

Position Description

Position Title:	Security and Compliance Officer
Division:	ICT
Reporting To:	Head of Infrastructure
Direct Reports:	Nil

ABOUT NORTHCOTT:

Who is Northcott?

Northcott is a not-for-profit disability service provider that works with customers to realise their potential.

As one of Australia's largest not-for-profit disability service organisations, we provide services from metropolitan and regional locations throughout NSW, QLD, and the ACT. We have more than 90 years of experience and expertise in the disability service industry.

A registered NDIS provider, we employ approximately 2,600 staff and provide empowering, personalised services to over 13,500 people with disability, their families and carers each year.

What do we do?

Northcott provides personalised and dynamic support, delivered by a committed team who will optimise and maximise support and services for every customer.

Our experience and expertise gives confidence to our customers they are in good, trustworthy hands, while our commitment to innovation and pushing boundaries allows us to tackle any challenge currently creating barriers for our customers to reach their potential.

What is our promise to each customer?

We will work creatively and relentlessly with each customer to unlock, discover and unleash their potential, supporting and empowering them to be the best they can be now and in the future.

Our customers are not numbers; they are unique individuals. We personalise our services to each customer's current and future needs and goals, every single one, to ensure their development and growth.

As advocates for our customer's inclusion, we will empower them with confidence, choice and opportunity so they can live their life, as they choose, in their own way.

Our Values

Our values have always been a significant part of our service to customers and they have helped shape Northcott into the wonderful organisation it is today. We are Innovative because we develop new ideas and solutions with creativity in anticipation of changing needs. We are Respectful because we believe that everyone's voice is unique and that they have the right to be heard. We are Brave because we have the courage to stand up for people with all abilities even in the face of adversity.

Position Description

Diversity and Inclusion

Northcott actively promotes diversity and inclusion. We are committed to providing a workplace where every person is valued, respected and supported to progress. Northcott ensures no one is disadvantaged on the basis of their Aboriginal and Torres Strait Islander identity, culture, LGBTIQ+ identity, disability, gender, age, religion or caring responsibilities. We recognise the important role language and cultural understanding play in connecting with and supporting our diverse communities.

KEY OBJECTIVE OF THE SERVICE/DEPARTMENT:

To define, deliver and continuously improve Northcott's digital products and experiences so they better support customers, families/carers and staff, and enable efficient, compliant and high-quality service delivery.

KEY OBJECTIVE OF THE POSITION:

- Own and maintain a prioritised cybersecurity roadmap aligned with Northcott's risk appetite, ICT strategy and operational needs.
- Coordinate Essential Eight maturity uplift, security remediation and assurance activities across internal teams and delivery partners.
- Maintain clear security governance, policies, standards, risk records, control evidence and audit documentation.
- Build strong stakeholder ownership of security controls through practical advice, communication, training and transparent reporting.

PERSON SPECIFICATIONS (SKILLS & KNOWLEDGE)

- Highly organised, persistent and accountable, with strong follow-through on actions and commitments.
- Collaborative and approachable, with the confidence to coordinate across technical, operational and executive stakeholders.
- Detail-oriented and careful when handling sensitive information, evidence and audit documentation.
- Pragmatic and solutions-focused, balancing security improvement with operational impact and business priorities.
- Clear written and verbal communicator who can make security requirements understandable and actionable.
- Working knowledge of Microsoft 365 security capabilities, identity and access controls, data protection and security reporting.
- Strong documentation, analysis, prioritisation and stakeholder communication skills, with the ability to translate technical risks into practical business actions.

ESSENTIAL QUALIFICATIONS & EXPERIENCE REQUIRED

- Demonstrated experience in cybersecurity governance, security product ownership, risk, compliance, audit coordination or technology assurance.

Position Description

- Practical knowledge of the ASD Essential Eight, security control frameworks, access governance, privacy and audit evidence requirements.
- Experience coordinating internal teams, managed service providers, auditors and specialist vendors to deliver security outcomes.
- One or more of the following certifications are highly regarded:
 - Relevant Microsoft Security certification, such as SC-900, SC-300, AZ-500 or SC-100.
 - ISO 27001 Foundation, Lead Implementer or Lead Auditor.
 - CISSP, CISM, CRISC or equivalent security, risk or governance certification.
 - Product ownership, project delivery or IT service management certification.

DELEGATION LEVEL

- NIL

CORE COMPETENCIES OF THE ROLE

Security and Compliance Ownership and Roadmap

- Maintain the security roadmap, backlog, priorities, dependencies and delivery status in consultation with ICT leadership.
- Translate audit findings, risk assessments and business needs into clear control requirements, actions and measurable outcomes.
- Coordinate work across ICT, business owners, Inteliworx and specialist security partners, escalating blockers and risks promptly.

Governance, Risk, Compliance and Assurance

- Coordinate internal and external security audits, including evidence collection, validation, safe information sharing and stakeholder follow-up.
- Maintain security policies, standards, procedures, control records, risk and remediation registers, and auditable decision records.
- Coordinate recurring access and permissions reviews for key systems and ensure exceptions and findings are documented and addressed.
- Support alignment with the ASD Essential Eight, ISO 27001 principles, privacy obligations, NDIS requirements and relevant contractual commitments.

Security Controls, Data Protection and Awareness

- Monitor the effectiveness of assigned security controls across Microsoft 365, identity, endpoint, application and data environments, working with technical owners to resolve gaps.
- Support secure use of AI and emerging technologies through appropriate assessments, guardrails, data protection requirements and governance documentation.
- Coordinate security awareness initiatives and practical guidance for staff, privileged users and system owners.
- Provide clear reporting on control performance, risks, overdue actions and improvement opportunities.

Incident Preparedness, Response and Communication

Position Description

- Maintain security incident and disaster recovery playbooks, stakeholder contacts, escalation paths and communication templates.
- Coordinate technical recovery activities, vendor engagement, evidence capture and status reporting during security incidents.
- Support post-incident reviews and track agreed corrective actions through to closure.

DUTIES

The typical duties of this position include:

1. Security roadmap priorities, dependencies and delivery status are current, visible and actively managed.
2. Essential Eight and other agreed security maturity targets show measurable progress.
3. Audit evidence is complete, accurate, securely shared and available when required.
4. Access reviews, risk treatments and remediation actions are completed within agreed timeframes, with exceptions clearly documented.
5. Security incidents and recovery activities are coordinated effectively, with timely stakeholder communications and lessons captured.
6. Stakeholders understand their security responsibilities and report confidence in the clarity, practicality and responsiveness of the security function.

This list is indicative only and is subject to change. All Northcott employees are required to comply with any reasonable work requests as directed by their employer from time to time.

NORTHCOTT POLICY AND PROCEDURES

All Northcott employees are expected to be familiar with and adhere to Northcott policies and procedures. For more information, see your manager or refer to the policy and procedures available on the Northcott Intranet.

Employee's Signature

Employee's Name

Date

Please forward a signed copy to Human Resources.