Cyber Security Law
Law No. (16) of 2019

Article (1) : This Law shall be cited as the (Cyber Security Law for the Year 2019) and shall come into force as of the date of its publication in the Official Gazette.

Article (2) : The following words and expressions, wherever they appear in this law, shall have the meanings designated hereunder below unless the context indicates otherwise.

Cyberspace : An environment consisting of the interaction of persons, data, information, information system, programs on information networks, telecommunications systems and the infrastructure related thereto.

Cyber Security : The measures taken to protect information systems and networks and critical infrastructures from Cyber Security incidents and the ability to return them to their running order and continuation; notwithstanding whether those were accessed without authorization, by misuse or as a result of failing to follow security measurers or being subject to deception leading thereto.

Authorization : The permission given by the related person to a person or more or to the public to access or use an Information System or the Internet with the intention of viewing, deleting, cancelling, adding to, changing, or republishing information or data, blocking access thereto, suspending the operation of devices or changing, closing or modifying the content of a website.

The Council : The National Cyber Security Council.

The Center : The National Cyber Security Center.

Data : Numbers, letters, symbols, forms, sounds, images or drawings which does not have a meaning by its own.

Information : Data that has been processed and became meaningful.

Information System : A group of programs and devices set out for electronically creating, sending, receiving, processing, storing, managing, or displaying data or information in electronic means.

Information Networks	:	A connection between more than one Information System to make available and receive Data and Information.
Critical Infrastructure	:	The set of electronic systems and networks and material and non-material assets or cyber assets and systems the continuous operation of which is necessary to ensure the security of the state and its economy and the safety of the society.
Programs	:	A group of technical orders and instructions designated for completing an accomplishable mission using Information Systems.
Cyber Security Incident	:	The act or attack that represents a risk to data, information, Information Systems, Internet, or infrastructure related thereto and requires a response to suspend or to minimize the consequences or effects thereof.
Cyber Security Operations	:	A set of procedures related to the management, monitoring and discovery of Cyber Security incidents and the threats within Cyberspace and place response plans thereto and the application thereof.
Cyber Security Services	:	Technical, administrative and consultative activities in the field of Cyber Security including security evaluation, monitoring, audit and consultancy services.

Article (3) : A. A Council shall be formed in the Kingdom to be called (the National Cyber Security Council); it shall consist of a chairman to be appointed by a Royal Decree and a number of members representing the following entities:

1. The Ministry of Digital Economy and Entrepreneurship.
2. The Central Bank of Jordan
3. Jordan Armed Forces- Arab Army.
4. General Intelligence Department.
5. Public Security Directorate.
6. National Center for Security and Crisis Management.
7. Three members to be nominated by the Council of Ministers upon the proposal of the Chairman of the Council for a term of two years, renewable for one term and provided that two of them be experienced

persons from the private sector.

B. In the first meeting thereof, the Council shall elect from among its members a Deputy Chairman who shall substitute the Chairman in his absence.

C. The Council shall hold its meetings upon the invitation of its Chairman or the Deputy Chairman four times a year or as needed, the meeting shall be deemed legally convened if attended by at least two thirds of the members and decisions shall be taken with the majority voting of attending members.

D. The Chairman of the Council may invite any person to attend a meeting of the Council in order to provide an opinion on the issues put before the Council, such person shall not have the right to vote.

E. The Chief Officer of the Center shall attend the meetings of the Council but shall have no voting right.

F. The Chief Officer of be Center shall nominate an employee of the Center as a secretary for the Council, the so appointed employee shall be in charge of organizing the agenda of the Council, recoding the minutes of its meetings, the safekeeping of its records and logs, following up on the execution of its decisions and any other works entrusted thereto by the Chairman of the Council.

G. Notwithstanding the provisions of Paragraph (C) of this Article and in exceptional cases as determined by the Chairman of the Council or the Deputy thereof in case of his absence, the Council may convene a meeting with the attendance of at least four of the members provided in items (1) to (6) of Paragraph (A) of this Article; the decision shall be legally binding provided that other members of the Council are informed therewith in the next meeting convened with the stipulated forum.

Article (4) : The Council shall assume the following duties and have the following authorities:

A. Approving strategies, policies and standards relevant to Cybers Security

B. Approving plans and programs needed for the Center to perform its duties and responsibilities thereof including international and regional cooperation programs.

C. Approving quarterly reports concerning the Cyber Security status in the

Kingdom and the annual report of the Center.

D. Forming coordinating committees from concerned entities in order for the Center to achieve the objectives thereof provided that their duties and responsibilities shall be specified in their formation resolution in addition to holding their meetings and the issuance of their resolutions.

E. Approving the annual budget of the Center.

Article (5) :

A. A center shall be established in the Kingdom under the name of (the National Center for Cyber Security); the Center shall enjoy juridical personality and administrative and financial independence, and in such capacity the Center shall be eligible to acquire ownership of movable and immovable monies and conduct all transactions as required for the realization of its objectives including entering into contracts. The Center shall also have the right to litigate and shall be represented in any judicial proceedings by the Governmental Cases Management Attorney.

B. The Center shall be affiliated with the Prime Minister.

C. The office of the Center shall be in the city of Amman and it may open branches in the governorates of the Kingdom.

Article (6) :

A. The Center aims at building, developing and organizing an effective system for Cyber Security on national level to protect the Kingdom from Cyber Security threats and encounter them with efficiency and effectiveness to ensure sustainability of operation and protection of national security and safety of persons, properties and Information.

B. In course of achieving its' objectives, the Center shall assume the following duties and authorities:

1. Preparing strategies, policies and standards for Cyber Security, observing the application thereof, putting plans and programs as required for their execution and refer the same to the Council for approval.

3. Developing and executing Cyber Security operations and providing the support and consultation needed to build Cyber Security Operations teams both in private and public sectors and coordinating the efforts for

responding thereto and interfering when necessary.

4. Setting the Cyber Security standards and conditions and classifying Cyber Security incidents in accordance with instructions to be issued for this purpose.
5. Giving licenses to the providers of Cyber Security services based on the set requirements, conditions, and fees according to regulations to be issued for this purpose.
6. Exchanging information, enacting cooperation and partnerships and entering into agreements and memoranda of understanding with national, regional and international organizations concerned with Cyber Security.
7. Developing the programs needed to build national capacities and experience in the area of Cyber Security and enhancing awareness thereof on the national level.
8. Cooperating and coordinating with related entities to enhance the security of Cyberspace.
9. Preparing draft legislations relevant to Cybersecurity in coordination with the relevant entities and submitting the same to the Council.
10. Continuously evaluating the status of Cyber Security in the Kingdom in cooperation with the relevant entities both in private and public sector.
11. Specifying Critical Infrastructure Networks and the requirements of its sustainability.
12. Establishing a database regarding cyber threats.
13. Evaluating the security aspects of electronic government services.
14. Evaluating and developing Cyber Security Incidents resilience teams.
15. Preparing a policy containing the standards for information security and protection.
16. Supporting scientific research in the field of Cyber Security in cooperation with universities.
17. Conducting exercises and competitions related to Cyber Security.
18. Preparing the draft annual budget of the Center, the annual report thereto

and the closing financial statements.

19. Preparing quarterly reports on the Cybersecurity status of the Kingdom and submit the same to the Council.
20. Any other duties or authorities as provided in the bylaws and the instructions issued pursuant to the provisions of this Law.

Article (7) :

A. A Chief Officer with experience and competence in the field of Cybersecurity shall be appointed for the Center for a term of four years, renewable for one term only; by a decision from the Prime Minister upon the recommendation of the Chairman of the Council , and provided that the appointment decision shall be sanctioned by a Royal Decree. The salaries and other financial entitlements of the Chief Officer shall be provided in the appointment decision thereof.

B. The Chief Officer of the Center shall represent the Center before third parties.

C. The method of managing the Center and other issues relevant thereto, and the duties of the Chief Officer thereof shall be determined in a bylaw to be issued for this purpose.

Article (8) :

A. The Center shall receive complaints and reports relevant to Cyber Security and Cyber Security incidents, and may follow up on the same and take the appropriate measure to prevent the reoccurrence or the continuation thereof as per the authorities granted thereto.

B. Ministries, Governmental departments and official; public; private; and non-governmental entities shall:

1. Abide by the policies, standards and conditions issued by the Center for each sector in accordance with the provisions of this Law and the bylaws and instructions issued pursuant thereto.
2. Provide the Center with the information needed to enable the same of performing its duties to the extent that this is not in contradiction with the laws in force.
3. Report any incident threatening Cyber Security or related to Cyberspace

to the Center and take all measures needed to avoid its occurrence.

C. The Center shall work with the General Intelligence Department when in course of preparing strategies and policies and establishing systems and purchasing services needed for the disposal of its duties.

Article (9) :

A. A Cyber Security incident that represents a threat to the security and integrity of the Kingdom shall be determined by a decision of the Council upon the proposal of the Chief Officer of the Center.

B. The Center shall be responsible for managing and directing the response to Cyber Security incidents provided in Paragraph (A) of this Article and all entities shall abide by the instructions and directions issued by the Center.

Article (10) :

A. It shall be prohibited for any person or entity to provide any Cyber Security Services without obtaining the required license as per the provisions of this Law and the bylaws and instructions issued pursuant thereto.

B. All entities and persons who provide Cyber Security Services in the Kingdom must rectify their status according to the provisions of this Law, the bylaws and instructions issued pursuant thereto

Article (11) :

A. The Council of Ministers may, upon the proposal of the Chairman of the Council, delegate to any regulatory authority, governmental department or official or public entity some of the duties and authorities of the Center as provided under the provisions of this Law and the bylaws and instructions issued pursuant thereto.

B. Entities provided in Paragraph (A) of this Article shall submit periodic reports to the Center concerning the duties delegated thereto and as needed, those entities shall also inform the Center in case of an actual or suspected occurrence of any Cyber Security incident.

Article (12) : Information, data, documents and their copies that are received by the Center, or related to its work or seen by those who work at the center are considered protected documents and are subject to the provisions of the Law of Protecting the Secrets and Documents of the State.

Article (13) : A. The Chief Officer of the Center and the employees delegated thereby in writing shall, for the purposes of disposition of their duties, have the capacity of judicial police and shall have the right to enter to and investigate any place were indications suggest that it is being used for any practices that threats or breaches Cyber Security, and shall have the right to confiscate apparatus, equipment, devices, programs, Information Systems and Internet that indicators suggest are being used to commit any of the mentioned practices and keep them, and shall prepare a report in relation of such breaches.

B. The employee who undertook investigation or confiscation as per the provision of Paragraph

Article (14) : The financial resources of the Center shall consist of the following:

A. The allocations made thereto in the General Budget.

B. Aids, grants, donations and any other resources approved by the Council, provided that those shall be subject to the approval of the Council of Ministers if they are from a non- Jordanian source.

C. Fees and charges of the services provided by the Center.

D. The collected fines that were imposed by the Center.

Article (15) : A. The monies and the rights of the Center with third parties shall be considered public monies and shall be collected in accordance with the Law of the Collection of Public Monies.

B. The Center enjoys exemptions and facilities similar to the Ministries and Government Departments

Article (16) : A. The Center may take one measure or more of those provided below against any person who breaches the provisions of this Law and the bylaws, instructions, and decisions issued pursuant thereto which shall be commensurate with the nature of the breach and the entity that committed such breach:

1. Written warning calling to rectify the breach within the period to be

specified.

2. Rectification of the breach and claiming the expenses incurred by the Center as a result of such the breach.
3. Blocking, shutting down or suspending the telecommunication network, the Information System, the Internet and the telecommunication devices and private electronic messages with any relevant entity for any person suspected to have committed or participated in any act that represents a Cyber Security incident.
4. Compelling the breaching entity to take legal measures against the staff member thereof who is proven to have caused the breach.
5. Cancelling or suspending the license of the person licensed to provide any Cyber Security Services for the period deemed appropriate by the Center.
6. Imposing a fine of no less than (500) Dinars and no more than (100000) dinars, to be doubled in case of repeat the offense.

B. For the purpose of enforcing provisions of Paragraph (A) of this Article, the Council shall issue instructions defining the breach measures, conditions thereof and due actions thereon

Article (17) : A. The Center shall be subject to the Civil Service Regulations, the Financial Regulations, the Supplies and Works Regulations and the Travel and Transportation Regulation in force at Ministries and governmental entities and any other regulations replacing any of the aforementioned, and for this purpose the Chief Officer of the Center shall assume the powers of the Minister, the Competent Minister and the Undersecretary, and the Council shall assume the authorities of the Council of Ministers as provided in such Regulations.

B. Subject to the provisions of the legislations in force, the Chief Officer may request to transfer any of the staff of the Jordanian Armed Forces and the security departments to the Center (subject to the approval of such entities); those so transferred shall enjoy all rights and privileges as offered thereto in their units.

C. The Center may award bonuses or financial incentives to any member of its staff or those transferred thereto pursuant to instructions to be issued by the Council upon the proposal of the Chief Officer of the Center.

Article (18) : The Council of Ministers shall issue the bylaws as needed to execute the provisions of this Law.

Article (19) : The Prime Minister and the Ministers are in charge of executing the provisions of this Law.