<< Organisation Logo>>

<< Information Security Policy >>

Version: 1.0
Date

Revision History

Date	Version	Author	Summary of Changes

Approvals

Name	Signature	Title	Issue Date	Version

Contents

Contents

INTRODUCTION

DOCUMENT PURPOSE

The Information Security Policy is the apex policy for [organisation] Information Security strategy. It details out the statements for maintaining and improving the [organisation] information security plans and defines how Information Security will be set up, managed, measured and reported

The objective of information security policy is to reduce the risk to [organisation] by protecting information, information systems and communications that deliver information, from failures of integrity, confidentiality and availability, whether information is in storage, processing, or transmission. Information Security is seen as an enabler to achieve [organisation] business strategy and objectives.

SCOPE

This policy encompasses all [organisation] employees, consultants, contractors, and vendors conducting business with [organisation]. The policy applies to all information in physical and electronic format (including cloud if applicable) held by or entrusted to [organisation] throughout the information lifecycle, which includes creation, transfer, collection, storage, distribution, archiving and disposal.

POLICY

Below statements shall be complied with: -

Policy Statements

No:	Statements
	All [organisation] personnel who have access to the information are expected to comply with acceptable use policy in the use of information created , stored, transmitted, or disposed of in the course of their job duties, regardless of the medium in which that information is maintained.
	[organisation] personnel are prohibited from attempting to circumvent or subvert any [organisation] information security control. No authorized user may install, remove, or

	otherwise modify any information security controls for the purpose of bypassing, avoiding, or defeating any filtering, monitoring, or other security controls [organisation] may have put in place. All functionalities allowed/configured on the infrastructure shall be justified to the business and approved appropriately.
	All changes to the infrastructure shall be requested, approved and shall be traceable.
	All staff shall be kept abreast of this policy.
	All new [organisation] Staff shall undergo an information security training as part of the induction program upon resumption. Information security awareness will be propagated using various methods such as screensavers, newsletters, memos, etc at regular intervals at the discretion of the information security unit.
	A program shall be in place to monitor all service providers on information security related matters.
	A program shall be in place to monitor all relevant compliance status at least annually if applicable.
	All logs and alerts are to be monitored and reviewed at intervals and all systems components and configurations shall be secured against unauthorised modification and monitored accordingly and backed up.
	This policy will be reviewed annually and at when there is a significant change(s) to ensure continuing suitability, adequacy and effectiveness.
	All staff shall attest to having read and understood this policy.
	All staff access control accounts must undergo risk assessment approval before staff usage
	Access to [organisation] laptops, application and servers must be via access control.
	Deleted, or disabled, any accounts for staff who are no longer with your [organisation]
	Staff should have exact privileges for their job role, and this must be monitored as they change job responsibilities.