Request for proposal (RFP)

Name of project: Managed Services Provider Tender

Our Watch ABN 60 164 123 844

Date: 18th August 2025

Acknowledgement of Country

Our Watch acknowledges the Traditional Owners of the land across Australia on which we work and live. We pay our respects to Aboriginal and Torres Strait Islander peoples past and present.

Type of goods or services

Technology Managed Services Provider

Key dates for this RFP

- Closing date for supplier questions: Friday, 5th September 2025. Questions must be submitted via email. Responses will be de-identified and information shared with potential suppliers to this RFP.
- Closing Date for supplier responses: Friday, 26th September 2025

Our Watch contact person

All communication should be directed to:

Paul Chan
Manager Technology and Facilities
+61 417 609 658
paul.chan@ourwatch.org.au

Contents

This document consists of:

Part A – About us

1. Our Watch background

Our Watch is a national leader in the primary prevention of violence against women and their children in Australia. We work to embed gender equality and prevent violence where Australians live, learn, work, and socialise.

Our Watch is a company with an independent Board. The company members include the Commonwealth, State and Territory governments.

2. Change the story: a shared framework

- *Change the story* is our evidence-based framework for a national approach to preventing violence against women.
- *Changing the picture* is a resource to support the prevention of violence against Aboriginal and Torres Strait Islander women.
- *Changing the landscape* is a resource to support the prevention of violence against women and girls with disabilities.

See publications Change the story, Changing the picture, and Changing the landscape.

3. Our values

Our Watch's Strategic plan 2024-29 describes our values as an organisation.

Our Watch is committed to our Stretch Reconciliation Action Plan. Our Watch shares Reconciliation Australia's vision of a reconciled, just and equitable Australia, where the voices, experiences and ideas of Aboriginal and Torres Strait Islander peoples are central.

We are dedicated to an intersection approach, recognising the impacts of multiple intersecting forms of social inequality, discrimination and disadvantage.

Part B – Goods & services requirements

1. Purpose

Our Watch is seeking proposals from Managed Service Providers (MSPs) with a proven track record in delivering comprehensive IT services and support. We require an MSP with expertise in Microsoft 365 and SaaS environments, with capability to enhance our cybersecurity posture, and to provide proactive IT support as well as being flexible enough to align with our organizational needs.

2. Reporting

The Supplier will report to the Manager of Facilities and Technology. The IT function reports to the Director of Corporate Services.

3. Standards, guides, and materials

3.1 The Supplier must ensure goods and services comply with all applicable standards. This includes but is not limited to:

- Australian Cyber Security Recommendations (Essential 8).
- Australian Privacy Act 1998 (Cth) and Australian Privacy Principals (APPs).
- Information Technology Operations and Governance Frameworks, such as: the Information Technology Infrastructure Library Principals (ITIL).

3.2 In addition, Our Watch may provide its own policies, confidential materials, or data that is directly relevant to the goods or services.

4. Requirements

4.1 Transition Plans

Our Watch is currently supported by a managed services provider. A range of transition plans should be provided with a clear recommendation as to a preferential plan. For example:

- An immediate cut-over transition likely spanning a few weeks.
- A slower transition plan likely spanning a few months.
- A phased approach where the Supplier would provide consultants to aid in bringing the Technology stack inhouse and completing some transformational

projects. Once complete, transitioning to a managed services contract for on-going support.

4.2 Core IT Services Scope

a) Management and support of Microsoft 365 including:
   - Licensing
   - Onboarding/Offboarding Staff Members
   - Troubleshooting and general support
   - Regular backups and restore as required time-to-time
   - Advising us on emerging Microsoft technologies and cyber-security changes.
   - Tenancy alignment with the selected Cyber Security Roadmaps.
   - Integration of SaaS applications to Microsoft 365 tenancy.

b) Core networking infrastructure management and support including:
   - Provisioning of data connectivity to our office premises within Australia.
   - Provisioning of Wi-Fi networks in accordance with industry best practice and to ensure alignment to selected Cyber Security Roadmaps.
   - Managing networking infrastructure: Logging and troubleshooting traffic issues and ensuring network performance is adequate to meet staff needs.

c) End user computing management and support:
   - Maintain documentation for in-support devices.
   - Onboard devices onto central management system, and offboard when retired.
   - Provide system configuration and user support when required for staff issued with a device – excepting any software, SaaS product, or cloud products managed by ourselves.
   - Configure, apply, and maintain security settings and associated software to ensure alignment to selected Cyber Security Roadmaps.
   - Provide advice as to hardware selection and recommend warranty service appropriate for in-service devices.
   - Deliver a helpdesk service for first-level triage and end-user support to our staff, both in our Melbourne offices and to staff working remotely across Australia.
   - Provide remote support for staff travelling overseas.
   - Provide escalation pathway for complex issues as well as issues that are time sensitive.
   - Configure, maintain, and support Microsoft 365 environment for the End User.
   - Assist user in hardware fault diagnosis and assist with any warranty claim for on-site service.

d) Procurement services on request:
   - Quotations for hardware as required including end-user devices, and network infrastructure.
   - Quotations for software, SaaS products, or cloud services as required.

e) Ability to access any available not-for-profit pricing from vendors.

4.3 Security and Compliance Scope

a) Implementation and maintenance of cybersecurity best practices (e.g., SOC monitoring, endpoint protection, incident response plans).
b) Advice and recommendations in adoption of Cyber Security controls to comply with relevant frameworks (e.g., ISO 27001, NIST, Essential 8).
c) Proposal for the resourcing and provision of technical resources for cybersecurity and infrastructure projects.
d) Advice and support in supplying cybersecurity awareness training and phishing simulations.

4.4 Proactive IT Management

a) Regular reporting on issues reported and resolved. Eg: Ticket statistics like resolution time, number of tickets opened/closed etc.
b) Regular meetings with customers to review projects and escalated tickets.
c) Supporting periodic IT auditing, IT Security reviews, and other activities such as Penetration Testing.
d) Advising us on our technology roadmap development and strategic IT direction.

4.5 Organisational cultural fit

a) Experience in dealing with similar not-for-profit organisations as our organisation.
b) Our Watch welcomes the opportunity to work with suppliers who have similarly aligned values as our organisation. We welcome respondents to outline any existing policies, initiatives, evidence or certifications that may demonstrate their alignment. This may include:
    - Embedding gender equality within their organisation and/or sector
    - Empowering Aboriginal and Torres Strait Islander businesses and Peoples
    - Fostering thriving communities and supporting people from marginalised groups
    - Reducing environmental impacts and addressing climate change
    - Human rights and eliminating modern slavery.

5. Evaluation Criteria

5.1 Key evaluation criteria:

a) Proven experience in managing Microsoft 365.
b) Strong track record in cybersecurity and risk mitigation.
c) Clear Service Level Agreements (SLAs) with rapid response and resolution times.
d) SLA breach procedures and conditions.
e) Transparent pricing and contract flexibility.
f) Dedicated account management and strong customer service.
g) Ability to scale services as needed.
h) Alignment with Australian Cyber Security guidelines, Australian Privacy Act 1988 - Australian Privacy Principals (APPs), and Information Technology Infrastructure Library Principles (ITIL).

5.2 Additional Evaluation Criteria:

i) Organisational cultural fit – experience with non-profit clients, and alignment with Our Watch values.

Part C – Supplier Response Form

Please include this Part C – Supplier Response Form as part of your quote.

Name of Supplier	
ACN or ABN	
Address	
Contact name, phone and email	

I accept the terms and conditions of this Request for Proposal. Signed by a supplier delegate, who represents they have the authority to act on behalf of the Supplier:

Signature	
Name and role	

1. Details of proposal

Your response must address these queries.

Focus area 1 – Your capabilities and experience

1.1 Provide a company overview covering your background, experience, and values alignment to Our Watch.

1.2 Describe your approach to service delivery. How will your organisation meet our service needs?

1.3 Tell us about your commitments to service delivery. Describe any Service Level Agreements (SLAs) – what are the response and resolution times. What happens if these are breached?

1.4 Provide your proposed service structure, escalation process, and key staff members that will be allocated to support this structure.

1.5 Provide an outline of your Security & Compliance strategy. How will you use this to enhance and strengthen our cyber security posture?

1.6 Describe the termination terms of any engagement with you. What data handover processes, transition-out assistance, administrator privileges handover, and other relevant clauses.

1.7 Are you able to provide the contact details for 1 or 2 referees?

Focus area 2 – Draft contract terms

1.8 Will you use the Our Watch Contractor Agreement (Attachment 1) as the basis to reach a fully signed agreement? [Yes/No]

If no, please explain, or attach your proposed contract terms and conditions.

2. Proposed pricing

2.1 Please provide your proposed pricing. Amounts should be stated exclusive of GST. The price is all-inclusive and covers expenses, unless otherwise stated.

2.2 How long is this quote valid for?

3. Quality, Risk and Compliance

3.1 **Insurance information** – Provide details of your relevant insurance(s) including:

- Name of insurance company

- Policy type (e.g. public liability, professional indemnity, cyber, etc)

- Amount / limit

- Expiry date

3.2 **Compliance and legal** – In the past 2 years, has your organisation had Court proceedings, orders or legal rulings against it for breach of any laws? If so, please list.

3.3 **Employment conditions** – Does your organisation have suitable practices in occupational health and safety, wages, and superannuation entitlements?

3.4 **Working with children or vulnerable people** – If the goods or services require working with children or vulnerable people, please outline any safety strategies you will implement. If applicable, does your organisation comply with Working with Children Checks?

3.5 **Modern slavery –** Is your yearly consolidated revenue over $100 million? If so, is your organisation compliant with Modern slavery laws? Are your hardware and software vendors compliant with modern slavery laws?

3.6 **Conflict of interest** – Provide details of other interests, relationships or clients that create a conflict of interest, or might create one. Outline the processes you have in place to manage a conflict of interest.

3.7 **Vendor Qualifications/Certifications** – Provide details of relevant qualifications or certifications. For example: ISO 9001 Quality Management Certification, ISO 27001 Information Security Management, or other industry specific certification.

4. Other

Include any additional information about your proposal here. Include any other services that might differentiate your organisation from others.

Part D – RFP terms and conditions

1. Our Watch may amend this RFP at any time before the Closing Date.
2. Our Watch, acting in good faith, may stop or pause this RFP process, decline to accept a response, decline to issue a contract, or fulfill its work requirements separately from this RFP process.
3. At any time before execution of the contract, Our Watch may seek information from, and enter discussions with, any Potential Suppliers in relation to their responses. But Our Watch will not allow any Potential Supplier to substantially tailor or amend their response.
4. No contract will be formed until executed by Our Watch.

Evaluation of RFP

5. Our Watch will assess the extent to which the response meets RFP requirements and will determine the best value outcome for Our Watch.
6. Our Watch may consider if a response helps Our Watch to deliver social procurement outcomes, including gender equality, eliminating modern slavery, the environment, and social enterprise.
7. Our Watch will notify all Potential Suppliers of the final decision and, if requested, will provide a debrief following award of the contract.

Use of information and confidentiality

8. Our Watch may publicly disclose the Supplier's name, address and other details about the contract, including contract value and the names of subcontractors.
9. Potential Suppliers acknowledge that Our Watch has reporting and transparency requirements, including responsibilities to its funders, and company members ("reporting requirements"). Our Watch may disclose information to its funders or company members, where this is reasonably necessary.
10. Potential Suppliers must identify any of their information they consider confidential or sensitive. Our Watch will treat information as confidential, subject to any laws and Our Watch's reporting requirements.

Conflict of interest & proper conduct

11. Potential Suppliers must notify Our Watch immediately if an actual or perceived conflict of interest arises.
12. Any contract agreement will require that sub-contracting is only permitted with in-writing consent from an authorised Our Watch employee.
13. Potential Suppliers and their officers, employees, agents and advisors must not engage in fraudulent, anti-competitive, or similar improper conduct, in connection with this RFP.
14. Suppliers may need to engage with Our Watch's Australian government stakeholders. Our Watch is required to note that giving false or misleading information to the Commonwealth is an offence (Criminal Code Act 1995 (Cth)).

Attachment 1: Template Contractor Agreement

Refer to template Contractor Agreement attached.