IT@RAMS
Galambila, Durri, Biripi, Tobwabba & Werin

Access to Confidential data from Unsecured Computer Equipment Policy & User Declaration

Issued: 21st August 2020

Author: Jon Rolph

BYO/REMOTE ACCESS POLICY

Document Control

Date	Ver #	Change Description	Author
27/03/2013	0.1	First draft	Jon Rolph
30/05/2016	1.0	Complete first published document	Jon Rolph
18/08/2020	1.1	Change name from 'IT Remote Access User Declaration' to 'IT BYOD & Remote User Declaration'. Make site specific and add requirement for malware recognition training.	Jon Rolph & Damian Cutler
24/08/2020	1.2	Minor updated following feedback in IT Management meeting	Jon Rolph

Authorisation

Name	Position	Signature & Date
Reuben Robinson	CEO Galambila	
Lisa Ogolo	CEO Biripi	
Chris Spencer	Interim CEO Tobwabba	
Stephen Blunden	Acting CEO Durri	
Fay Adamson	CEO Werin	

Initials: _____

BYO/REMOTE ACCESS POLICY

1. Introduction

This document is a supplement to the 'Internet, Email and Computer Use Policy & User Declaration'. It is intended for users who are provided with access to business information from outside the network managed by IT@RAMS or from computers and other similar devices that are not provided by IT@RAMS (called 'Remote/BYOD access' throughout this document).

Werin Aboriginal Corporation (Werin) recognises the usefulness of Remote/BYOD access, particularly to provide the flexibility of home working and access to check medical results when away from the clinic. This way of working does, however, introduce a number of additional risks to the confidentiality and integrity of the information within our IT systems. This policy sets out the risks and the mitigation that users of this facility must adhere to.

Remote/BYOD access is a privilege and provided only to employees who adhere to this policy. Violation of the policy could result in disciplinary and/or legal action leading up to and including termination of employment. Employees may also be held personally liable for damages caused by any violations of this policy. All employees are required to acknowledge receipt and confirm that they have understood and agree to abide by the rules hereunder.

This policy does not form part of an employee's contract of employment or any other User's contract.

If you are unsure about any matter covered by this policy, you should seek the assistance of your supervisor, the IT Helpdesk or the Regional IT Manager.

2. Scope

This policy applies to all employees, consultants and contractors of Werin who access confidential information related to Werin from outside locations or when using non-IT@RAMS equipment. An example or this would be accessing Medical records from a personal home computer.

3. Guidelines for Remote/BYOD access to confidential information

Users must comply with the following guidelines when using Remote/BYOD access to confidential information:

(a) Only the person named in this declaration is permitted to access confidential information under this declaration.

(b) Any information related to the technologies, configurations or techniques used to gain Remote/BYOD access is to be kept confidential and not disclosed to **any** party without the express permission of Werin.

(c) Remote/BYOD access must only to be gained in a private environment where both the information accessed and the method of accessing it are expected to unobserved.

(d) Users should ensure that they do not leave the device, through which they gain Remote/BYOD access unattended at any time whilst Remote/BYOD access is being utilised.

(e) Users must log off from applications used to gain Remote/BYOD access (Medical Director, MYOB, etc.) at the end of each Remote/BYOD access session.

Initials: _____

(f) Remote users must undertake a short e-learning course on tips for recognising phishing.
This should be requested via email to it-training@Werin.org.au

4. Support of Remote/BYOD access

Remote/BYOD access is necessarily outside the normal support processes of IT@RAMS. Support for this solution is therefore restricted to the following:

(a) Where support relates to components within the IT@RAMS IT environment (for example, Domain password reset) normal support will be provided. This is Monday to Friday 8am to 5pm via phone or email.

(b) Written instructions of how to set up remote access on a number of common devices will be provided.

(c) Telephone support (business hours) during the initial set-up of the Remote/BYOD access software will be provided.

5. Breach of this Policy

Any breach of this policy may result in disciplinary action, including any of the following:

(a) Counselling

(b) Warning

(c) Suspension (Permanent or Temporary)

(d) Termination

(e) for contractors, the termination or non-renewal of contractual arrangements

6. Document completion

Please complete the statement below and initial each page of this document. Once completed this document should be returned to your supervisor and will be kept in your personnel file.

A copy of the completed document must be attached to your IT Access form, along with proof of completing the phishing e-learning course, within five working days of you first accessing the IT Services. Failure to do so may result in revocation of remote access.

7. Acknowledgement Statement

I acknowledge receiving this policy, which contains important information about conditions for Remote/BYOD access to confidential information. I confirm that I have read and understand the information contained in the policy and agree to comply with the requirements contained within.

Your name: _____

Signed: _____

Date: _____

Initials: _____