LUX ISLAND RESORTS LTD (LIR) – IT SECURITY POLICY

Introduction

Information is a critical asset of the Company and must be protected from unauthorized exposure, deletion, and modification, whether deliberate or accidental. In view of their importance, information systems must be effectively protected. Reliable protection allows LIR to better see to its interests and efficiently carry out its information security mandate. Inadequate protection affects a business' overall performance, and can negatively impact image, reputation and investor confidence.

This document relates to the physical and logical security of all the components implemented on LIR systems, with the aim of achieving a necessary and sufficient level of security for all types of information. It includes hardware, software, human and logistical aspects.

Everyone associated with the Company has a role in information security. The Company's success depends upon its ability to offer products and services with a high level of customer satisfaction. LIR is the trusted custodian of data provided to us by our customers, candidates, and employees; therefore, LIR must ensure that due care is exercised in the protection of this data.

This information security policy identifies the guiding principles that all employees must adhere to in order to ensure the confidentiality, integrity, and availability of LIR.

Executive Summary

a. The selection of passwords, their use and management as a primary means to control access to systems must strictly adhere to the password policy guidelines.
b. Access control standards for information systems must strictly follow the guidelines as per Access Control section of the policy.
c. All LIR properties should as far as possible be protected from unauthorised access and equipped with access control systems to control physical access.
d. System Hardware, Operating Systems and Applications Software, Networks and Communication Systems must all be adequately configured and safeguarded against both physical attack and unauthorised network intrusion.
e. Information System administrators must ensure that adequate backup and system recovery procedures are in place and tested on a regular basis.
f. System testing procedures will incorporate a period of parallel running prior to the new or amended system being acceptable for use in the live environment. Results of parallel running should not reveal problems of difficulties which were not previously passed during user acceptance testing.
g. Business Continuity Plans (BCP) must be prepared, maintained and regularly tested to ensure that damage or disruption caused by internal and external threats or attacks can be minimised and restoration takes place as quickly as possible.

h. A formal Risk Assessment should be undertaken in order to determine the requirements of a Business Continuity Plan that covers all essential and critical business functions and tested at regular intervals.
i. Human Resources must ensure that all employees are fully aware of their legal responsibilities with respect to their use of computer base information systems and data and fully complies with the data protection Act and that such responsibilities are to be included within key staff documentation such as Staff Manual.
j. All information, data and documents must be clearly labelled so that users are aware of the ownership and classification of information with respect to their level of confidentiality, integrity, sensitivity, value and criticality.

Objective

The objectives of the IT Security Policy are as follows:

a. To establish responsibility and accountability for Information Security in the organisation.
b. To safeguard the organisation's information resources from theft, abuse, misuse and any form of damage/tampering.
c. To protect the organisation's business information and any guest information within its custody by safeguarding its confidentiality, integrity and availability.
d. To encourage Management and staff to maintain an appropriate level of awareness, knowledge and skills to allow them to minimise and prevent Information Security incidents.
e. To guarantee business continuity and minimal disruption in the company activities in the event of major Information Security breach/incidents.

Scope

The main requirement of this policy is the development of a secure information system environment which is in line with LIR objectives for information security.
The information security policy ensures that:

- Information will be protected against any **unauthorized access**;
- **Confidentiality** of information will be assured;
- **Integrity** of information will be maintained;
- **Availability** of information for business processes will be maintained;
- **Legislative and regulatory** requirements will met;
- **Business continuity plans** will be developed, maintained and tested;
- **Information security training** will be available for all employees;

Audience

The Audience of this policy includes all users. Users are defined as anyone with authorized access to the LIR technology resources, including permanent and temporary employees or third party personnel such as temporaries, contractors, consultants, and other parties with valid LIR access accounts and are responsible for participating in the security of the IT environment.

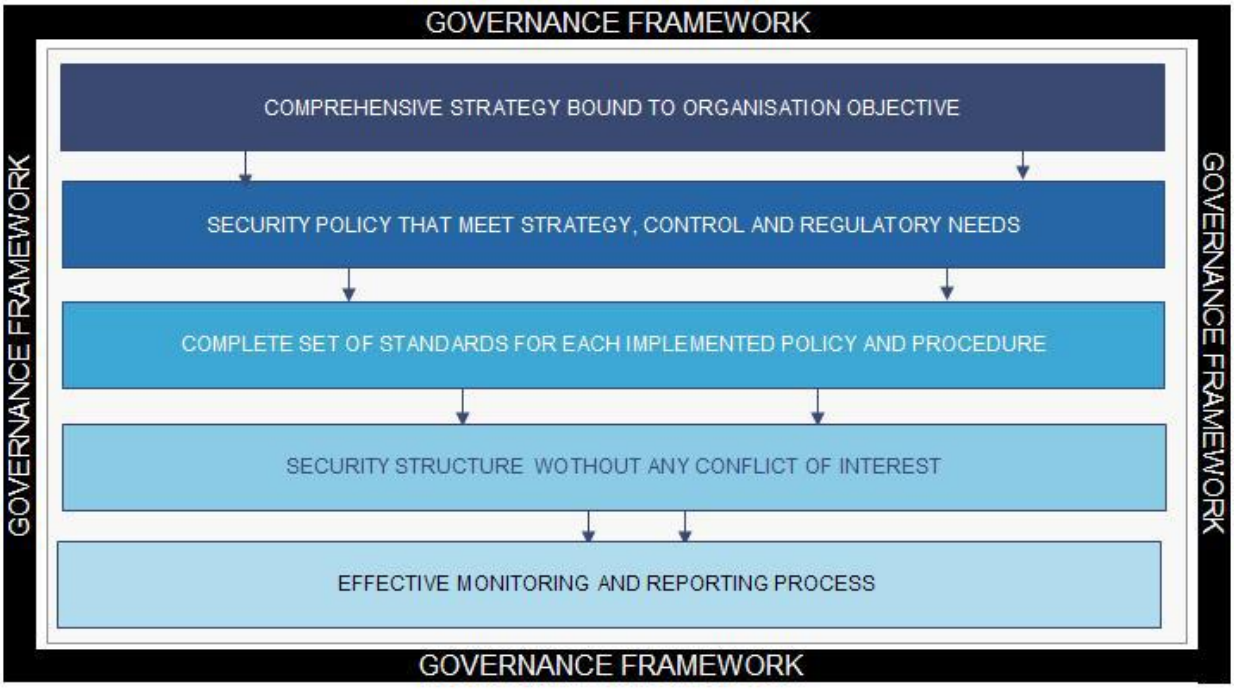

Fig 1 – IT Security Governance Framework