<< [Organisation] Logo>>

<< Wireless Access 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 purpose of this document is to outline policy statement to be followed to protect [Organisation] resources while being access via wireless commination, thus protecting the [Organisation] from unauthorised use and/or malicious attack that could result in loss of information, damage to critical applications, or damage to [Organisation] 's reputation.

All users employing wireless methods of accessing technology resources must adhere to [Organisation] defined policy for doing so, using approved access points. Unauthorised access to the wireless network is not permitted.

SCOPE

This policy only pertains to staff accessing technology resources via an onsite located access point.

POLICY

The following are the statement for wireless access to technology resources.

Policy Statements

No:	Statements
	All staff will have access to the wireless network via a secure access control mechanism .
	Wireless access points will be setup and managed only by ICT Team.
	By using [Organisation] 's wireless network with personal or [Organisation] -supplied equipment, staff must understand that their machines are a de facto extension of [Organisation] 's network, and as such, must comply with the [Organisation] 's policies.
	It is the responsibility of the staff to maintain latest virus definitions and operating system service packs/patches.
	It is the responsibility of the staff with wireless privileges to ensure that unauthorised

	persons are not allowed access to internal networks.
	The [Organisation] does not allow unauthorised network sniffing and/or monitoring on the wireless network. Staff found using this type of software will be prevented from accessing the wireless network. Please contact ICT Team if you suspect that this is occurring.
	Only authorised staff can access the Internet through [Organisation] 's wireless network.
	Connecting your own WiFi access point to the [Organisation] network is strictly forbidden.