

CERTIFICATE

This is to certify that:

Authable Partners Pty Ltd

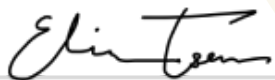
ABN: 59675173565
VIC 3444
Australia

is hereby certified as having attained
the following certification:

Cyber Security Certification Australia (CSCAU)



**LEVEL 3
GOLD**



Dr Elinor Tsen
Certification Registrar

This certificate of registration is issued to Authable Partners Pty Ltd (Organisation) by CyberCert in reliance on the Letter of Attestation provided by the organisation dated 15/10/2024.

The organisation has permission to display the relevant CyberCert certification badge including on the organisation's website. This certification may be revoked by CyberCert if the organisation fails to meet any of the certification requirements. This certification can be validated online by scanning the QR code.



Certificate ID:
012430000059675173565G

Standard Release:
SMB1001:2023

Issue Date:
15 October 2024

Expiry Date:
16 October 2025

SCAN QR CODE TO VALIDATE



CyberCert Pty Ltd
ABN 87 662 681 423
60 Martin Place,
Sydney, NSW 2000
Australia

Schedule of Conformity

Cyber Security Certification Australia (CSCAU)

Standard Release: SMB1001:2023

Certification Requirements - Implemented

The Organisation has attested that the following certification requirements have been implemented within the Organisation.

ID	Requirement Name
1.1.0.0	Engage a technical support specialist for your organization
1.2.0.0	Install and configure a firewall
1.3.0.0	Install anti-virus software on all organizational devices
1.4.0.0	Automatically install tested and approved software updates and patches on all organizational devices
1.5.0.0	Install TLS certificates on all public internet facing websites
1.6.0.0	Ensure all servers are updated and patched
2.1.0.0	Change passwords routinely
2.2.0.0	Ensure employee accounts do not have administrative privileges
2.3.0.0	Ensure employees have individual user accounts
2.4.1.0	Implement a password manager system
2.5.0.0	MFA on all employee email accounts
2.6.0.0	MFA on all business applications and social media accounts
3.1.0.0	Implement a backup and recovery strategy for important digital assets
4.1.0.0	Confidentiality agreement for all employees
4.2.0.0	Implement a policy with procedures to prevent Invoice Fraud
4.3.0.0	Implement a visitor register
4.4.0.0	Implement a cyber security policy
4.5.0.0	Implement a response plan for cyber related incidents
4.6.0.0	Utilize secure methods of physical document destruction
4.7.0.0	Ensure all computer devices that store sensitive, private, and/or confidential information are disposed of securely
4.8.0.0	Implement and maintain a digital asset register
5.1.0.0	Conduct cyber security awareness training for all employees
