Information Security Policy

EO-ISMS-PL-IS-001

Version 1.2

Public

March 7th, 2019

TABLE OF CONTENTS

1. INFORMATION SECURITY POLICY

1.1 INTRODUCTION

This policy provides primary governance for Information security (IS) management at E-OCEAN (PVT) limited. We are committed to maintain and improve the confidentiality, integrity and availability of all information assets of the organization to ensure that regulatory, operational and contractual requirements are fulfilled. To this end, we have established an information security management system that presents framework to identify the information we need to protect and how we must protect it with major intent of continual improvement in compliance with international best practices required for the defined scope of organization.

1.2 SCOPE

This policy covers establishment and continual improvement of a complete Information Security Management System, including related documentation, implementation and regular monitoring, both through planned audits and through reporting of any security incidents. Adherence to the policy is mandatory for all permanent and contractual employees, consultants and other workers at E-ocean, including all personnel affiliated with third parties and those who is/are granted the access to organization's information assets.

1.3 POLICY DESCRIPTION

E-ocean aims that:

i. IS objectives must be defined, planned, facilitated, monitored and tracked for completion.
ii. A comprehensive information security management system shall be developed, implemented and maintained to initiate & control the implementation of information security within the organization.
iii. All information assets of organization shall be classified to indicate required degree of protection.
iv. Risks to all corporate assets (tangible/intangible) are assessed and against all risks appropriate treatment is done.
v. Physical, logical and remote accesses to the information and associated information processing facilities shall be controlled.
vi. Business information and information processing facilities shall be protected from physical security threats and environmental hazards. Business information and information processing facilities supporting critical or sensitive business activities shall be housed in secure areas with appropriate entry controls
vii. Security shall be applied on operating system to restrict unauthorized access to computer resources.
viii. All information system and the security control systems shall be monitored to detect deviation from access control policy.
ix. All security requirements related to Human Resource shall be fulfilled.
x. All resources in terms of technical, tactical and human capital resources in order to defined, implement, monitor and improve the information security management system shall be provided adequately.
xi. Awareness of information security requirements, policies and procedures must be given to all staff.
xii. Mechanism shall be in place to facilitate the prompt reporting of Information security incidents.
xiii. Controls shall be established to prevent and detect viruses and other malicious software.

xiv. Routine procedures shall be established for taking back-up copies of information and system software, logging events and faults and, where appropriate, monitoring the equipment installed for this purpose (e.g. camera recording and its audit logs, etc.).
xv. Information within networks and passing over public networks shall be secured and protected adequately.
xvi. Changes to information assets and information processes facilities must be controlled through structured mechanism.
xvii. Mechanism shall be established for the handling, storage and disposal of paper and removable media.
xviii. Controls shall be established to protect exchanges of information and software.
xix. Controls shall be established to mitigate the security risks associated with mobile computing and wireless networks.
xx. Security requirements shall be identified and agreed prior to the processing of information system activities.
xxi. Current capacity shall be monitored, future capacity projections shall be made and operational requirements of new systems shall be established, documented and tested prior to their acceptance and implementation.
xxii. Redundancies to the information system and Information processing facilities shall be defined, implemented and monitored for appropriateness in order to protect critical business processes from the effects of major failure or disasters.
xxiii. Information security continuity shall be planned to avoid information security breaches in case of adverse operational situations.
xxiv. Information systems shall be audited for compliance.
xxv. The complete management system must be review by the management or designated persons on defined frequency for effective measurement and continual improvement of the system.
xxvi. To ensure the protection of its information assets from all threat, internal or external, deliberate or accidental and natural disasters, E-ocean ensures the full compliance with the local government laws and the contractual obligations.
xxvii. Secure software development principles must be adopted.

1.4 POLICY COMMUNICATION

Internal: This policy must be available to all employees through the company's intranet.
External: To all external parties, the uncontrolled copy of will be provided in hard copy format or on email, if and when requested/required.
Vendors/ Contractors: priori to start the activity, the policy will be handed over to all those contractors/vendors who will be given physical / logical access to E-ocean's premises, information assets, information system and/or information processing facilities.

1.5 REVIEW

This policy has been approved by the company management and shall be reviewed annually for its continuing suitability, adequacy, and effectiveness.