Company Name

ICT Management and Security Policy

Month – 2022

Table of Contents

Document Control

Type of Information	Document Data
Title	ASSIGNED Policy
Version	<Document Number>
Issue Date	<Year>
Document Owner	<COMPANY>
Document Creator	<Name>

Revision History

Version	Date	Author	Summary of Changes
1.0	1 Mar 2022	<Name>, <Designation>	First document

Document Approver

Version	Approval Date	Approving Authority	Signature
1.0	1 April 2022	<Designation>	

ICT Management and Security Policy

Purpose

This Information and Communications Technology Management & Security Policy provides the governance framework for the management and security of **COMPANY** Information Technology and Communications Systems ("**ICT Systems**").

The company relies on the integrity and availability of its ICT System and infrastructure to meet its needs and ensure effective communication, security and working practices. Improper use of the Company's ICT Systems can adversely impact the business, waste time resources, create legal liability, and impose a security risk and embarrassment for both the company and the user.

The company's ICT System must include but is not limited to software, hardware, telephone, server, and computer systems.

The company must protect its ICT Systems from illegal, defamatory, fraudulent, or other misuses. This policy contains guidance on the measures that Company staff members must take, Legal Entity Customers (Business Customers), workers, contractors, and any other users ("**Users**") to ensure that the Company's ICT systems are secured, and proper standards are met.

The company reserves the right to amend this policy at any time without notice.

Responsibility

The company is responsible in maintaining this policy and keeping it under review.

Users must be responsible for complying with the terms of this policy and be responsible for familiarising themselves with this policy, as is appropriate. Any queries regarding this policy or how it might improve it must be directed to <Email>.