# Law No. (15) of 2024

# Concerning the

# Dubai Electronic Security Centre[1]

**We, Mohammed bin Rashid Al Maktoum, Ruler of Dubai,**

After perusal of:

Federal Law by Decree No. (31) of 2021 Issuing the Crime and Punishment Law and its amendments;

Federal Law by Decree No. (34) of 2021 Concerning Combating Rumours and Cybercrimes and its amendments;

Federal Law by Decree No. (38) of 2021 Concerning Copyright and Related Rights;

Federal Law by Decree No. (46) of 2021 Concerning Electronic Transactions and Thiqa Services;

Federal Law by Decree No. (38) of 2022 Issuing the Criminal Procedure Code and its amendments;

Law No. (11) of 2014 Establishing the Dubai Electronic Security Centre;

Law No. (22) of 2015 Regulating Partnership between the Public Sector and the Private Sector in the Emirate of Dubai;

Law No. (1) of 2016 Concerning the Financial Regulations of the Government of Dubai, its Implementing Bylaw, and their amendments;

Law No. (5) of 2021 Concerning the Dubai International Financial Centre;

Law No. (9) of 2022 Regulating the Provision of Digital Services in the Emirate of Dubai;

Law No. (22) of 2023 Concerning the Dubai Digital Authority;

Law No. (26) of 2023 Concerning the Executive Council of the Emirate of Dubai;

Decree No. (22) of 2009 Concerning Special Development Zones in the Emirate of Dubai;

Executive Council Resolution No. (13) of 2012 Concerning Information Security at the Government of Dubai and its amendments;

©2024 The Supreme Legislation Committee in the Emirate of Dubai

[1] *Every effort has been made to produce an accurate and complete English version of this legislation. However, for the purpose of its interpretation and application, reference must be made to the original Arabic text. In case of conflict, the Arabic text will prevail.*

Executive Council Resolution No. (25) of 2020 Concerning the Central Register of Employees of the Government of Dubai and its amendments;

Executive Council Resolution No. (15) of 2022 Concerning the Information and Communications Technology Policies of Government Entities in the Emirate of Dubai; and

The legislation establishing and regulating free zones in the Emirate of Dubai,

**Do hereby issue this Law.**

## Title of the Law
## Article (1)

This Law will be cited as "Law No. (15) of 2024 Concerning the Dubai Electronic Security Centre".

## Definitions
## Article (2)

The following words and expressions, wherever mentioned in this Law, will have the meaning indicated opposite each of them unless the context implies otherwise:

| | |
|---|---|
| Emirate: | The Emirate of Dubai. |
| Ruler: | His Highness the Ruler of Dubai. |
| Government: | The Government of Dubai. |
| Executive Council: | The Executive Council of the Emirate of Dubai. |
| DESC: | The Dubai Electronic Security Centre. |
| Board of Directors: | The board of directors of DESC. |
| CEO: | The chief executive officer of DESC. |
| Government Entity: | Any of the Government departments; public agencies and corporations; Government councils; public authorities, including the authorities supervising Special Development Zones and free zones, such as the Dubai International Financial Centre; or other public entities affiliated to the Government. |
| Non-government Entity: | Any legal person that is not covered by the definition of Government Entity, including, but not limited to, Government Companies, non-government companies, trade associations, commercial establishments, and public-benefit entities, which |

| | |
|---|---|
| | are licensed to operate within the Emirate, Special Development Zones, or free zones, such as the Dubai International Financial Centre. |
| Critical Non-government Entity: | A Non-government Entity classified by the DESC as a critical entity, as per the classification system adopted by the Board of Directors. |
| Electronic Security: | This includes Information Security, Information Systems, and Critical Infrastructure. |
| Information Security: | A set of procedures and measures that must be implemented to protect the Data and Information stored on computers, or exchanged via the internet, or through any other means, or otherwise accessed, used, disclosed, disabled, altered, destroyed, cancelled, or deleted as a result of unauthorised action, misuse, or failure to comply with the security procedures or measures. |
| Information System: | An implement or a set of interrelated or independent implements that are used to store, sort, organise, retrieve, process, develop, and exchange Data, in accordance with the commands and instructions related to such implements. This includes all inputs, outputs, and associated infrastructure used to manage and process Data. |
| Critical Infrastructure: | The physical and virtual assets, critical electronic systems and programmes, and telecommunications network whose failure, compromise, breach, or destruction would have a significant and serious impact on the ability of Government Entities and Critical Non-government Entities to conduct their activities, as well as on the economy and security of the Emirate, including its Electronic Security. |
| Critical Sectors: | The Critical Infrastructure of the Emirate whose Hacking or destruction would cause significant damage to Electronic Security. |
| Data: | A collection of structured or unstructured inputs, facts, concepts, instructions, observations, or measurements, in the form of numbers, alphabets, words, symbols, images, or any other form, that are collected, produced, or processed by |

| | |
|---|---|
| | individuals, entities, or computers, and from which Information is generated through processing or exchange. |
| Cloud Computing: | The internet-connected computing resources and systems through which a range of integrated computing services can be easily and smoothly provided to users. This includes, but is not limited to, Data storage and backup, automatic synchronisation, task scheduling, email, and remote printing. |
| Electronic Security-related Activity: | Any of the activities, fields, services, and roles related to Electronic Security, as approved/ certified by DESC. |
| Hacking: | Unauthorised access, including access that contravenes authorised use of, or unlawful entry into, or unauthorised presence within, an Information System, computer, IT network, or any similar system. |
| Leak: | The deliberate disclosure or divulging of Information or Data classified as sensitive, personal, or confidential, without the knowledge or consent of its owner. |
| Interception: | The viewing, monitoring, accessing, or acquisition of Data or Information for the purpose of eavesdropping, disrupting, storing, Copying, recording, manipulating, altering the content, misusing, re-routing, or redirecting this Data or Information, or for any other unlawful or illegitimate purpose. |

## Scope of Application
## Article (3)

The provisions of this Law apply to the Dubai Electronic Security Centre established pursuant the above-mentioned Law No. (11) of 2014 as a public corporation having legal personality and the legal capacity required to achieve its objectives and perform its functions under this Law, the resolutions issued in pursuance hereof, and other legislation in force in the Emirate.

## Head Office of DESC
## Article (4)

The head office of DESC will be located in the Emirate. Other branches of DESC may be established within the Emirate pursuant to a resolution of the Board of Directors.

## Objectives of DESC
## Article (5)

DESC aims to:

1. establish an efficient and advanced Electronic Security ecosystem in the Emirate;

2. protect the Data, Information Systems, and Critical Infrastructure of Government Entities and Critical Non-government Entities against any potential risks, threats, Hackings, Leaks, or Interceptions;

3. enhance the ability of Government Entities and Non-government Entities to counter the risks and challenges related to Electronic Security; and develop the procedures adopted by them for prevention, impact mitigation, control, and non-recurrence of such risks;

4. enhance the efficiency of the methods used by Government Entities and Non-government Entities for the storage, exchange, and dissemination of Data and Information; and

5. raise awareness of Electronic Security, support and develop national capabilities, and cultivate qualified cadres capable of competing internationally in this field.

## Functions of DESC
## Article (6)

DESC is the competent official entity in the Emirate in charge of all matters related to Electronic Security. For the purpose of achieving its objectives, DESC will have the duties and powers to:

1. formulate, in coordination with the concerned entities, the Electronic Security strategies of the Emirate; submit the same to the Executive Council for approval; and follow up on their implementation;

2. approve and manage, in coordination with the concerned entities in the Emirate, the Electronic Security systems, standards, and guidelines;

3. establish the general framework for determining the Critical Sectors and Critical Infrastructure in the Emirate for the purposes of Electronic Security;

4. develop, in coordination with the concerned entities in the Emirate, the policies, plans, initiatives, programmes, and projects required for protecting Information and addressing potential risks, threats, Hackings, Leaks, Interceptions, and attacks that may compromise Information Systems and Critical Infrastructure; have the same approved by the Board of Directors; and supervise their implementation;

5. develop the Information Security Regulation and oversee compliance by the Government Entities and Critical Non-government Entities with this regulation;

6. develop, in coordination with the concerned entities in the Emirate, the necessary controls for protecting the Critical Infrastructure; have the same approved by the Board of Directors; and oversee their implementation;

7. establish and update the regulations, standards, frameworks, work models, and guidelines related to Electronic Security; and develop the necessary tools for their implementation;

8. develop, in coordination with the concerned entities in the Emirate, the measures required for auditing and assessing compliance with the Electronic Security legislation, policies, regulations, standards, and manuals; and assess compliance by Government Entities and Critical Non-government Entities therewith;

9. propose the legislation and approve the policies, controls, standards, measures, and procedures governing Encryption and decryption; and regulate the import, operation, and use of Encryption and decryption devices;

10. oversee and monitor Information Systems, Critical Infrastructure, Cloud Computing, electronic platforms used for Data processing at Government Entities and Critical Non-government Entities; assess their performance levels; ensure their effectiveness; and verify that they are not subject to any Hacking, Interception, or Leak;

11. supervise the collection, storage, and processing of various Data Sources related to Government Entities and Critical Non-governmental Entities; and connect these sources to the networks of certified Data centres, certified Cloud Computing providers, and authorised systems;

12. issue, in coordination with the concerned entities in the Emirate, the certifications required for conducting the Electronic Security-related Activities, in accordance with the relevant prescribed requirements and procedures; and oversee and supervise those conducting these activities;

13. specify, in coordination with the concerned entities, the devices, equipment, systems, and software whose import and operation within the Emirate requires a prior licence from DESC; and establish the necessary conditions and procedures for the issuance of this licence;

14. combat, in cooperation and coordination with the concerned entities in the Emirate, all types of cybercrimes targeting the entities that are subject to the jurisdiction of DESC or other entities associated with the Critical Infrastructure;

15. qualify national cadres in the field of Electronic Security;

16. raise awareness of the importance of Electronic Security;

17. provide consultations, and conduct training courses and workshops specialised in Electronic Security;

18. conduct research and studies on Electronic Security, and keep abreast of best practices and methodologies pertaining to Electronic Security, with the aim of benefiting from the findings of these research, studies, practices, and methodologies;

19. coordinate with federal, local, regional, and international government entities, in all matters related to Electronic Security;

20. represent the Emirate before local, regional, and international organisations and entities in all matters related to Electronic Security; and participate in the relevant conferences, symposia, projects, and programmes; and

21. exercise any other duties or powers required for the achievement of the objectives of DESC, as assigned by the Ruler or the Chairman of the Executive Council.

**Formation of the Board of Directors**
**Article (7)**

a. DESC will have a Board of Directors comprised of a chairman, a vice chairman, and a number of experienced and specialised members appointed pursuant to a decree of the Ruler.

b. The Board of Directors will convene at the invitation of its chairman, or vice chairman where the chairman is absent. Meetings of the Board of Directors will be valid if attended by the majority of its members, provided that the chairman or vice chairman of the Board of Directors is in attendance.

c. Resolutions and recommendations of the Board of Directors will be passed by majority vote of attending members, and in the event of a tie, the chair of the meeting will have a casting vote. Resolutions and recommendations of the Board of Directors will be recorded in minutes of meetings signed by the chair of the meeting and attending members.

d. A rapporteur will be appointed to the Board of Directors by its chairman. The rapporteur will be responsible for sending meeting invitations to members of the Board of Directors, recording its minutes of meetings, following up on the implementation of its resolutions and recommendations, and performing any other duties assigned to him by the chairman of the Board of Directors.

## Board of Directors Functions
## Article (8)

a. The Board of Directors will undertake general supervision of DESC. For this purpose, the Board of Directors will have the duties and powers to:

1. approve the Electronic Security strategy of the Emirate; submit the same to the Executive Council for final approval; and supervise its implementation;

2. approve the general policy of DESC and supervise its implementation;

3. approve the annual budget and Financial Statements of DESC, and submit the same to the competent entities in the Emirate for final approval;

4. approve the framework for classification of Critical Non-government Entities for the purposes of Electronic Security;

5. approve the standards for determining Critical Sectors and Critical Infrastructure of the Emirate for the purposes of Electronic Security;

6. approve the plans, initiatives, programmes, and projects required for protecting Information;

7. approve Information Security regulations and the controls required for the protection of Critical Infrastructure;

8. approve the resolutions regulating Electronic Security-related Activities, and the requirements and procedures required for issuance of certifications to conduct such activities;

9. approve the resolutions prescribing the requirements and procedures for issuing licences for the devices, equipment, systems, and software whose import or operation requires a prior licence from the DESC;

10. monitor and evaluate the performance of the executive body of DESC, and ensure that it achieves the objectives of DESC and that it performs its functions;

11. approve the organisational structure of DESC, as well as the bylaws regulating the administrative, financial, and technical work of DESC, including the human resources regulations;

12. form permanent and temporary specialised committees and work teams, and determine their duties and powers, to achieve the objectives of DESC; and

13. exercise any other duties or powers related to the achievement of the objectives of DESC, as assigned to it by the Ruler or the Chairman of the Executive Council.

b. The Board of Directors may delegate any of its powers stipulated in sub-paragraphs (a)(4), (a)(5), and (a)(6) of this Article to the CEO, provided that such delegation is specific and in writing.

**Executive Body of DESC**
**Article (9)**

a. The executive body of DESC will be comprised of the CEO and a number of administrative, finance, and technical Employees.

b. The rights and duties of the CEO and Employees of DESC will be determined pursuant to a special regulation to be issued by the Board of Directors. The CEO and Employees will continue to be governed by the human resources legislation applicable to DESC as of the effective date of this Law, until the said regulation is issued.

**CEO of DESC**
**Article (10)**

a. A CEO will be appointed to DESC pursuant to a resolution issued by the Chairman of the Executive Council upon the recommendation of the Board of Directors.

b. The CEO will be directly responsible to the Board of Directors for performing the duties assigned to him under this Law, the resolutions issued in pursuance hereof, and other legislation in force in the Emirate.

**Functions of the CEO**
**Article (11)**

a. The CEO will undertake daily supervision of the work and activities of DESC, and management of its affairs. For this purpose, the CEO will have the duties and powers to:

1. propose the Electronic Security strategy of the Emirate and the policies derived therefrom; and submit the same to the Board of Directors for approval;

2. develop the general policy of DESC; and submit the same to the Board of Directors for approval;

3. prepare the draft annual budget and Financial Statements of DESC; and submit the same to the Board of Directors for approval;

4. develop the framework for the classification of Critical Non-government Entities for the purposes of Electronic Security; and submit the same to the Board of Directors for approval;

5. propose the standards for determining Critical Sectors and Critical Infrastructure in the Emirate for the purposes of Electronic Security; and submit the same to the Board of Directors for approval;

6. propose the plans, initiatives, programmes, and projects required for protecting Information; and submit the same to the Board of Directors for approval;

7. propose an Information Security Regulation and the controls required for the protection of the Critical Infrastructure; and submit the same to the Board of Directors for approval;

8. propose the resolutions regulating Electronic Security-related Activities and the requirements and procedures for the issuance of certifications to conduct such activities; and submit the same to the Board of Directors for approval;

9. propose the resolutions prescribing the requirements and procedures for the issuance of licences for the devices, equipment, systems, and software whose import or operation requires prior licensing from DESC; and submit the same to the Board of Directors for approval;

10. prepare the organisational structure of DESC; draft the bylaws regulating its administrative, financial, and technical work; and submit the same to the Board of Directors for approval;

11. form specialised permanent and temporary committees and work teams; and determine their duties and powers;

12. undertake daily supervision of the work of the executive body of DESC;

13. follow up on the implementation of the plans, policies, programmes, projects, and initiatives assigned to DESC;

14. submit periodic reports on the performance of DESC to the Board of Directors to issue the relevant directives as it deems appropriate;

15. represent DESC before third parties, and conclude contracts and memoranda of understanding with Government Entities and Non-government Entities, within or outside of the Emirate, in areas related to achievement of the objectives of DESC; and

16. exercise any other duties or powers vested in the CEO under the legislation in force, or assigned or delegated to him by the Board of Directors.

b. The CEO may delegate any of his duties and powers under paragraph (a) of this Article to any of the DESC Employees, provided that this delegation is specific and in writing.

## Confidentiality of Information
## Article (12)

All Data relating to the work of DESC which is provided by Government Entities and Non-government Entities is deemed confidential. The Employees of DESC may not grant third parties access to this Data, disclose it, or use it for other than its intended purposes except in the cases prescribed by law or as required by the competent Judicial Authorities.

## Oversight and Measures
## Article (13)

a. DESC will establish the controls required to prevent any attempt to interrupt, disrupt, vandalise, or compromise the Critical Infrastructure or the contents of Information Systems. DESC may take any action to prevent any such acts or attempts whether initiated from within or outside of the Emirate.

b. DESC may take any action required to ensure protection of the Critical Infrastructure and Information Systems of the Emirate against any Hacking, and to identify vulnerabilities in the telecommunications network and Information Systems to avoid any potential risks.

c. In emergency or urgent cases, DESC may monitor, infiltrate, process, cancel, disable, or block the telecommunications network and its devices, as well as the Information Systems and Electronic Messages of any individual or entity found to be contributing to, or engaged in, any act or activity that may compromise the security, economy, heritage, or civilisation, or public order of the Emirate, or its relations with others; or endanger critical facilities, Government Entities, Non-Governmental Entities, lives, or property. DESC must notify the competent Judicial Authorities of any of these measures within one week from the date on which they are taken to enable these authorities to take legal action against the perpetrators of such acts.

d. In emergency or urgent cases, DESC may seek the assistance of experts and consultants, as it deems appropriate, to assist it in responding to any threats and incidents that may compromise Electronic Security.

## Obligations of Government Entities and Critical Non-government Entities
## Article (14)

A Government Entity or a Critical Non-government Entity must:

1. comply with the Electronic Security regulations, standards, and rules issued by DESC; provide DESC with all the Data it requires; and fully cooperate with the competent Employees or authorised representatives of DESC;

2. meet Electronic Security requirements, in accordance with the provisions of this Law and the resolutions issued in pursuance hereof;

3. develop the bylaws, regulations, and plans required for ensuring its Information Security; and take all necessary action to implement the same, in accordance with the nature of its work, provided that these bylaws, regulations, and plans do not contradict the provisions of this Law, the resolutions issued in pursuance hereof, and other legislation in force in the Emirate;

4. notify DESC immediately in the event of facing any threats, Hacks, Leakage, Interceptions, or risks that may compromise the security of the Emirate or its Electronic Security;

5. connect to the security operations centre of DESC or to any other operations centre certified by DESC;

6. assign any of its organisational units, work teams, or Employees to manage the Electronic Security affairs; and ensure that they report to the highest authority therein;

7. not disclose, make accessible, or exchange with a third party any Electronic Security Data without first obtaining the relevant written approval of DESC. This approval will be issued in accordance with the rules prescribed by the Board of Directors in this respect;

8. not engage any private company or establishment specialised in Electronic Security or host the Data of such a company or establishment, unless this company or establishment is certified by DESC in accordance with the relevant standards and rules prescribed by DESC;

9. not engage any person to work as an Information Security officer therewith without first obtaining the relevant authorisation from DESC. This authorisation will be issued in accordance with the standards and rules prescribed by DESC in this respect; and

10. comply with any other obligations prescribed by the relevant resolutions of the Board of Directors.

## Electronic Security Requirements for Non-government Entities
## Article (15)

a. Government Entities overseeing the activities of Non-government Entities, each within its own jurisdiction, must:

1. establish the Electronic Security controls, directives, and measures that Non-government Entities must implement to protect their Data, Information Systems, and technical infrastructure; and have the same approved by DESC;

2. verify compliance by Non-government Entities with the controls, directives, and measures referred to in sub-paragraph (a)(1) of this Article, in accordance with the procedures adopted by the respective Government Entities for oversight and inspection of these Non-government Entities; and

3. perform any other obligations prescribed by the relevant resolutions of the Board of Directors.

b. A Government Entity overseeing the activities of Non-government Entities may outsource any of its functions under this Law and the resolutions issued in pursuance hereof to any public or private entity certified by DESC, pursuant to an agreement concluded with that entity for this purpose. This agreement will determine the rights and obligations of both parties.

**Outsourcing**
**Article (16)**

DESC may, in accordance with the legislation in force, outsource any of its functions under this Law and the resolutions issued in pursuance hereof to any public or private entity pursuant to an agreement concluded with that entity for this purpose. This agreement will state its term and the rights and obligations of both parties.

**Financial Resources of DESC**
**Article (17)**

The financial resources of the DESC will consist of:

1. the financial appropriations allocated to the DESC in the General Budget of the Government;

2. the fees and charges collected in return for the services provided by the DESC; and

3. any other resources approved by the Board of Directors.

**Accounts and Financial Year of DESC**
**Article (18)**

a. In managing its accounts and records, DESC will apply the rules and principles of government accounting.

b. The Financial Year of DESC will commence on 1 January and will end on 31 December of each year.

## Penalties and Administrative Measures
## Article (19)

Without prejudice to any stricter penalty prescribed by any other legislation, any Person who violates the provisions of this Law or the resolutions issued in pursuance hereof will be punished by the penalties and administrative measures prescribed by the relevant resolution issued by the Chairman of the Executive Council.

## Law Enforcement
## Article (20)

DESC Employees or other Persons responsible for enforcing this Law and the resolutions issued in pursuance hereof, nominated pursuant to a resolution of the CEO will have the capacity of law enforcement officers to record the acts committed in breach of the provisions of this Law and the resolutions issued in pursuance hereof. For this purpose, they may issue the relevant violation reports.

## Compliance
## Article (21)

All Government Entities, Non-government Entities, and Persons governed by the provisions of the Law must comply with the provisions hereof within a period not exceeding one (1) year from its effective date. The Board of Directors may extend this grace period once for the same period.

## Issuing Implementing Resolutions
## Article (22)

Except for the resolutions which the Chairman of the Executive Council is exclusively authorised to issue under this Law, the chairman of the Board of Directors will issue the resolutions required for implementing the provisions of this Law, subject to approval of these resolutions by the Board of Directors. These resolutions will be published in the Official Gazette.

## Supersession and Repeals
## Article (23)

a. This Law supersedes the above-mentioned Law No. (11) of 2014.

b. The above-mentioned Executive Council Resolution No. (13) of 2012 is hereby repealed. Any provision in any other legislation is also hereby repealed to the extent that it contradicts the provisions of this Law.

c. The legislation issued in implementation of the above-mentioned Law No. (11) of 2014 and Executive Council Resolution No. (13) of 2012 will remain in force to the extent that it does not contradict the provisions of this Law, until new superseding legislation is issued.

**Publication and Commencement**
**Article (24)**

This Law will be published in the Official Gazette and will come into force on the day on which it is published.

**Mohammed bin Rashid Al Maktoum**

**Ruler of Dubai**

Issued in Dubai on 4 September 2024

Corresponding to 1 Rabi al-Awwal 1446 A.H.