Executive Support Letter

Information security within DLS

As a government department that seeks excellence and leadership in providing real estate services and protecting real estate property, DLS recognizes at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, and other stakeholders.

In order to provide such a level of continuous operation, DLS has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001.

The operation of this ISMS has many benefits for the business, including:

- Maintain customer service levels and customer confidence.
- Protect sensitive data and assets.
- Improve risk management by reducing the impact of internal and external threats.
- Enhance operational effectiveness for processes by sustaining DLS activities and services.
- Continually improve the department's information security and reduce their costs.
- Compliance with legal and regulatory requirements.

An Information Security Policy is available in both paper and electronic form and will be communicated within the organization and to all relevant stakeholders and interested third parties.

Commitment to the delivery of information security extends to senior levels of the organization and will be demonstrated through the information security policy and the provision of appropriate resources to establish and develop the ISMS.

Top management will also ensure that a systematic review of performance of the program is conducted on a regular basis to ensure that information security objectives are being met and relevant issues are identified through the audit program and management processes.

A risk management approach and process will be used which is line with the requirements and recommendations of ISO/IEC 27001. Risk management will take place at several levels within the ISMS, including:

- Assessment of risks to the achievement of our information security objectives
- Regular information security risk assessments within specific operational areas
- Assessment of risk as part of the business change management process
- At the project level as part of the management of significant change

We would encourage all employees and other stakeholders in our business to ensure that they play their part in delivering our information security objectives.

Yours sincerely,
Dr.Ahmad Al-Omoosh
12 Sep 2024