

CYBERSECURITY & COMPLIANCE FOR NDIS PROVIDERS

Why this applies to disability care providers

■ NDIS Practice Standards – the NDIS Commission requires providers to have information management and risk systems in place as a condition of registration.	■ Privacy Act 1988 – covers collection, storage and breach handling of participant personal and health information, with mandatory notification for eligible data breaches.
■ Essential 8 / ISO/IEC 27001 – not mandatory for every provider, but increasingly expected by insurers, funders, and larger referral partners as evidence of good practice.	

What's typically at risk

■ Participant health and personal data stored across shared drives, email, or rostering/case management systems.	■ Staff and support worker access — devices, shared logins, and remote access to client records.
■ Incident and breach reporting obligations to the NDIS Commission and Office of the Australian Information Commissioner (OAIC).	

How we help

■ A practical gap assessment against NDIS Practice Standards, Essential 8, and Privacy Act requirements.	■ A prioritised remediation plan sized to your team — no dedicated security hire required.
■ Ongoing support so compliance stays current as your organisation and the standards evolve.	

