two years, renewable once, provided that two of them are experienced from the private sector
- B- The council shall choose from among its members at its first meeting a deputy chairman of the council, who will take his place in his absence
- C- The council meets at the invitation of its chairman or deputy four times a year or whenever the need arises, and its meeting is legal in the presence of no less than two thirds of its members and makes its decisions by a majority of the votes of its members present
- D- The president of the council may invite any person to attend the council's meeting to seek his opinion on the matters presented to him without having the right to vote



G- Notwithstanding what is stated in Paragraph (C) of this Article and in exceptional cases estimated by the Speaker or his deputy in his absence, a meeting of the Council may take place in the presence of at least four of the members stipulated in clauses (1) to (6) of the paragraph (A) of this Article, and the decision is legally binding, provided that the remaining members of the Council are notified of it in the first meeting that follows it in which the quorum is complete

Article 4

: The council assumes the following duties and powers

- A- Approving strategies, policies and standards related to cybersecurity
 - B- Approving the plans and programs necessary for the center to perform its duties and duties, including international and regional cooperation programs
 - C - Approving the quarterly reports on the Kingdom's cyber security situation and the annual report on the work of the Center
 - D - Forming the coordinating committees from the stakeholders to enable the center to achieve its goals, provided that in its formation decision it determines its tasks and duties, and how its meetings are held and its decisions are taken
 - E- Approving the center's annual budget
-

Article 5

- A- A center called (the National Center for Cyber Security) shall be established in the Kingdom, enjoying a legal person with financial and administrative independence, and in this capacity he possesses movable and immovable funds and undertakes all legal actions necessary to achieve his goals, including the conclusion of contracts, and he has the right to litigate and is represented in judicial proceedings by an administration agent State issues
 - B - The center is linked to the Prime Minister
 - C - The center shall be located in the city of Amman, and it may open branches in the governorates of the Kingdom
-

Article 6

A- The center aims to build, develop, and organize an effective cybersecurity system at the national level to protect the Kingdom from the threats of cyberspace and confront them efficiently and effectively so as to ensure the sustainability of work and maintain national security and the safety of people, property and information

B - In order to achieve its goals, the center will assume the following tasks and powers:

1- Preparing cybersecurity strategies, policies and standards, monitoring their implementation, setting plans and programs necessary for their implementation, and submitting them to the Council for approval

2- Developing and implementing cyber security operations and providing the



- Defining cybersecurity standards and controls and classifying cyber security -3
.incidents according to instructions issued for this purpose
- Granting a license to cybersecurity service providers in accordance with the -4
requirements, conditions and fees specified under a system issued for this
.purpose
- Exchange information, activate cooperation and partnerships, conclude -5
agreements and memoranda of understanding with national, regional and
.international bodies related to cybersecurity
- Developing the necessary programs to build national capabilities and -6
experiences in the field of cybersecurity and to enhance awareness of it at the
.national level
- Cooperation and coordination with the relevant authorities to enhance -7
.cyberspace security
- Preparing draft legislations related to cyber security in cooperation with the -8
.concerned authorities and submitting them to the Council
- Continuous evaluation of the cyber security situation in the Kingdom in -9
.cooperation with the concerned authorities in the public and private sectors
- .Identify critical infrastructure networks and their sustainability requirements -10
- .Create a database with cyber threats -11
- .Evaluating the security aspects of e-government services -12
- .Evaluating and developing cyber security incidents response teams -13
- .Preparing a policy that includes information security and protection standards -14
- Supporting scientific research in the fields of cybersecurity in cooperation with -15
.universities
- .Conduct cybersecurity exercises and competitions -16
- Preparing the Center's annual draft budget, the annual report on its activities -17
.and the final financial statements
- Prepare quarterly reports on the Kingdom's cyber security situation and submit .18
.them to the Council
- Any other tasks or powers stipulated in the regulations and instructions issued -19
.according to the provisions of this law

Article 7

A- The Center shall appoint a president with experience and specialization in the field of cybersecurity for a period of four years, renewable for one time, by a decision of the Prime Minister upon the recommendation of the President of the Council, provided that the appointment decision is accompanied by a royal royal will, and his salary and other financial rights shall be specified in his appointment .decision

.B- The head of the center represents the center with others

C - The manner in which the center is run, other affairs related to it, and the .functions of its president are determined by a system issued for this purpose



Article 8

A- The center receives complaints and intelligence related to cyber security and cyber security incidents, and it has the right to follow them and take appropriate action to address them and prevent them from occurring or continuing according to the powers granted to them.

B- Ministries, government departments, official, public, private and private institutions shall abide by the following:

Follow the policies, standards and controls issued by the Center for each sector - 1 in accordance with the provisions of this law and the regulations and instructions issued pursuant to it.

Providing the center with the necessary information to enable it to carry out its work in a manner that does not conflict with the laws in force - 2

Inform the center of any incident that threatens cybersecurity or related to cyberspace security and do everything necessary to avoid its occurrence - 3

C- The center works with the General Intelligence Department when preparing strategies and policies, building systems and purchasing services necessary to perform its duties.

Article 9

A- The Cyber Security Incident which poses a threat to the Kingdom's security and safety shall be determined by a decision of the Council upon the recommendation of the Center's head.

B- The center shall be responsible for managing and directing the response to cyber security incidents referred to in paragraph (a) of this article, and all authorities shall abide by the instructions and directions issued by the center.

Article 10

A- Any person or entity is prohibited from providing any of the cybersecurity services without obtaining the necessary license in accordance with the provisions of this law and the regulations and instructions issued pursuant thereto.

B- The entities and persons that provide cybersecurity services in the Kingdom should correct their conditions according to the provisions of this law and the regulations and instructions issued pursuant thereto.

Article 11

A- The Council of Ministers, upon the recommendation of the Speaker, authorizes any supervisory body, government department, or official or public institution to perform some of the Center's tasks and powers specified in the provisions of this law and the regulations and instructions issued pursuant thereto.

B - The authorities referred to in Paragraph (A) of this Article shall submit periodic reports to the Center on the work assigned to them and whenever the need arises, as they shall inform the Center immediately upon the occurrence or suspect of a cyber security incident.



Article 12

Information, data and documents and their copies that are returned to the center or related to its work or viewed by its employees are considered protected documents to which the provisions of the Law on Protection of State Secrets and Documents

Article 13

A- The head of the center and the employees authorized from him in writing for the purposes of carrying out their duties shall have the capacity of the judicial police, and they shall have the right to enter and search any place indicating that he performs any of the practices that constitute a threat or a breach of cyber security. Evidence that they will be used to commit and maintain any of these .practices and that they should regulate violators

B - The employee who inspected or seized it according to the provisions of Paragraph (A) of this Article must submit a report to that effect to the Center's .head

Article 14

- :The financial resources of the Center consist of the following

.A- What is provided for in the general budget

B- Aids, gifts, donations, grants and any other resources accepted by the Council, provided that the Council of Ministers approves it if it comes from a non-Jordanian .source

.C- Fees and charges for services provided by the center

. D- The outcome of the fines imposed by the Center

Article 15

A - The center's funds and rights with others are considered public funds that are .collected according to the provisions of the Public Funds Collection Law

B - The center enjoys the exemptions and facilities enjoyed by ministries and .government departments

Article 16

A- The Center may take one or more of the following procedures against those who violate the provisions of this law, regulations, instructions and decisions issued pursuant thereto in a manner commensurate with the nature of the - :violation and the party that committed it

.Written warning to correct the violation within the specified period -1

Correcting the violation and referring the violator to the expenses incurred by -2
the center as a result



Blocking, canceling, confiscating or disrupting the communication network, the -3
information system, the information network, the private communication devices
and electronic messages with the relevant authorities from all those suspected of
.committing or participating in any act that constitutes a cyber security incident

Obliging the violating party to take legal measures against those found to have -4
.caused the violation from its employees

Cancellation or suspension of the licensee's license to provide any of the -5
.cybersecurity services for the period deemed appropriate by the center

Imposing a fine of no less than (500) dinars and not exceeding (100,000) dinars, -6
.and the fine shall be doubled in case of repetition of the violation

B- For the purposes of implementing the provisions of paragraph (a) of this Article,
the Council shall issue instructions specifying the standards, controls and
.procedures due to the violations of the violations

Article 17

A- The civil service system, the financial system, the supplies system, the works
system, the transportation system and the travel system in place with ministries
and government departments and any systems that replace them, shall be applied
to the center, and for this purpose the center president shall exercise the powers
of the minister, the concerned minister and the general secretary, and the council
.will exercise the powers of the cabinet stipulated in those regulations

B- Taking into consideration the legislation in force, the head of the center may
request that any of the employees of the Jordanian Armed Forces and the security
services be attached to work in the center and with the approval of these
. authorities

C- The center may grant rewards or financial incentives to any of the employees or
those attached to it according to instructions issued by the council upon the
.recommendation of the center president

Article 18

The Council of Ministers shall issue the necessary regulations to implement the
.provisions of this law

Article 19

.Prime Minister and Minister in charge of implementing the provisions of this law



المملكة الأردنية الهاشمية
ديوان التشريع و الرأي



SUBSCRIBE TO NEWSLETTER



CONTACT US

Location: Amman Fourth Circle

POBox: 5694

PostalCode: 11183

phone: (962) 6 5622266

phone: (962) 6 5622201

Email: dewanlob@lob.gov.jo

Site Map

SUGGESTIONS AND INQUIRIES