السياسة العامة لأمن المعلومات بدائرة المالية

DOF Information Security High Level Policy

Policy 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.

الهدف من السياسة

تهدف هذه السياسة إلى حماية الموارد المعلوماتية للدائرة من كافة التهديدات، سواء الداخلية أو الخارجية، المتعمدة أو غير المتعمدة، وبالتالي ضمان عدم انقطاع الخدمات عن الموظفين والمعنيين والمتعاملين مع الدائرة، كما تهدف لإدارة المخاطر وضمان استقرارها ضمن الحدود المقبولة من خلال تصميم وتنفيذ وصيانة نظام فعال لإدارة أمن المعلومات على مستوى الدائرة.

Policy Statement

DOF is committed towards securing the Confidentiality, Integrity and Availability of information for the business operations, as the security of information is vital for the success of business operations of DOF.

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

DOF Information Security Policy clauses:

- All information assets shall be used in a manner that supports the strategic goals and objectives of DOF.
- All applicable legal and/or regulatory requirements pertaining to information security shall be addressed.
- All information & information processing systems shall be identified, valued and classified to ensure adequate protection.
- Develop and Maintain Information Security Risk Management methodology to assess Information Security risks.
- Provide appropriate Information Security Training & awareness to all employees (permanent & contract employees).
- Employees and vendors or third-party contractors shall adhere to the information security policies, procedures, standards, guidelines etc. approved by the management of DOF.
- 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.
- Information and information processing systems shall be accessible to the authorized users as per their business needs.
- Information and information processing systems shall be physically secured from any loss of confidentiality, integrity & availability.
- All changes related to information and information processing systems shall be managed in a secured manner.

بيان السياسة

تلتزم دائرة المالية بضمان سرية وسلامة وتوافر معلومات أنشطة وعمليات الدائرة حيث يعتبر أمن المعلومات عاملاً أساسياً لنجاح أعمال الدائرة.

وفيما يلي النقاط التي يجب اتباعها من أجل ضمان فعالية تطبيق وإدارة هذه السياسة:

بنود السياسة العامة لأمن المعلومات

- استخدام كافة أصول المعلومات لدعم تحقيق الأهداف والتوجهات الاستراتيجية لدائرة المالية.
- مراعاة كافة المتطلبات القانونية و/أو التنظيمية المتعلقة بأمن المعلومات.
- تحديد وتقييم وتصنيف كافة المعلومات وأنظمة معالجة المعلومات المعمول بها في الدائرة لضمان توفير الحماية المناسبة.
- تقييم مخاطر أمن المعلومات من خلال إعداد وتطوير منهجية لإدارة المخاطر على مستوى الدائرة
- تقديم التدريب والتوعية اللازمة لكافة موظفي الدائرة (الموظفين الدائمين أو موظفي عقود التعهيد الخارجي) فيما يتعلق بأمن المعلومات.
- ضمان التزام كافة الموظفين والموردين ومقاولي الطرف الثالث بالسياسات والمبادئ والمعايير والإرشادات المعتمدة لأمن المعلومات في دائرة المالية.
- استخدام وإدارة المعلومات بصورة آمنة لضمان عدم فقدان أي من عوامل سرية أو سلامة أو توافر المعلومات أثناء إنشائها، أو تخزينها، أو إرسالها، أو التخلص منها.
- ضمان منح صلاحيات الوصول إلى المعلومات وأنظمة معالجة المعلومات للمستخدمين المخولين وبحسب احتياجات أعمالهم.
- ضمان تأمين وحماية المعلومات وأنظمة معالجة المعلومات تجاه كل ما قد يعرضها لفقدان عوامل سريتها أو سلامتها أو توافرها.
- إدارة كافة التغييرات المتعلقة بالمعلومات وأنظمة معالجة المعلومات بصورة آمنة.

السياسة العامة لأمن المعلومات بدائرة المالية

DOF Information Security High Level Policy

- ضـــمان الإبلاغ عن كافة الحوادث المتعلقة بأمن المعلومات وإدارتها في الوقت المناســب تبعاً لمصــفوفة التصــعيد المعتمدة والمتبعة لمعالجة الحوادث شديدة الخطورة في الدائرة.
- ضـــرورة تحديد خطط إدارة اســـتمرار الأعمال لتقنية المعلومات وتنفيذها واختبـارها بشـــكـل ملائم لضـــمـان توافر المعلومـات وأنظمـة معـالجـة المعلومات خلال أي طارئ.
- المراجعة والتحســـين المســـتمر لممارســـات أمن المعلومات لضـــمان استمرارية الالتزام بهذه السياسة.
- يمنع على الموظفين أو غير العاملين لدى دائرة المالية محاولة تجاوز أي ضابط من ضوابط أمن المعلومات.
- ضـمان الامتثال للمعايير والممارسـات العالمية المتعلقة بأمن المعلومات، على ســـبيـل المثـال: المعيـار الـدولي لإدارة أمن المعلومـات ISO 27001:2013 ولوائح أمن المعلومات لحكومة دبي ISR.

- information security incidents shall be reported and managed in timely manner with proper escalation matrix defined for treating high severity incidents.
- IT Business Continuity plans shall be defined implemented and tested adequately to ensure availability of information and information processing systems during any emergency.
- The posture of information security shall be continuously reviewed and improved to ensure continuous adherence to this policy.
- Employees and non-employees of DOF shall not attempt to bypass any of the information security controls.
- Ensure compliance to applicable standard and regulations on information security e.g. ISO 27001:2013 and Dubai ISR.

عبدالرحمن صالح آل صالح – المدير العام

Abdulrahman Saleh Al Saleh – Director General