<< Organisation Logo>>

<< Information System Risk Management 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

Every [organization] has a mission. In this digital era, as [organizations] use automated information technology (IT) systems to process their information for better support of their missions, risk management plays a critical role in protecting an [organization]'s information assets, and therefore its mission, from IT-related risk.

Risk management relates to the culture, processes and structures directed towards the effective management of potential risks and adverse effects within [organization] environment. The purpose of this policy is to explain the [organization]'s underlying approach to risk and risk management.

SCOPE

This policy applies to [organisation] critical services, critical business locations, infrastructure; all employees, including temporary staff, contractors, service providers, consultants and third parties.

DEFINITIONS

Risk: The threat or possibility that an action or event will adversely or beneficially affect [organization] ability to achieve its goals. Risk is measured in terms of likelihood and impact.

Risk Assessment: The overall process of risk identification and evaluation.

Risk Management: The culture, processes and structures that are directed towards the effective management of potential risks and possible adverse effects within an environment.

Internal Controls: Systematic measures such as policies, procedures, processes, reviews, checks and balances instituted by an organization to conduct its business in an efficient manner, safeguard its assets and resources, and deter and detect errors, fraud and theft.

Risk Management Process: The systematic application of policies, procedures and practices to the tasks of establishing the context of, identifying, analyzing, evaluating, communicating, treating and monitoring risk.

Risk Mitigation: A risk mitigation action refers to actions that must be taken to lower the likelihood of the risk occurring and/or to minimize the impact if the risk did occur. Risk can never be totally eliminated, but it can be mitigated to lessen its likelihood and or impact

POLICY

Below are statements that should be complied with.

Policy Statements

No:	Statements
	[Organisation] shall identify and adopt a risk assessment methodology that is suited to its business, legal and regulatory requirements.
	Formal risk assessments of [organisation] IT environment shall be conducted annually. Adequate mitigating controls to reduce or eliminate these risks shall be implemented.
	Procedures and processes shall be put in place to monitor the effectiveness of the implemented security controls.
	[Organisation] shall develop criteria for accepting risks and identifying the acceptable levels of risk.
	The risk assessment methodology selected must ensure that risk assessments produce comparable and reproducible results.
	Network resources should be assigned one of the following three risk levels and the appropriate level of security based on this classification should be applied. o **Low Risk** Systems or Data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would not disrupt the business or cause legal or financial ramifications. The targeted system or data can be easily restored and does not permit further access of other systems. o **Medium Risk** Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause a moderate disruption in business, minor legal or financial ramifications, or provide further access to other systems. The targeted system or data requires a moderate effort to restore or the restoration process is disruptive to the system. o **High Risk** Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause an extreme disruption in business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore or the restoration process is disruptive to the business or other Systems.
	[organisation] shall develop and implement specific risk management plans for high impact risks, while lower impact risks may be accepted and monitored.
	There must be oversight and review of the Risk Register and any changes that might affect it.

	Monitoring and review of [organisation] risks shall occur throughout the risk management process.
	Appropriate communication and consultation shall take place with internal and external stakeholders at relevant stages of the risk management process in a way that will enable [organisation] minimise losses and capitalise on opportunities.
	There shall be an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment
	Risk assessment must be carried out on all changes across the IT infrastructures & assets.

The risk assessment process must have a clearly documented process as shown below: