GOVERNMENT OF DUBAI

Department of Finance

Information Security High Level Policy

Information Security Policy

DOF-IS-POL-1

Version 1.1

Owner: ISSC

Date of issues: 2018

Classification: Confidential

Document Control

Document History

Date	Version	Author(s)	Description
07.03.2018	0.1	Protiviti	Initial Draft
02.05.2018	1.0	DOF	Reviewed & Approved
12.09.2019	1.0	DOF	Reviewed & No Changes
02.08.2020	1.1	DOF	Reviewed & Approved

Table of Contents

1. Information Security High Level Policy

1.1 Objective

The objective of this policy is to protect the information assets of DOF from all threats, whether internal or external, deliberate or accidental thereby ensuring uninterrupted services to Employees and Stakeholders and manage the risk to the acceptable level through design, implementation and maintenance of an effective Information Security Management system.

1.2 Policy Statement

DOF is committed towards securing the Confidentiality, Integrity and Availability of information for the business operations. The security of information is therefore regarded as vital for the successful business operation of DOF.

The principles that need to be followed for the effective implementation and management of this policy are explained in this section.

1.3 Policy

1.3.1 Information Security High Level Policy

1. All information assets shall be used in a manner that supports the strategic goals and objectives of DOF.
2. All applicable legal and/or regulatory requirements pertaining to information security shall be addressed.

3. All information & information processing systems shall be identified, valued and classified to ensure adequate protection.
4. Develop and Maintain Information Security Risk Management methodology to assess Information Security risks.
5. Provide appropriate Information Security Training & awareness to all employees (permanent & contract employees).
6. Employees and vendors or third party contractors shall adhere to the information security policies, procedures, standards, guidelines etc. approved by the management of DOF.
7. Information shall be handled in a secured manner to avoid any loss of confidentiality, integrity, and availability during its creation, storage, processing, transmission and disposal.
8. Information and information processing systems shall be accessible to the authorized users as per their business needs.
9. Information and information processing systems shall be physically secured from any loss of confidentiality, integrity & availability.
10. All changes related to information and information processing systems shall be managed in a secured manner.
11. All information security incidents shall be reported and managed in a timely manner with proper escalation matrix defined for treating high severity incidents.

12. IT Business Continuity plans shall be defined implemented and tested adequately to ensure availability of information and information processing systems during any emergency.
13. The posture of information security shall be continuously reviewed and improved to ensure continuous adherence to this policy.
14. Employees and non-employees of DOF shall not attempt to bypass any of the information security controls.
15. Ensure compliance to applicable standard and regulations on information security e.g. ISO 27001:2013 and Dubai ISR.

2. Policy Update

This policy shall be reviewed yearly or whenever there is a need, the updates will be in line with changes that may occur in the internal or local or federal lows, or to accommodate new concepts related to the management and archiving of paper or electronic, or to take advantage of best practices on measuring its effectiveness of the procedure.

Future update shall also include the necessary adjustments to reflect performance measurement indicators, and results of the internal and external evaluation.

3. Key Performance Indicators

Measurement will be as per DESC Standards and requirements

***** End of the Document*****