cybercert

CERTIFICATE

This is to certify that:

Iriq Pty Ltd

ABN: 75138262674
Trading as: Iriq Pty Ltd

QLD
Australia

is hereby certified as having
attained the following certification:

Dynamic Standards International (DSI)

DYNAMIC STANDARDS INTERNATIONAL

SMB1001 - LEVEL 3
GOLD

cybercert
SMB1001
GOLD
LEVEL 3

Certificate ID:
012630000075138262674Y

Standard Release:
SMB1001:2026

Issue Date:
2 Oct 2026

Expiry Date:
3 Oct 2027

Ryan Ettridge
Chief Executive Officer

SCAN QR CODE TO VALIDATE

This certificate of registration is issued to Iriq Pty Ltd (Organisation) by CyberCert in reliance on the Letter of Attestation provided by the organisation dated 10/02/2026.

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.

CyberCert Pty Ltd
ABN 650 892 514
60 Martin Place
Sydney, NSW 2000
Australia

TURN OVER FOR SCHEDULE OF CONFORMITY

Schedule of Conformity

Dynamic Standards International (DSI)

Standard Release: SMB1001:2026

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
1.2.0.1	Install and configure a firewall
1.3.0.1	Install anti-virus software on all organization devices
1.4.0.0	Automatically install tested and approved software updates and patches on all organization devices
1.5.0.0	Install TLS certificates on all public internet facing websites
1.6.0.1	Ensure all servers are updated and patched
1.12.0.0	Implement Endpoint Detection and Response (EDR)
2.1.0.1	Ensure strong password hygiene is maintained
2.2.0.0	Ensure employee accounts do not have administrative privileges
2.3.0.0	Ensure employees have individual user accounts
2.4.1.1	Implement a password manager system
2.5.0.0	Multi-factor authentication (MFA) on all employee email accounts
2.6.0.0	MFA on all business applications and social media accounts
2.7.0.1	Ensure Remote Desktop Protocol (RDP) occurs only over Virtual Private Network (VPN) connections
2.12.1.0	Email Authentication and Anti-Spoofing
3.1.0.1	Implement a backup and recovery strategy for important digital assets
3.2.0.0	Purchase and maintain business or cyber insurance
4.1.0.1	Confidentiality agreement for all employees, contractors and third parties
4.2.0.1	Implement a policy with procedures to manage Invoice Fraud
4.3.0.0	Implement a visitor register
4.4.0.0	Implement a cybersecurity 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
4.11.0.0	Implement a policy for the responsible and secure use of AI technology
5.1.1.0	Conduct cybersecurity awareness training for all employees