UNIQ You National Security & Cyber Risk Management Plan

Last Updated: 16 February 2026

Purpose

This National Security & Cyber Risk Management Plan outlines how UNIQ YOU identifies, assesses and manages cyber security and national security risks that may impact organisational operations, personal information, safeguarding systems and service delivery.

As an organisation working with children and young people, UNIQ YOU recognises that cyber security is directly linked to child safety, privacy and organisational integrity.

This Plan aligns with:

- Privacy Act 1988 (Cth)
- Australian Privacy Principles
- Notifiable Data Breaches Scheme
- Applicable Working With Children legislation across Australian jurisdictions
- National Principles for Child Safe Organisations

This Plan operates in conjunction with the Privacy Policy, Information Technology Policy and Child & Youth Risk Management Strategy.

Scope

This Plan applies to:

- All Board members
- Employees
- Volunteers
- Advisors
- Contractors
- Third-party service providers

It applies to:

- Cloud platforms
- Online delivery systems
- Email and communications
- Data storage systems
- Devices used for organisational purposes
- Digital engagement environments

Security Governance and Oversight

Cyber and security risks are overseen by the Board and Executive leadership.

Leadership is responsible for:

- Monitoring risk trends
- Ensuring adequate safeguards
- Allocating appropriate resources
- Reviewing incident responses
- Ensuring compliance with national legislation

Cyber risk is integrated into the organisational risk register and reviewed periodically.

Risk Identification

UNIQ YOU identifies and monitors potential threats including:

- Unauthorised access to personal information
- Data breaches
- Phishing and social engineering attacks
- Ransomware and malware
- Insider misuse of information
- Compromise of online delivery platforms
- Supply chain and third-party vendor risks

- Loss or theft of devices
- System outages impacting safeguarding operations

Risks are assessed based on:

- Likelihood
- Impact
- Impact on child safety
- Reputational impact
- Regulatory impact

Technical Safeguards

Technical controls are implemented through internal Information Technology policies and operational procedures.

Safeguards include:

- Role-based access controls
- Multi-factor authentication
- Secure cloud-based storage
- Encrypted data transmission
- Secure password standards
- Regular software updates
- Access logging and monitoring
- Controlled administrative privileges

Detailed system-level controls are documented in the Information Technology Policy (internal document).

Information Handling and Privacy Alignment

All personal information is managed in accordance with the UNIQ YOU Privacy Policy.

Cyber security controls support privacy compliance by:

- Limiting access to authorised personnel
- Protecting against unauthorised modification
- Preventing unlawful disclosure
- Ensuring secure destruction or de-identification

This Plan does not duplicate privacy provisions but supports their enforcement.

Incident Response and Escalation

In the event of a cyber security incident:

1. Immediate containment measures are initiated
2. Systems are assessed to determine scope and impact
3. Child safety implications are prioritised
4. Executive leadership is notified
5. External specialists may be engaged where required
6. Assessment is conducted under the Notifiable Data Breaches Scheme
7. Regulatory notifications are made where required

If an incident impacts child safety, response procedures align with the Child Safety & Wellbeing Policy and Managing Breaches Plan.

All incidents are documented and reviewed.

Business Continuity

UNIQ YOU maintains continuity measures to ensure safeguarding functions can continue in the event of:

- Cyber attack
- System outage
- Loss of cloud access
- Device compromise

Critical functions include:

- Safeguarding reporting
- Access to risk management documents
- Communication with schools and authorities
- Access to child safety procedures

Continuity planning is reviewed periodically.

Third-Party Risk

Where third-party providers are engaged (including cloud service providers), UNIQ YOU:

- Assesses vendor security standards
- Reviews privacy compliance obligations
- Monitors contractual safeguards
- Ensures reasonable steps are taken to align with Australian Privacy Principles

UNIQ YOU recognises that third-party risk forms part of its overall cyber risk exposure.

Cultural Safety Considerations

Cyber security responses must consider potential cultural impacts, particularly where information involves Aboriginal and Torres Strait Islander children and families.

Data breaches or cyber incidents must be managed in ways that:

- Avoid further harm or retraumatisation
- Respect cultural identity and privacy
- Prevent discriminatory misuse of information

Monitoring and Continuous Improvement

UNIQ YOU monitors cyber security performance through:

- Incident trend analysis
- Access audits

- Staff training compliance
- Periodic review of risk assessments
- Board oversight

This Plan is reviewed annually or following significant incident.

Relationship to Other Policies

This Plan should be read alongside:

- Privacy Policy
- Information Technology Policy (internal)
- Child Safety & Wellbeing Policy
- Child & Youth Risk Management Strategy
- Managing Breaches Plan
- Code of Conduct