CUATIS2024 Schedule 2 - Specification / Statement of Requirements

1. Statement of Requirements

This Request document outlines the requirements for a new Common Use Arrangement (CUA) for Technology Infrastructure and Solutions (CUATIS2024).

CUATIS2024 will operate as a standing offer arrangement (Head Agreement), with orders (Customer Contracts) to be placed on an 'as required' basis by WA public authorities and other Potential Customers to support business operations.

The CUA will be mandatory within the Perth metropolitan area and non-mandatory within regional and remote areas.

Respondents are invited to submit an Offer for one or more categories.

The Contract Authority reserves the right to appoint one or more Contractors to each category.

2. CUA Scope

CUATIS2024 will comprise of the following panels and associated categories:

2.1 Panel 1 - Infrastructure and Facilities

This panel covers the acquisition and leasing of infrastructure equipment and the necessary supporting functions, including software licencing and installation. It consists of the following categories:

- **Category 1A - Networking Equipment**

  This category covers infrastructure used to support IP networking including, but not limited to, modems, firewalls, security appliances, routers, switches and wireless.

  This excludes infrastructure for end-use or telemetry equipment with the in-built ability to connect to public voice, data cellular and satellite networks.

  For public voice, cellular and satellite connectivity equipment refer to the '**Telecommunications Solutions CUA (CUATEL2021)'**.

- **Category 1B - Data Centre Equipment**

  This category covers infrastructure for use within a data centre including, but not limited to, servers, storage systems, appliances, UPS and peripherals.

  For administrative management services, '**Panel 3 – Category 3B**', under this CUA is to be used.

- **Category 1C - Colocation**

  This category covers the leasing of secured areas, racks or rack space with associated managed power, cooling, security and connectivity services.

  For administrative management services, '**Panel 3 – Category 3B**', under this CUA is to be used.

2.2 Panel 2 - Hybrid Cloud

This panel covers the management of software defined platforms with subscription or consumption-based pricing that simplify the management of technical infrastructure.

The provision of hybrid cloud under Panel 2 may include IT infrastructure equipment to meet the procurement outcomes.

In submitting an offer for Panel 2, Respondents are not required to submit a separate offer under Panel 1 **unless** the offered infrastructure and facilities will be offered in isolation to Panel 2.

For the procurement of any supporting software covered by an existing mandatory CUA, the Customer is required to adhere to the Buying Rules of the existing CUA.

Public cloud services are out of scope of this CUA.

Panel 2 consists of the following category:

- **Category 2A - Hybrid Cloud**

  This category covers platforms and associated infrastructure to manage software workloads including but not limited to development tools, databases, application servers, containers, and virtual machines across on-premises, private and/or public cloud resources including high performance computing.

2.3 Panel 3 - Managed Services

This panel encompasses the management of IT infrastructure and services ensuring optimal performance and security.

The provision of managed services under Panel 3 may include IT infrastructure equipment to meet the procurement outcomes.

In submitting an offer for Panel 3, Respondents are not required to submit a separate offer under Panel 1 **unless** the offered infrastructure and facilities will be offered in isolation to Panel 3.

Panel 3 consists of the following categories:

- **Category 3A - Managed Communications**

  Proactive management, monitoring and troubleshooting of customer-owned or bundled communication platforms to ensure seamless connectivity and communication.

  For the procurement of any supporting software covered by an existing mandatory CUA, the Customer is required to adhere to the Buying Rules of the existing CUA.

- **Category 3B - Managed Infrastructure**

  Comprehensive management of operating systems and the underlying infrastructure, whether located on the customer's premises or provided by the Contractor. This includes maintenance, updates and optimisation for supporting customer workloads.

3. Infrastructure Sourcing Models

The Contractor may offer a range of purchasing options based on the Customer's requirements and the State's current policy direction.

All Customer Contracts are based strictly on a direct contract between the Contractor and the Customer. The Contractor must not require the Customer to enter into any third-party contracts based on either pricing model.

Fully transparent cost model disclosure, regardless of which pricing model is applied, should be provided by the Contractor to the Customer prior to the Commencement Date of the Customer Contract.

The Customer reserves the sole right to accept/decline any pricing model offered by the Contractor.

4. Warranty Requirements

4.1 Infrastructure Warranty

The Contractor must ensure that the Customer receives the full benefit of the standard manufacturer's warranty for all Infrastructure supplied under this CUA. The following minimum requirements apply:

- **Warranty Duration:** At a minimum align with the supplied manufacturer's warranty at Customer's acceptance.
- **Coverage:** All defects in materials, workmanship and performance under normal use.
- **Remedy:** Repair or replacement of defective Infrastructure at no additional cost to the Customer, including parts, labour and associated shipping costs.
- **Contractor's Responsibility:** The Contractor shall facilitate all warranty claims, coordinate repairs and ensure the Customer receives the full benefit of the warranty.

4.2 Non-Warranty Repairs

- **Notification**

  If the Contractor determines a repair is not covered by warranty, the Contractor must provide written notification to the Customer promptly prior to the commencement of any repairs. The notification should include the reason(s) for the non-coverage and an estimated cost for the out-of-warranty repair.

- **Customer Options**

  Without derogating from the rights in clause 20.4 of the GCOC, the Customer may elect to:

  - Authorise the repair at the estimated cost provided by the Contractor; or
  - Decline the repair. If declined, the Contractor may charge a standard non-warranty service call fee.

4.3 Extended Warranties

The Contractor may offer the Customer options for extended warranties beyond the standard manufacturer's coverage. Upon request, the Contractor shall provide the Customer with pricing and terms for extended warranty options. It is at the sole discretion of the Customer to accept/decline extended warranties.

5. Risk-Based Security, Modern Slavery and Resilience

5.1 ICT and Third-Party Risk Assessments

Applicable to Panels 2 and 3 only.

ICT Risk Criteria Tolerance Assessment

To ensure informed decision-making, the Customer may evaluate potential risks associated with proposed ICT Goods and Services, considering their internal risk tolerance and industry best practices. The 'ICT Risk Criteria Tolerance Assessment' will determine whether an 'ICT Risk Assessment Report' and/or 'Security Monitoring and Reporting' is necessary as part of the Customer Contract.

If the Customer determines that the level of risks warrants further investigation, the Customer reserves the right to request the Contractor complete and provide a comprehensive risk assessment as part of its response to the Quote/Order Form. The Contractor must address the potential cybersecurity threats, operational disruptions and other risks relevant to the services offered in line with the following:

- **Data Sensitivity:** Services handling classified, highly confidential or significant amounts of personally identifiable information (PII) necessitate a thorough risk assessment due to the potential impact of a breach.
- **System Criticality:** Mission-critical systems supporting core government functions or services with minimal downtime tolerance require the highest level of scrutiny to ensure operational resilience.
- **Complexity and Scale:** Large-scale deployments spanning multiple sites or impacting numerous users warrants increased attention. Services with intricate integrations into existing systems also fall into this category.
- **Access and Control:** Assessment of the level of access granted to third parties, particularly those handling sensitive data or critical systems. This may necessitate an evaluation of security measures surrounding remote access capabilities.
- **Compliance and Regulations:** Certain services may be subject to specific regulations (privacy, finance and/or cybersecurity) that mandate detailed risk assessments.

The risk assessment should employ recognised risk management frameworks (e.g., NIST Risk Management Framework and ISO 31000 Risk Management) aligned with the Contractor's operations and the Customer's risk profile. The risk assessment report must include at a minimum identified vulnerability, risk mitigation strategies and any noted exceptions.

5.2 Security Monitoring and Reporting

Applicable to Panels 2 and 3 only.

Where identified by the Customer as part of the 'ICT Risk Criteria Tolerance Assessment' the Contractor must implement 24/7 security monitoring covering infrastructure, applications, and data. Tools such as SIEM, threat intelligence feeds and anomaly detection should be used. The Contractor must provide the Customer with visibility into security operations and vulnerability management via an online portal (preferred) or regular reports, to be defined in the Customer Contract. The report should include security performance metrics and KPIs, analysis of threat activity and incident trends, and vulnerability inventories and remediation progress.

The Customer and Contractor must maintain open communication and collaboratively address risk mitigation and incident response activities.

5.3 Vulnerability Management

Applicable to Panels 2 and 3 only.

The Contractor is responsible for implementing continuous vulnerability scanning of both internal and external infrastructure as related to any purchased service or product. Identified vulnerabilities should be addressed promptly by the responsible party based on risk severity. The Contractor must notify the Customer within 24 hours of a confirmed critical vulnerability that could impact the Customer's assets and/or service delivery.

5.4 Incident Response and Recovery

Applicable to Panels 2 and 3 only.

The Contractor must maintain a robust incident response plan and notify the Customer within a maximum of 24 hours (the Customer reserves the right to specify an alternate timeframe based on its risk assessment findings) of detecting any security incidents or potential breaches impacting the Customer's data or systems. The Contractor must also develop and maintain appropriate disaster recovery and business continuity plans that address cyber incidents and other disruptive events to ensure minimal service interruptions.

5.5 Supply Chain Risk Management

Applicable to all panels.

The Contractor must assess and manage supply chain risks relevant to the Goods and Services offered. This includes:

- **Third-Party Risk:** Evaluating the security practices and vulnerabilities of suppliers and subcontractors who handle sensitive data or have access to critical systems.
- **Component Integrity:** Assessing the risks associated with infrastructure and software components, including potential for counterfeit or compromised Goods.
- **Supply Chain Disruptions:** Planning for potential disruptions in the supply chain (e.g. component shortages and vendor outages) and their impact on service delivery.

The Contractor must provide the Customer with visibility into supply chain risk assessments and mitigation strategies if requested by the Customer.

5.6 Modern Slavery Risk Considerations in ICT Procurement

The WA Government is committed to upholding human rights and ensuring its procurement practices do not contribute to modern slavery. This commitment extends to the procurement of Goods and Services, which often involve complex global supply chains with potential risks of forced labour and other human rights abuses.

While specific legislation mirroring the federal *Modern Slavery Act 2018* is not currently in place in WA, the WA Government has a strong commitment to combating modern slavery through existing policies and expects the Contractor to be aligned as such.

ICT Procurement and Modern Slavery Risks

ICT supply chains are particularly vulnerable to modern slavery risks due to its global nature, labour-intensive manufacturing processes and complex sourcing practices. These risks can occur at various stages from raw material extraction to the final assembly and distribution of ICT products.

To ensure responsible and ethical ICT procurement, the Contractor is encouraged to:

- **Prioritise Ethical Sourcing:** Consider its adherence to international labour standards and human rights principles.
- **Conduct Due Diligence:** Consider its potential modern slavery risks, including its operations and those of its subcontractors. Look for transparency in supply chain reporting and commitments to ethical practices.
- **Incorporate Contractual Clauses:** Compliance with relevant modern slavery legislation and/or adhere to internationally recognised labour standards.
- **Monitor Supplier Performance:** Establish ongoing monitoring and reporting mechanisms to ensure its commitment to ethical practices throughout the contract period.

5.7 Responsible Artificial Intelligence Compliance

The Contractor must ensure that all artificial intelligence (AI) technologies and solutions provided under this CUA complies with relevant state and federal legislation on responsible AI usage, including but not limited to ethical considerations, data privacy and security standards.

6. Additional Services

6.1 Buyback and Trade-In Services

6.1.1 Buyback Services

The Contractor **may** offer buyback services for eligible Customer infrastructure with remaining commercial value. Eligibility and pricing will be determined based on market value at the time of assessment. Where the Customer requests buyback services, the Customer has the option to receive the buyback value either as credit

towards the purchase of new or existing Goods and Services from the Contractor or as a direct bank deposit. Buyback quotes must remain valid for a minimum of 30 days. The Customer is under no obligation to accept any buyback offer. Customers with sensitive data have the right to return infrastructure without storage drives to ensure data security.

6.1.2 Trade-In Services

The Contractor **may** offer trade-in services for eligible Customer infrastructure. A Customer seeking to trade in old infrastructure at the time of a new purchase can request quotes from any Contractor, regardless of the original infrastructure provider. Trade-in quotes must be based on market value at the time of assessment and may be applied as account credit towards new or existing Goods and Services or as a direct bank deposit. Quotes remain valid for a minimum of 30 days. The Customer is under no obligation to accept trade-in offers. Customers with sensitive data have the right to trade in infrastructure without storage drives to ensure data protection.

6.1.3 Collection Services

The Contractor **may** supply collection services in connection with buyback and trade-in services.

The Customer reserves the right to make its own arrangements to transport old Infrastructure to the Contractor.

6.1.4 Data Sanitisation

The Contractor **may** offer data sanitisation services to the Customer using buyback or trade-in services.

The Contractor must dispose of Goods in accordance with the WA Government's relevant Disposal Guidelines.

6.1.5 E-Waste Reduction and Landfill Diversion

The WA Government is committed to minimising the environmental impact of e-waste and upholding the *Waste Avoidance and Resource Recovery (E-waste) Regulations 2024*. To achieve this, the Contractor supplying ICT Goods and Services through this CUA must demonstrate its commitment to responsible e-waste management and landfill diversion.

6.2 Subcontracting Arrangements

The Contractor may engage subcontractors for the delivery of Goods and/or Services under this CUA.

The Contract Authority and Customer will only establish a contractual relationship with the Contractor and **not** any subcontractors. The Contractor will therefore be responsible for:

- all Goods and/or Service provided by the subcontractor.
- the management and performance of the subcontractor in accordance with the terms and conditions of the Head Agreement and Customer Contract.
- ensuring the subcontractor provides Goods and/or Services in accordance with the terms and conditions of the Head Agreement and Customer Contract.

- ensuring the subcontractor's application of the Head Agreement price schedule and/or Quote/Order Form.
- ensuring the subcontractor meets the following requirements under CUATIS2024:
    - Insurance; and
    - Risk-based security and resilience outcomes.

The Contractor is to notify the Customer of any subcontracting arrangements prior to the delivery of Goods and/or Services under the Quote/Order Form. The Customer reserves the right to decline the use of a subcontractor and/or request a substitution throughout the term of the Customer Contract. If requested by the Customer, the Contractor is required to remove/replace the subcontractor at no cost to the Customer in accordance with a timeframe that has been agreed to by both parties.

The Contractor is to ensure the ongoing smooth delivery of Goods and/or Services throughout the term of the Customer Contract.

7. Confidentiality

Clause 24.1 of the GCOC is amended to include "the Contractor acknowledges that (f) the Customer may disclose to another State Agency the Customer Contract without the consent of the Contractor".

8. Locational Zoning

Refer to the Department of Local Government, Sport and Cultural Industries website for information on locational zoning in Western Australia.

9. Contract Management Requirements

9.1 Governance

The Contract Authority retains the rights and responsibilities for risk management, performance management, dispute resolution, extensions, variations, reviews and termination issues relating to the Head Agreement.

The Customer retains the rights and responsibilities for risk management, performance management, dispute resolution, extensions, variations, reviews and termination issues relating to the Customer Contract.

9.2 Contractor Profile

The Contractor is required to:

- Complete and return the Contractor Profile template to the Contract Authority within seven days before the Commencement Date of CUATIS2024.
- Inform and provide the Contract Authority with an updated Contractor Profile template within seven days of any changes to its Contractor Profile.

Refer to '**Appendix 2**' for an example of the Contractor Profile Template.

9.3 Reporting Requirements

The Contractor is required to provide the following reports to the Contract Authority:

9.3.1 Sales Report

The Contractor must accurately record all transactions made through the CUATIS2024 Head Agreement and report those transactions to the Contract Authority quarterly in the Sales Report Template, refer to '**Appendix 1**'.

The Contractor is required to submit Sales Report until the expiry of the Customer Contract Term, even after the expiry of the Head Agreement Term.

For the purpose of reporting, a "Quarter" shall mean a period of three months ending on 31 March, 30 June, 30 September and 31 December respectively.

The Contractor must submit the Sales Report in accordance with the reporting requirements to be provided by the Contract Authority upon commencement of the CUA. The Sales Report must be submitted in an electronic format through the Contract Authority's online reporting tool.

The Contract Authority may, at its absolute discretion, amend the content and format of the Sales Report during the Term of the Head Agreement. This may be required from time to time to meet the WA Government's policy commitments and to meet the changing and increasing demand for management information.

9.3.2 Sustainability Reporting

ICT has a significant environmental impact. The WA government is committed to sustainable practices and seeks partners who share this vision.

As part of this partnership the Contractor must provide the Contract Authority, via email, an annual Sustainability Report. Refer to '**Appendix 3**' for further information.

The Sustainability Report is to be provided within 30 calendar days of the anniversary of the CUATIS2024 Commencement Date.

In completing the Sustainability Report, the Contractor is to provide quantifiable data. Where this information cannot be accurately provided, the Contractor is to provide estimated data with an explanation as to how this was derived.

9.3.3 Other Reports

The Contractor may be required to provide Customer-specific and/or ad-hoc reports to the Contract Authority or Customer.

The Contractor will be required to provide the following information on an ad-hoc basis by the Contract Authority:

- Information for a 'Customer Buyers Guide' to be provided at contract formation and as required throughout the Term of the Head Agreement;
- The Contractor must promptly notify the Contract Authority of any changes to the circumstances of the organisation including change of address and contact information or company winding up whether voluntary or by court order; and
- The Contractor must promptly notify the Contract Authority of changes to the nominated Account Manager. The outgoing Account Manager must notify the Contract Authority at least 14 calendar days prior to departure and provide contact information for the incoming Account Manager.

The Customer may specify any ad-hoc reporting requirements in the Quote/Order Form and/or through agreement with the Contractor over the term of the Customer Contract.

9.4 Active CUA presence

The Contractor must maintain an active presence under CUATIS2024, defined as the fulfilment of a minimum of one Customer Contract over the initial term of the Head Agreement.

Prior to any exercise of the extension option under the Head Agreement, the Contract Authority will review all quarterly Sales Reports. Where the Contractor has returned 'nil' total sales since the Commencement Date of the Head Agreement, the Contract Authority has absolute discretion not to exercise the extension option for that Contractor.

9.5 Key Performance Indicators

9.5.1 Head Agreement

The Contractor must meet or exceed the key performance indicator (KPI) targets specified in the table below and report on them to the Contract Authority when requested.

KPI	KPI Target	Frequency
Sales Reports submitted on time and correctly completed.	Sales reports completed correctly and submitted within 30 calendar days post the end date of a relevant sales reporting period. **Note**: "Submitted" means fully loaded with no missing data and without errors into the system, and does not refer to the date in which the report was forwarded to the Contract Authority.	Quarterly
WAIPS Exemption Reporting	Submission of a completed Exemption Report to the Contract Authority on the anniversary of the CUA contract commencement date.	Annually
Sustainability Report	The Contractor must submit a Sustainability Report within 30 calendar days of the anniversary of the CUATIS2024 Commencement Date.	Annually
Currency of Insurance Certificates.	100% of insurance certificates submitted to the Contract Authority no later than 30 calendar days post the expiry of the previous certificate.	Annually
Contractor performance / Customer satisfaction	The Contract Authority will conduct an annual Customer Satisfaction Survey of the Contractor's performance under CUATIS2024. Overall survey results must meet or exceed 90% satisfaction.	Annually

Contractor Profiles	The Contractor must notify the Contract Authority within 14 days of a change to its Contract Manager details.	When required

9.5.2 Customer Contracts

The Customer may establish its own KPIs for each Customer Contract established under this Head Agreement.

Schedule 5 – Quote/Order Form

Schedule 16 - Additional Documents

Appendix 1 - Sales Report Template

The following attachments are drafts only with the final documents to be made available to the Contractor upon CUA commencement:

- CUATIS2024 Sales Report Template.
- CUATIS2024 Reporting Requirements.

The Accountable Authority reserves the right to amend the templates at its sole discretion throughout the term of the CUA.


CUATIS2024 Sales Report Template.xls


CUATIS2024 Reporting Requirem

(To access the template, double click the icon.)

Appendix 2 - Contractor Profile Template

The following '**Contractor Profile**' is a draft template only.

The final template will be made available to the Contractor prior to the Commencement Date of CUATIS2024.

The Accountable Authority reserves the right to amend the template at its sole discretion throughout the term of the CUA.

CUATIS2024 CONTRACTOR PROFILE	
Instructions: The Contractor is complete and return the Contractor Profile template to the Contract Authority.	
Contractor Specific Reporting	
Company Name	
ACN	
ABN	
Website	
Contact Information	
Full Name	
Title	
Phone	
Email	
Business Hours	
Business Days	
Business Hours (Western Australia)	
Orders Via:	
Background	
Industry Partners/Affiliations	
Date of Last Update	

Appendix 3 - Sustainability Report Template

The following '**Sustainability Report**' is a draft template only.

The final template will be available upon CUA Commencement Date.

The Contract Authority reserves the right to amend the template at its sole discretion throughout the term of the CUA.

CUATIS2024 SUSTAINABILITY REPORT

Instructions:

- The Contractor is to complete and return this Sustainability Report to the Contract Authority within 30 calendar days of CUATIS2024 Commencement Date anniversary.
- The Contractor is to provide quantifiable data. Where this information cannot be accurately provided, the Contractor is to provide estimated data with an explanation as to how this was derived.
- Panel Applicable Reporting:
  - The Contractor is to provide information specific to the Goods and Services under the panel(s) for which it has been appointed to.
  - The Contractor is to state 'Not Applicable', where a field is not relevant to the types of Goods and Services provided by the Contractor in relation to CUATIS2024.

Contractor Specific Reporting

List the sustainability policies, frameworks and initiatives that your company currently adhere to. Examples may include alignment to such frameworks as ISO 14001, EPEAT or policies targeted at sustainability outcomes.

[Response]

Panel Applicable Reporting

Equipment Energy Efficiency

Equipment Type (high-level categorisation eg. server, desktops, etc)	Average Energy Consumption (kWh/year)	Energy Star Compliance [Yes/No]
[add additional rows as required]		

Cloud Services Energy Efficiency

Average data centre power usage effectiveness (PUE):	
Percentage of renewable energy used:	

Cloud Sustainability

Initiatives: Briefly outline any waste reduction or circularity programs by cloud providers.

[Response]
Sustainable Materials
Recycled Content: Estimated percentage in major components.
[Response]
Extended Lifespan
Average Lifespan: Expected years of use for major equipment types (high-level categorisation eg. server, desktops, etc).
[Response]
Vendor Support: Duration of security updates/maintenance offered.
[Response]
End-of-Life Management
Take-back Programs: Describe vendor-provided options and certifications (e-Stewards, R2, etc.).
[Response]
Recycling/Reuse: Estimated percentage of equipment recycled or reused.
[Response]
E-Waste Reduction and Landfill Diversion: Estimated percentage of EOL products that have ended in a landfill.
[Response]