Executive Council Resolution No. (13) of 2012

Concerning

Information Security at the Government of Dubai[1]

We, Hamdan bin Mohammed bin Rashid Al Maktoum, Crown Prince of Dubai, Chairman of the Executive Council,

After perusal of:

Federal Law No. (3) of 1987 Issuing the Penal Code and its amendments;

Federal Law No. (7) of 2002 Concerning Copyright and Related Rights and its amendments;

Federal Law No. (1) of 2006 Concerning Electronic Transactions and e-Commerce;

Federal Law No. (2) of 2006 Concerning Combating Information Technology Crime;

Law No. (2) of 2002 Concerning Electronic Transactions and e-Commerce;

Law No. (3) of 2003 Establishing the Executive Council of the Emirate of Dubai;

Law No. (27) of 2006 Concerning Management of the Government of Dubai Human Resources and its amendments;

Law No. (7) of 2009 Establishing the Dubai eGovernment; and

Law No. (8) of 2010 Concerning the Financial Audit Department and its amendments,

Do hereby issue this Resolution.

Definitions
Article (1)

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

Emirate:	The Emirate of Dubai.
Government:	The Government of Dubai.
Government Entities:	Government departments, agencies, public corporations, councils, and authorities, including free zone authorities, and any other entity

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

	affiliated to the Government.
DeG:	The Dubai eGovernment Department.
Information:	The information, data, documents, and information resources whether printed, written on paper, electronically saved, processed, sent by post or electronic media, appearing in video or audio recordings, or disclosed during face to face conversations or in any other means of communication.
Information Systems:	Any computerised or manual system used by Government Entities for the purpose of information management and processing.
Information Security:	Any procedure or measure taken to protect Information Systems or Information against unauthorised access, use, disclosure, disabling, variation, destruction, cancelling, or deletion.
Information Security Governance:	A branch of corporate governance which comprises strategic orientation, regulatory structure, and the procedures required for the security and confidentiality of vital Information resources.
Information Security System:	The general Information Security framework adopted by the Committee.
Committee:	The Information Security Committee formed pursuant to this Resolution.

Objectives of the Information Security System
Article (2)

The Information Security System will have the objectives to:

1. establish and develop an integrated strategy and a standard policy for Information Security and Information Systems of the Government and protect these against attack and against risks, as Information is of great strategic and vital value for the Emirate;

2. create a safe and reliable environment for storing and maintaining the Information of the Government, and adopt the most effective ways to reduce the risk of Information Security breaches;

3. raise awareness on the importance of Information Security in order to ensure a secure electronic culture and a safe Information community;

4. clearly determine the roles and responsibilities of Government Entities, their employees, and persons dealing with Government Entities in respect of Information Security in such a manner as to avoid any conflict or duplication of such roles and responsibilities;

5. set the procedures that will ensure incidents related to Information Security are responded to in an efficient manner, and determine the practices and instructions that will contribute to minimising the risk of such incidents; and

6. ensure the best performance in order to secure the Information Systems adopted by Government Entities in a manner that assists these entities to perform their duties and achieve their strategic objectives in a secure and efficient manner.

Scope of Application of the Information Security System
Article (3)

a. The Information Security System will apply to:

    1. Government Entities and their employees;

    2. Government Information regardless of the type and the medium in which it is contained; and

    3. persons and entities whose activities require access to the Information Systems of Government Entities.

b. The requirement to implement the Information System will not apply to Government Entities which the Committee decides to exclude, wholly or partially, from implementation if the cost of the implementation of the Information System at these entities exceeds the anticipated risks or the importance of the Information to be protected.

Components of the Information Security System
Article (4)

The Information Security System will be comprised of:

a. Information Security domains that are divided into three (3) major categories which include Information Security Governance, Information operating processes, and Information protection. Each of the three (3) domains has an objective that the Information Security System seeks to achieve. These domains and related objectives will be as follows:

    1. **Information Security Management and Governance**: This domain aims to ensure that the concept of Information Security features in the programmes and strategies of Government Entities.

    2. **Information and Related Asset Management:** This domain aims to prevent unauthorised access to the Information which is classified as confidential, and to protect the Information resources of Government Entities.

3. **Incident and Problem Management:** This domain aims to ensure that Information Security incidents and weaknesses are addressed, and reported for corrective measures to be taken in a timely manner by Government Entities.

4. **Risk Management:** This domain aims to establish and develop a plan to face and address Information Security risks by determining potential threats, weaknesses, and areas for security improvement of Information and Information Systems of the Government.

5. **Access Control:** This domain aims to maintain and protect the confidentiality of Information through controlling access to Information to ensure that it remains accurate, intact, and consistent across Government Entities.

6. **Operations, Systems, and Communication Management:** This domain aims to minimise risk relating to the day-to-day operation of Information Systems, applications, networks, and communication tools whether in use at Government Entities or for the use of the persons dealing with them.

7. **Planning for Business Continuity:** This domain aims to ensure that Information Technology services and infrastructure is able to withstand the risks resulting from errors, incidents, or attacks, to ensure availability of Information and uninterrupted operation at Government Entities.

8. **Owning, Developing, and Managing Information Systems:** This domain aims to integrate Information Security in the Information Systems development and acquisition lifecycle to prevent unauthorised changes to these systems or the misuse of Government Information, and to set the foundation for secure programming.

9. **Protecting the Information Environment:** This domain aims to prevent damage, threats, and misuse of and/or tampering with the Information and Information resources processing facilities at Government Entities.

10. **Human Resources Role and Responsibilities:** This domain aims to determine the roles and responsibilities of employees of Government Entities and the persons dealing with them in respect of Information and Information processing facilities in order to minimise any associated risks or breaches.

11. **Legislative Framework and Audit:** This domain aims to determine the required Information Technology legislation and to raise awareness of the same amongst employees and persons dealing with Information Technology to prevent any breaches or violations of this legislation.

12. **Information Security Assurance and Performance Evaluation:** This domain aims to identify, implement, and develop the Information Security measures that support decision making and improve performance at Government Entities.

b. major and minor controls that ensure achievement of the objectives of the domains outlined in paragraph (a) of this Article; and

c. Information Technology-related technical terms and their clear and precise meanings.

Obligations of the DeG
Article (5)

For purposes of this Resolution, the DeG must:

1. prepare the Information Security System and submit it to the Committee for approval;

2. provide Government Entities with the Information Security System approved by the Committee, and provide the information and instructions required for the application and implementation of this Information Security System;

3. devise an effective strategy that will reinforce partnership, cooperation, and exchange of Information and expertise between Government Entities and the private sector in the area of Information Security;

4. devise a general emergency plan for the Government and Government Entities in order to ensure Information Security, monitor the implementation of this plan, conduct tests to assess the success of the plan to ensure protection of Information and Information Systems against potential risks and threats, and submit the required reports to the Committee;

5. notify Government Entities of any emergencies that may impact Information Security, and provide these Government Entities with the actions and procedures that ensure minimising the relevant potential risks;

6. take the necessary measures to keep abreast of innovative international Information Security solutions, and utilise these solutions to build, update, and develop effective technologies to protect the Information and Information Systems of the Government;

7. devise, design, and implement specialised Information Security training programmes that are up to date with the technical developments in this domain, and lead to the application of best practices required for Information protection and risk control;

8. disseminate the Information Security culture among employees of Government Entities and persons dealing with these entities, and develop the appropriate awareness and education programmes in this regard;

9. provide technical and administrative support to the Committee, and follow up the implementation of the resolutions and recommendations passed by the Committee;

10. coordinate with Government Entities in relation to methods of developing the Information Security System and redressing any flaws that hinder the implementation of the system by these entities; and

11. coordinate with Government Entities with respect to the procedures required for implementation of the general emergency plan at the Government level.

Formation of the Committee
Article (6)

a. Pursuant to this Resolution, a committee named the "Information Security Committee" is formed under the chairmanship of the Director General of the DeG. The Information Security Committee will be comprised of:

    1. a representative from Dubai Police as vice chairman;

    2. a representative from the General Department of State Security;

    3. a representative from the General Secretariat of the Executive Council;

    4. three (3) representatives from Government Entities and private entities determined by the Director General of the DeG; and

    5. two (2) representatives from the DeG, one of whom will be the rapporteur of the Committee.

b. The representatives from the entities referred to in paragraph (a) of this Article will be nominated by those in charge of these entities, provided that the nominated representatives have experience in the area of Information Security.

Committee Meetings
Article (7)

a. The Committee will convene at the invitation of its chairman, or vice chairman if the chairman is absent, at least once every three (3) months or when necessary. Committee meetings will be valid if attended by the majority of its members provided that the chairman or vice chairman of the Committee is in attendance.

b. The Committee will pass its recommendations and resolutions unanimously or by majority vote of attending members. In the event of a tie, the chair of the meeting will have the casting vote.

c. The Committee may seek assistance from the experts and specialists it deems appropriate, provided that they will not have a vote during the deliberations of the Committee.

d. Meetings and resolutions of the Committee will be recorded in minutes of meeting to be signed by the chair of the meeting and all attending members.

Functions of the Committee
Article (8)

The Committee will:

1. study the Information Security System prepared by the DeG and approve it no later than three (3) months from the date of its referral to it by the DeG;

2. follow up implementation of the Information Security System at Government Entities and their compliance with the application of this system, and submit the required reports in this regard to the Chairman of the Executive Council of the Emirate of Dubai;

3. conduct periodic reviews of the Information Security System and assess its performance and efficiency in protecting Government Information and Information Systems, determine the areas of development and improvement that can be introduced to the Information Security System and the system flaws and weaknesses, and issue the resolutions and recommendations required in this regard;

4. study the reports sent to the Committee by Government Entities on the outcome of the risk assessment related to Information Security at these entities and issue the appropriate resolutions in this regard;

5. ensure that Information Security emergency plans are in place at Government Entities, conduct periodic assessment of these plans, and issue the resolutions and recommendations required in this regard;

6. propose the legislation, policies, plans, and programmes required to ensure further protection of Government Information and Information Systems; and

7. propose the measures required for promoting coordination and cooperation among Government Entities in the area of Information Security, and consolidate the efforts of these entities to protect their Information Technology infrastructure.

Obligations of Government Entities
Article (9)

A Government Entity must:

1. within a maximum of six (6) months from the date of receiving the Information Security System, provide the Committee with a compliance document which includes the domains that are applicable to the Government Entity and a schedule indicating the plans, methods, and stages for applying these domains;

2. develop the technical programmes and systems, policies, and procedures governing the operations of the Government Entity in a manner that ensures implementation of the Information Security System in conformity with the type, nature, importance, sensitivity, and confidentiality of the Information maintained by the Government Entity;

3. familiarise the employees of the Government Entity and persons dealing with it with the Information Security System and train them on implementing it and all its domains, objectives, and controls, and monitor their compliance level with the same;

4. take the security and safety measures required to protect the Information maintained by the Government Entity, including prevention of unauthorised access to, or variation or modification of, Information, and protect such Information against any loss, leakage, damage, destruction, or any other damage;

5. devise an internal emergency plan that conforms to the general emergency plan adopted by the DeG with the aim to maintain Information Security and security of the Information Systems of the Government Entity, and conduct drills to assess this plan to ensure protection of the Information and Information Systems against potential risks and threats;

6. respond quickly, effectively, and orderly to any incidents that may cause damage to the Information and Information Systems of the Government Entity, to conduct the required investigation of these incidents, and to notify competent entities and the Committee of the same;

7. provide basic awareness of Information Security to the Government Entity employees whose job duties are related to Information Technology, and ensure that they are aware of their responsibilities in relation to the protection of Information Security, and of potential Information threats, risks, and breaches;

8. conduct periodic reviews of the domains and controls of the Information Security System adopted by the Government Entity based on assessment of current and potential risks, in order to verify the relevance and upgradability of these domains and controls to the duties and functions of the Government Entity, and submit the recommendations required in this regard to the Committee; and

9. provide the Committee with periodic reports on the outcome of Information Security risk assessment at the Government Entity and the action taken by the Government Entity with respect to implementation of the Information Security System.

Obligations of the Financial Audit Department
Article (10)

The Financial Audit Department must monitor the application of the Information Security System by Government Entities, prepare the reports required in this regard, and provide the Committee with copies of these reports.

Obligations of Employees of Government Entities
Article (11)

Employees of Government Entities must:

1. implement the Information Security System to ensure protection of the Information and Information Systems of the Government Entity in which they work;

2. not disclose any Information which is confidential by nature or pursuant to relevant instructions, without obtaining a prior written permission from the competent officer at the Government Entity in which they work;

3. maintain Information Security and not take any action that may cause change, modification, destruction, damage, deletion, cancellation, or loss of Information, unless this action is taken by an authorised competent officer;

4. notify their immediate supervisors and the competent entities of any threat, penetration, breach, or incident that may cause disclosure, change, modification, destruction, damage, deletion, cancellation or loss of the Information of the Government Entity in which they work;

5. not use or exploit Information for purposes other than the specified or intended uses; and

6. not allow unauthorised persons to access the Information Systems adopted by the Government Entities in which they work.

Measures and Procedures
Article (12)

Without prejudice to any applicable civil or criminal liability he may incur, an employee of a Government Entity who violates the security and safety measures adopted by the Government Entity in relation to Information Security in a manner that causes change, modification, destruction, damage, deletion, cancellation, or loss of Information will be subject to disciplinary action.

Obligations of Persons Dealing with Government Entities
Article (13)

Subject to the liability stipulated in the legislation in force, persons and entities conducting activities which, by their nature, require access to the Information Systems adopted by Government Entities must:

1. abide by the instructions issued by Government Entities in relation to Information Security;

2. not perform any act that may cause change, modification, destruction, damage, deletion, cancellation, or loss of the Government Information;

3. not perform any act that may cause failure of the Government Information Systems in a manner that renders them not fit for their purposes or unable to perform their functions;

4. not use or exploit any Government Information for other than the intended purposes;

5. not copy or publish any Government Information without obtaining prior written approval of the concerned Government Entity; and

6. not allow unauthorised persons to access the Information Systems adopted by the Government Entities they deal with.

Ownership of the Information Security System
Article (14)

The Information Security System and all its components, including data, Information, and software, are property of the Government. The Government will be exclusively authorised to dispose of the Information Security System by any means.

Modification of the Information Security System
Article (15)

Upon the recommendation of the Committee, the Director General of the DeG may modify any of the domains and objectives of the Information Security System and the controls for achieving these objectives in order for the system to fulfil its purposes, and notify the Government Entities which implement the system of this modification upon its approval by the Committee.

Time Limit for Preparation of the Information Security System
Article (16)

No later than three (3) months from the date on which this Resolution comes into force, the DeG must prepare the Information Security System, present it to the Committee for approval, and send it after approval to Government Entities for implementation and adoption.

Implementing Bylaws
Article (17)

The Director General of the DeG will issue the bylaws and instructions required for the implementation of the provisions of this Resolution.

Repeals
Article (18)

Any provision in any other resolution will be repealed to the extent that it contradicts the provisions of this Resolution.

Publication and Commencement
Article (19)

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

Hamdan bin Mohammed bin Rashid Al Maktoum

Crown Prince of Dubai

Chairman of the Executive Council

Issued in Dubai on 11 April 2012

Corresponding to 19 Jumada al-Ula 1433 A.H.