ISMS Policy

ISMS Implementation according to ISO/IEC 27001:2013

For

IT Security C&T

CLASSIFICATION: *Public*

DOCUMENT VERSION CONTROL

Item	Description
Client Name:	IT Security C&T
Project Name:	ISMS Implementation according to ISO/IEC 27001:2013
Document Name:	ISMS Policy
Document Issue No:	V1.0
Status:	Approved
Authors:	IT Security C&T Consultant Team
Approved by:	IT Security C&T
Data Classification:	*Public*
Date:	06/03/2018

Revision History

Revision Date	List of Changes	Author	Approval
07/03/2018	First draft	IT Security C&T	IT Security C&T

1. Scope

- ✓ The policy applies to all information created or received in IT Security C&T.
- ✓ This policy forms the basis of IT Security C&T Information Security Management System (ISMS) of related policies and procedures.

2. Purpose

It is the policy of IT Security C&T to ensure that appropriate controls and countermeasures are put in place to protect corporate and client's data, as well as the information technology systems, services and equipment of IT Security C&T. The purpose of the policy is to protect IT Security C&T's information assets from all threats, whether internal or external, deliberate or accidental.

3. Policy Statement

To ensure that all of the IT Security C&T information assets, people, intellectual property, computer systems, data and equipment are adequately protected from all threats, whether internal or external, deliberate or accidental on a cost-effective basis.

- ✓ IT Security C&T is protecting information assets from unauthorized access.
- ✓ IT Security C&T commits to comply with regulatory and legislative requirements.
- ✓ IT Security C&T commits to maintain a high level of competence for its staff.
- ✓ Information security risks shall be managed based on IT Security C&T Risk Management Methodology.
- ✓ IT Security C&T commits to continually improve its ISMS and information security
- ✓ IT Security C&T will control and restrict access to information assets based on need-to-know and least privilege principles.
- ✓ IT Security C&T will continually improve Information Security Posture by measuring the performance of the ISMS and suggest the needed actions to ensure effectiveness.
- ✓ Treat and resolve security incidents and suspected vulnerabilities per their respective nature.

4. Responsibilities

- ✓ All managers are directly responsible for implementing the ISMS Policy, and monitor the adherence of their staff.
- ✓ Compliance with this Policy and all other supporting policies, standards, and procedures is mandatory for all staff and third-parties. Violation of this policy or any other IS policies, standards, or procedures will result in corrective action by management. Disciplinary action will be consistent with the severity of the violation, as determined by an investigation, and as deemed appropriate by management.

Signature: