YYYY

Source Acknowledgement

This IPWEA Model Asset Tracking & Monitoring Specification is a free publication, available in editable Word format to allow for ease of use of the content. Updated versions will be issued in future by IPWEA, as and when required on IPWEA’s [AT&M Website](https://www.ipwea.org/home). When using extracts or adapting key sections of this document for your own use, users should acknowledge IPWEA as the source of this material (e.g., “Based on IPWEA’s Model Asset Tracking & Monitoring Specification X.X”).

Disclaimer

Although the information in this publication is believed to be correct at the time of publishing, the Institute of Public Works Engineering Australasia (IPWEA), and its agents, contractors, directors, employees, subcontractors and officers, do not accept any contractual, tortious or other form of liability (including in negligence) arising from the information contained herein, to the extent permitted by law. The information included in this publication is intended as a general guide only and is not tailored to your needs and circumstances. People using the information contained herein should apply, and rely upon, their own skills and judgement to the particular installations they are considering and seek appropriate professional engineering and financial advice as needed. This document is not a substitute for specialist, professional advice.

Document Information

This work is licensed under the Creative Commons Attribution 3.0 Australia Licence. To view a copy of this license, visit the [creative commons website](https://creativecommons.org/licenses/by/3.0/au/). The Institute of Public Works Engineering Australasia (IPWEA) through its Emerging Technology Program asserts the right to be recognised as author of the original material in the following manner:

Creative Commons Licensing - By Attribution

© IPWEA (AT&M Program) 2021

Acknowledgements

IPWEA acknowledges the intellectual and in-kind support of our corporate partners and members in delivering the Asset Tracking & Monitoring Program. The Program provides education and resources which assist our 4,000+ members make informed decisions about Asset Tracking & Monitoring solutions and related deployments to enhance asset management. In addition to providing education and resources in this area, IPWEA works jointly with our partners in advocating for measures that increase the adoption of emerging technologies in a rapidly changing field.

IPWEA specifically thanks the following organisations, which encompass both communications network providers and, device and service providers, for their contributions to the development of IPWEA’s Asset Tracking & Monitoring Program. They have variously engaged in discussions about the development of the program, participated in surveys, commented on draft documents and/or provided contributions of material for key documents and training materials.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **Actility** | **Intelematics** | **Optus** | | **Azentro** | **IntelliTrac** | **Pivotel** | | **Cody Corporation** | **Lacuna Space** | **Smartrak** | | **Digital Matter** | **M2M Connectivity** | **Teletrac Navman** | | **Eroad** |  | **Telstra** | | **Fleet Complete** |  | **Thinxtra** | | **Fleet Space Technologies** | **Movus / FitMachine** | **Netstar** | |  |
|  |  |

Contents

Acknowledgements 3

1 | Introduction………………………………………………………………………………………………………………… 5

2 | Information for Tenderers 8

3 | Overall System Description 11

4 | Central Management System (CMS) Specification 13

5 | Backhaul Communication Network Specification 17

6 | Communication Network Specification 18

7 | Asset Tracking & Monitoring Device Specification 22

8 | System Installation and Commissioning Specification 26

9 | System Maintenance Specification 30

10 | Appendix A: Terms and Definitions 32

11 | Appendix B: Standards References 35

12 | Appendix C: Returnable Schedules 36

**1| Introduction**

As the next development in our Emerging Technologies workstream, IPWEA has developed this document as a model specification for those wishing to procure and deploying asset tracking and monitoring technologies. It is accompanied by a guide to the business case for asset tracking and monitoring technologies to assist public buyers, vendors, contractors, funders and advisors to navigate the process for considering investment in asset tracking and monitoring systems, and to efficiently and economically engage in procurement of these systems and bring tendering efficiency and certainty to the market.

The need for this document and training about asset tracking and monitoring was identified in a 2020 review by IPWEA of the status of emerging technologies that had both demonstrably reached some commercial maturity and could provide material benefit its members.

As with IPWEA’s experience with its first Emerging Technology Program on Street Lighting & Smart Controls, stakeholders who were engaged in the development of this program noted fragmented approaches to asset tracking and monitoring procurement and deployment. While this pattern is typical of many new technology markets it suggests sub-optimal outcomes at a project-specific level and at a broader national level.

1.1 Purpose and Target Audience

This document is targeted at procurement and technical staff. It is intended to facilitate the acceleration of the adoption of asset tracking and monitoring. It seeks to do this by assisting buyers, vendors, contractors, funders and advisors to efficiently and economically engage in procurement of tracking and monitoring of assets.

The objective of this model specification is to provide an informative, structured template that is focused on the technical aspects for local governments, main road authorities, state government agencies and other entities to help them prepare their own customised specifications within a structured procurement either as a Request for Proposal (RFP), a Request for Quote (RFQ), or as a Request for Tender (RFT).

This Model Specification provides outcome-based guidance which has been harmonised with both international and local standards (where currently relevant) and specification requirements for asset tracking. It seeks to accommodate and encourage innovation within the bounds of compliance with prevailing design, safety and performance standards and specifications. Once customised to their own circumstances, a procuring entity can use the resulting specification to select a suitable asset tracking and monitoring system with confidence in the outcome.

1.2 How does ‘Model Asset Tracking & Monitoring Specification’ fit within the IPWEA Emerging Technologies Asset Tracking and Monitoring workstream?

The IPWEA Asset Tracking & Monitoring workstream is designed to help our members to leverage appropriate digital technologies to manage assets more effectively. This in turn helps them develop their skills in applying digital technology to the asset management task and provides benefits in relation to the performance of the assets themselves as well as the community services they underpin.

Diagram

Description automatically generated

The Asset Tracking and Monitoring workstream comprises the following elements:

* The Business Case for Asset Tracking & Monitoring
* Model Specification for Asset Tracking & Monitoring *(this document)*
* Online Learning Program (registration fee required) providing participants with the opportunity to:

1. Increase their knowledge and understanding of Asset Tracking and Monitoring technologies and use cases;
2. Access to tools and guidance materials to build a business case using inputs from their own organisation;
3. Earn certification via a digital badge in Asset Tracking & Monitoring technology and its application to asset management;
4. Access a Business Case Outline including an appendix providing a detailed survey of benefits of asset tracking and monitoring technology which will help members to develop business cases for applying asset tracking and monitoring technology in their own organisations; and
5. Access an Excel-based ‘Returnable Schedule’ to assist in a procurement process.

1.3 Document Guidance

This model specification is a multi-choice general guidance document targeted to assist procurement organisations to develop their own customised specification tailored to the exact needs and circumstances of the applicable region and organisation. The selectable content is divided into three categories, plus guidance notes (to be deleted after customisation):

1. Suggested text for inclusion in the tender document by **all** users is presented as mandatory requirements identified in normal black text;
2. Alternative options considered suitable for **some** users, is presented as an optional requirement to be chosen by the purchasing organisation are shown in Bold Green Italic; and
3. Where text is used to instruct user action, this is identified by bold blue coloured and/or by square brackets [ ].

**Note:** Explanatory text to guide user customisation is in burgundy coloured text boxes (as per this example) which is intended to be deleted after Users have finished compiling their own Customised Specification.

This Model Asset Tracking and Monitoring Specification document has been compiled and formatted in Microsoft Word 2016. Formatting is very important to facilitate comprehension of a necessarily complex and comprehensive subject so we recommend that Microsoft Word 2016 or later is used.

2 | Information for Tenderers

**Note:** This section makes recommendations about information to be provided to Vendors about the procurement timetable, the project being tendered, the required responses and how bids will be evaluated. The contents below are normally included in the ‘Information for Tenderers’ section of request for tender documentation and are included here for guidance only.

When Users are compiling a Customised Specification based on this Model Specification care is needed with selection options to only request quantities and levels of functionality for data collection and reporting to cater for tangible and identified User needs. Requesting additional or higher levels of functionality without identified User need (now or in future) may unnecessarily increase system complexity and cost. This has to be carefully weighed against the risk of insufficient future-proofing, as it would be a false economy if capacity to accommodate realistic future needs was not factored into procurement documents.

**2.1 Procurement Process Timetable**

The indicative timetable for this procurement process is as follows:

**Table 1 Procurement Process Timetable**

**Note:** It is strongly suggested that a clear procurement process timetable as per the approach above is included as an introductory part of any Asset Tracking and Monitoring tender. This serves to both increase tenderer confidence that they are participating in a robust process and compels suppliers, in later sections of this tender, to identify whether they can meet delivery timetables.

|  |  |
| --- | --- |
| **STAGE** | DATE |
| Tender release | DATE |
| Tender close | DATE & TIME |
| Short-listing notification | DATE |
| Short-listed candidates’ deadline for response with additional information requested | DATE  *Suggested as 1-2 weeks from short-listing notification* |
| Tender award date | DATE |
| Initial Control System delivery date | DATE  *Required delivery date of initial order. Typical delivery lead times are 12-16 weeks for most suppliers.* |
| Targeted end date for the project | DATE |

**2.2** **Project Description**

This tender specification is for an Asset Tracking and Monitoring System for**:** [Project Name] Covering: [Asset Tracking & Monitoring Devices] with a supporting Central Management System and Communications Network including backhaul requirements.

[Insert concise 50-100-word project description summarising the geographic area, asset types encompassed in the project and the overall functionality desired.]

This tender specification does not represent a guarantee that procurement in the volume indicated above will eventuate or will actually be required. This procurement process is undertaken in good faith, but with no explicit or implicit obligation.

2.3 Tender Response

In responding to this tender, tenderers need to provide the following completed schedules:

1. **Schedule A - Vendor Information & Referees**
2. **Schedule B - Asset Tracking & Monitoring Technical Specification Compliance Response for:**
   1. **Central Management System**
   2. **Communication Networks**
   3. **Asset Tracking & Monitoring Devices**
   4. **Installation & Maintenance**
3. **Schedule C - Pricing**
4. Schedule D - Warranty Information
5. Schedule E - Vendor or Project Performance Guarantees, Insurances, Bonds (Optional)
6. Schedule F - Tenderer Statutory Declaration (Optional)

For the purpose of evaluating tenders, details of both the Tenderer and the Manufacturer (if not the same company) need to be tabled separately as shown below.

2.4 Tenderer Assessment Criteria

The criteria below are provided for information only and shows the list of typical assessment criteria that could be used by the User for the evaluation of the suitability of the tender offer and the Vendor.

The weighting of these criteria and the results of the tender assessment would typically remain confidential.

**Mandatory Assessment Criteria**

1. Financial and commercial trading integrity
2. Ability of the tenderer to attend site(s) as and when requested
3. Demonstrated capacity to fulfil the work health & safety requirements
4. Adherence to environmental management, sustainability and procurement guidelines
5. A minimum of [X] Vendor referees from appropriate reference projects provided of the same or larger size than this project

Selective Assessment Criteria

1. Performance attributes and functionality as assessed against the project specification
2. Manufacturer capacity (including qualifications and experience of local technical staff), resources and track record
3. Distributor capacity (including qualifications and experience of local technical staff) and resources (if applicable)
4. Total value represented, considering:
5. Net Present Value (NPV) of the tender proposal over the asset lifetime, including initial tender price, operating fees and maintenance requirements; and
6. Strength of warranty and any other performance guarantees offered

3 | Overall System Description

3.1 Information for Tenderers

Asset Tracking and Monitoring systems can be described, in overview, as a set of three interacting Component levels:

1. **Central Management System,** with Software running on a central computer (cloud or on-premise server) that delivers web user interfaces on desktop and mobile devices;
2. **Network Communications Infrastructure,** is sub-divided into *Backhaul Communication Networks and Communication Networks* with Gateways widely distributed across a geographic region; and
3. **Asset Tracking & Monitoring Devices**, being those devices in the field tracking location and other parameters.

All three elements function together to respectively gather and create, transmit and relay, and display and analyse data to provide the region, city, town and/or asset maintenance company with operational functionality and information to improve the ability to locate and track assets and efficiently operate them.

3.2 Modular Procurement

**Note:** Within each of these three components there are various local and international Vendors and Manufacturers who supply the Components that comprise the whole system. While most systems are sold as integrated sets of Components, in some cases, Vendors and Manufacturers can provide individual system Components. In this “Modular” approach to procurement, Component Compatibility and Interoperability are critical and need to be managed by the procurement process to ensure a smoothly operating system.

There are technical, financial, commercial and operational advantages and disadvantages that should be considered by the User before including any requirements for Modular Procurement. The Modular Procurement approach allows for commercial competition among suppliers in each of the levels of the system. This has the potential to apply strong and ongoing commercial pressure on Vendors but the need for Interoperability at different levels could create additional procurement and management tasks and may restrict application freedom and/or innovation.

3.3 Turnkey Procurement

**Note:** In most cases, Vendors and Manufacturers provide a complete an end-to-end “Turnkey” package, and in this case, the responsibility for Compatibility and Interoperability of the three levels is fully covered by the single Vendor or Manufacturer.

There are technical, financial, commercial and operational advantages and disadvantages that should be considered by the User in deciding whether it is seeking a Turnkey solution. The Turnkey Procurement approach insulates the User from responsibility for Component and Module Compatibility and Interoperability risks, but there could be risks of single supplier lock-in that may not be in long term interests of the User.

3.4 System Capabilities

To achieve the goals identified above, the main features of an asset tracking and monitoring system are expected to cover the general capabilities listed below:

* 1. Install, commission and configure Gateways (or other network equipment where relevant) and Asset Tracking & Monitoring Devices easily, at low cost and without error;
  2. Collect and aggregate asset location or condition data with high accuracy for the User;
  3. Identify Asset Tracking & Monitoring Device failures and anomalies;
  4. Monitor operational hours and condition of devices for predictive maintenance purposes and for warranty enforcement;
  5. Collect data from Asset Tracking & Monitoring Devices and supply to the User or to third party software such as Asset Management Systems (AMS) or Geographical Information Systems (GIS);
  6. Provide interfaces and/or mechanisms to interact with a variety of sensors and platforms to provide the city with information to help improve service, comfort and safety in the city; and
  7. Be scalable to handle a growing volume of data and number of devices to accommodate growth.

4 | Central Management System (CMS) Specification

The Central Management System (CMS) is a computer environment that provides all shared System services and consolidates and stores all System data. A User may specify a Central Management System as part of a complete integrated Turnkey System, or as a Modular Component to be integrated with the other Components available.

4.1 Physical Features and Requirements

* 1. The System shall use a Central Management System that is hosted by:

Select ONE or more of the following options:

1. The User or a User specified Third Party
2. The Vendor. Hosting fees to be incorporated in first cost
3. The Vendor. Hosting fees to be separately identified as a recurring cost
4. The Vendor or 3rd party host [Insert “in Australia” or “in New Zealand”, if data sovereignty is a factor]
5. Other - Vendor proposed option
   1. The Vendor shall provide a description of the overall architecture, availability, reliability, redundancy, disaster recovery, scalability and security approach of the System irrespective of the hosting location and arrangements.
   2. The Vendor shall provide sample screen images depicting the following features and functions:
6. **Commissioning:** Installation and Configuration process of a new tracking devices
7. **Inventory:** Tracking device location with the ability to select on maps (e.g. using a lasso tool), description with multiple attributes (including identifier, type, model, supplier, address (where asset location is fixed), etc., ability to colour code assets and obtain a street level view of asset location – e.g. Google Street View
8. **Schedules/Calendars:** Defining schedules, assigning schedules to days and applying these calendars to groups of Asset Tracking & Monitoring Devices
9. **Failure analysis**: Display Asset Tracking & Monitoring Device failures on maps for the whole coverage area (very high zoom level) and for a particular geographical section (low zoom level, e.g. a block) on road maps as well as satellite map, from several map providers
10. **Real time view:** Asset Tracking & Monitoring Device and Gateway status (i.e. online, online reporting error, offline, failures),
11. **Data analytics:** generally displaying, for example, the history of any collected data on any Asset Tracking & Monitoring Device
    1. The CMS shall be accessible to authorised individual users only by unique user identifier and password loss to prevent unauthorised access or control of the system [The User may wish to consider stipulating automation of user authentication through integration with systems like an Active Directory, depending on their organisation’s policies].
    2. The CMS shall be accessible to authorised third party applications through a secure API.
    3. The CMS shall be capable of restricting user access to specific functions. These functions shall include the following:
12. Creating and managing users and groups
13. Installing/Commissioning/Removing/Replacing one or more Asset Tracking & Monitoring Device
14. Configuring one or more Asset Tracking & Monitoring Device
15. Collecting, displaying and analysing Asset Tracking & Monitoring Device failures on maps and reports
16. Controlling and monitoring one or more Asset Tracking & Monitoring Device in real time
17. Report generation for failure and other purposes
18. Custom report generation
    1. The CMS shall be accessible through desktop [User may wish to specify operating system] and handheld mobile devices (eg, smart phone and/or tablet) in a format designed to accommodate the size and user interface of the mobile device.
    2. All asset data shall be stored on the CMS. It shall be capable of storing the following asset and warranty information for all tracking devices:
19. Asset Tracking & Monitoring Device number
20. Asset Tracking & Monitoring Device type
21. Asset Tracking & Monitoring Device unique identifier on the network
22. Make, model and firmware version
23. GPS location (which may change in real time)
24. Asset Tracking & Monitoring Device grouping
25. Other information [Required information description]
    1. The Central Management System shall be capable of retrieving and storing all remote monitoring data.
    2. Unless otherwise specifically agreed, ownership of all data collected from and subsequently produced in the CMS will rest with the User.
    3. Optional: The Central Management System shall integrate with the requirements of existing User systems (e.g. Council or other public infrastructure owner/manager):
26. Asset Management Systems (AMS) - [Specify particular systems including data formats]
27. Works order and contract control systems - [Specify particular systems including data formats]
28. User dashboards and citizen fault reporting systems - [Specify particular systems including data formats]
29. Other systems (e.g., data lakes)

4.2 Logical Features and Requirements

The Central Management System shall:

* 1. Ensure secure communication between itself and all Asset Tracking & Monitoring Devices by enabling security features inherent to the underlying communications protocols;
  2. Be capable of detecting communication failures between Gateways and Asset Tracking & Monitoring Devices and the Central Management System and generate user alarms accordingly;
  3. Be capable of updating Asset Tracking & Monitoring Device firmware, auditing Asset Tracking & Monitoring Device firmware version and identifying Asset Tracking & Monitoring Device firmware corruption/hacking remotely and centrally, by group of Asset Tracking & Monitoring Devices;
  4. Be capable of remotely monitoring Communication Network and Asset Tracking & Monitoring Device performance, in order to identify and report any exception to normal operation;
  5. Have open interfaces (API’s) for integration with other software from other vendors (e. g., Asset Management Systems) in the data formats required;
  6. Radio Frequency Communications Compliance: The system shall comply with all relevant regulations for Radio Frequency Communications as they apply to the particular system used in a country and/or region (e.g., AS/NZS CISPR 15 and AS/NZS 4268); and
  7. System Security: The system shall be manufactured, installed and commissioned so that appropriate levels of best practice system security are achieved [Insert specific minimum security requirements if applicable to the organisation].

4.3 Functional Features and Requirements

The Central Management System shall be capable of:

* 1. Commissioning new Asset Tracking & Monitoring Devices and sending configuration parameters to them
  2. Collecting and storing the following online Asset Tracking & Monitoring Devices parameters:

1. Asset Tracking & Monitoring Device status (Online, Offline, Warnings, Errors) each time it changes
2. GPS location (via an integral sensor in each Asset Tracking & Monitoring Device)
   1. Collecting events or failures detected by the Asset Tracking & Monitoring Device.
   2. Programming the Reporting Frequency of online Asset Tracking & Monitoring Device parameters for all Asset Tracking & Monitoring Devices.
   3. Defining Asset Tracking & Monitoring Device groups to apply programs or calendars (e.g. via lasso tool on map)
   4. The Central Management System shall be provided with standard reports and allow the User to create custom reports (including trend graphing), on-demand (displayed on screen) or scheduled (sent by email), for any group of Asset Tracking & Monitoring Devices defined by a filter or by a geographical area, to analyse (at installation or in the future):
3. **Assets,** e.g. list the identifiers, address (where fixed), number of operating hour and any other attributes selected by the User
4. **Alarms or failures**, e.g. list the identifier, the GPS position, the Manufacturer and Model of Asset Tracking & Monitoring Device Failure and/or Communication Loss
   1. The Central Management System shall be capable of generating configurable alarms and sending them to identified Users by email or text message (SMS) or by Application Programming Interface (API) in case of:
5. An event (e.g. Asset Tracking & Monitoring Device Failure event) is received by the CMS from an Asset Tracking & Monitoring Device
6. A number of events (e.g. Communication Loss) are received from more than [Number] Asset Tracking & Monitoring Devices all located within a certain geographical area
7. More than [Percentage] % of Asset Tracking & Monitoring Devices have failed within a group

4.4 Interoperability - Central Management Systems

* 1. Optional: The CMS shall be compliant with [Insert one or more Options if an Interoperability Standard or protocol is to be met]

5 | Backhaul Communication Network Specification

The suggested technical specifications for a Backhaul Communication Network to be installed as part of the System are described in this section.

5.1 Backhaul Specification

**Note:** A Backhaul Communication Network links the Central Management System to the Gateways and the Communications Network links the Gateways to the Devices. A User does not usually specify a Backhaul Communication Network as this is usually selected by the Manufacturer or Vendor unless the User has negotiated a special arrangement with a Backhaul provider as part of other services, such as telecommunications (as described in Option A below).

Select one or more, as desired:

* 1. Optional***:*** The Backhaul Communication Network shall be provided by the User. It shall provide a minimum of secured encrypted IPv4/IPv6 communication channels (if multiple port – list all ports required between the Communication Network (e.g. Gateways) and the Central Management System). It shall be:

Select ONE or MORE, as desired:

1. One or more fibre optic networks that are operated by [Operator(s)] and to which the Central Management System shall connect; and/or
2. One or more mobile phone networks from [Operator(s)] with whom the User has negotiated a global communication contract.

Other[Specify particular systems]

* 1. Optional: The System shall use a Backhaul Communication Network specified by the Vendor.

6 | Communication Network Specification

The suggested technical specifications for a Communication Network to be installed or used as part of the System are described in this section.

6.1 Physical Features and Requirements

* 1. Communication Network components shall be capable of normal operation over an ambient temperature range of:

Select ONE of the following options:

1. -15 degrees C to +60 degrees C (hot environment); or
2. -25 degrees C to +55 degrees C (medium environment); or
3. -40 degrees C to +40 degrees C (cold environment).
   1. Communication Network component enclosures installed shall be rated to a minimum of IP65.

**Note:** Some Communication Network IT Components may require ventilation. The Ingress Protection (IP) requirement should be waived in such circumstances and a Vendor statement of suitability for the outdoor environment should be requested.

* 1. Communication Network components shall operate at 230V nominal (+10/-6%).

6.2 Logical Features and Requirements

The Communication Network shall:

1. Use a physical layer communication protocol or standard (such as IEEE 802.15.4g for wireless mesh networks or Global System for Mobile communications (GSM) standards for mobile networks or LTE for Narrow Band IoT networks).
2. Be capable of connecting to Central Management Systems using open, standards-based networking technologies (such as http, SMTP, SNMP, COAP, TCP, UDP or FTP).
3. Ensure that all data communications over the Communication Network be secured using a standards-based security protocol (e.g. TLS, DTLS, IPsec).
4. Allow only authenticated and authorised access to network services by a Central Management System, Gateway or Asset Tracking & Monitoring Device.
5. Be capable of maintaining accurate time either on its own or by synchronising with a remote service.
6. Provide a detailed view of the network and its topology, including all connected Gateways, Asset Tracking & Monitoring Devices, links, and ports.
7. Provide a real-time and historical detailed view of network performance, including available bandwidth, Gateways and Asset Tracking & Monitoring Device location, accessibility, signal strength, round-trip times, path costs, and packet delivery success/failure.
8. Provide a configuration management tool to view and remotely apply changes, updates, and patches to operating systems and applications on any single or a group of Communication Network components, including Gateways and Asset Tracking & Monitoring Devices.
9. Enable the operating system and applications to update all connected and active Gateways and Asset Tracking & Monitoring Devices within less than:

Select an Option:

1. 1 hour
2. 1 day
3. [Other User-specified duration]
4. Be capable of logging time-stamped activity. The logging level shall be configurable. Any write and execute operations completed by an Asset Tracking & Monitoring Device or Gateway shall be recorded together with the source IP address.
5. Provide basic firewall capabilities, including filtering by port, protocol, source IP address, and destination IP address.
6. Provide basic routing capabilities. The Gateway shall act as a multi-band Gateway, between the Backhaul Network and the Field Network.
7. Be capable of communicating using Internet Protocol version 4 or 6 (IPv4/IPv6). Every device must be addressable via an assigned IPv4/IPv6 address.
8. Electrical Safety Compliance: Gateways, Asset Tracking & Monitoring Devices and the Network system shall comply with all relevant regulations for electrical safety as they apply to the particular system used in the region (eg AS/NZS 3820).
9. Radio Frequency Communications Compliance: Gateways, Asset Tracking & Monitoring Devices and the Network system shall comply with all relevant regulations for Radio Frequency Communications as they apply to the particular system used in a country and/or region (eg AS/NZS CISPR 15 and AS/CA S2042).
10. System Security: The system shall be manufactured, installed and commissioned so that appropriate levels of best practice system security are achieved. [Insert specific minimum security requirements if applicable to the organisation]
11. The Communication Network and any connected device or system shall:

Select from the following options:

1. Optional: Be able to authenticate each other by a standard-based mechanism (e.g. X.509 certificates or pre-shared keys).
2. Optional: Be able to authorise each other by a standard-based mechanism (e.g. X.509 certificates).
3. Optional: Be kept confidential using a standard-based encryption algorithm (e.g. AES-128 or AES-256).
4. Optional: Be checked for integrity using a standard-based algorithm (e.g. keyed HMAC with SHA-256).

6.3 Functional Features and Requirements

The Communication Network shall be capable of:

* 1. Two-way communication.
  2. Automatically supporting failover to alternate routes.
  3. Automatic retries while attempting to deliver messages/packets.
  4. Generating asynchronous alerts and routing both Communication Network and other device alerts to the Central Management System.
  5. Addressing of groups of Gateways and Asset Tracking & Monitoring Devices for bulk messages including remote firmware upgrades and configuration changes.
  6. Allowing near real-time communication and receive and execute any manual override commands (sent by the User from the Central Management System) within less than:

Select ONE Option:

1. 1 minute
2. 1 hour
3. [Other User-specified duration]
   1. Optional: Maintaining Network Availability for

Select ONE Option:

1. 95%

2. 99%

3. [Other User-specified percentage availability]

of active and functional Gateways and Asset Tracking & Monitoring Devices at least

Select ONE Option:

1. 95%

2. 99%

3. [Other User-specified percentage availability]

of the time (other than for third party causes eg power cuts). The Vendor shall provide the tools to monitor the performance of such a Service Level Agreement.

6.4 Interoperability

1. Optional: The Communication Network shall be Interoperable with the following Asset Tracking & Monitoring Devices and Gateways [Insert descriptions of any existing devices or gateways that the User wishes to integrate].

6.5 Rated Life and Reliability

1. The Rated Life of all Communication Network components at an ambient temperature of 25 degrees Celsius shall be greater than:

Select ONE of the following options:

1. 10 years
2. 15 years
3. 20 years

**Note:** There is a procurement balance to be struck between the Rated Life of a Device and the Economic Life of the Device. It may be an expensive choice for a User to specify a long-rated life requirement for Gateways or Devices if the Devices could be replaced at an earlier point for other reasons, including to capture economic or functional advantages of future new technology updates. Note that the Rated Life is not the same as the Warranty term.

1. The Vendor shall provide the predicted reliability of Communication Network components (Gateways and Routers) as calculated by Mean Time between Failures (MTBF) according to Telcordia SR-332.

6.6 Networked Standby Mode Power Disclosure

* 1. The Vendor shall disclose the Networked Standby Mode Power consumption (W) for Gateways and Routers. Networked Standby Mode Power is power consumption when connected to a supply voltage with all functions off, except for support functions using a trigger from a network. This is in accord with the forthcoming AS/NZS 63103 based on IEC 63103.

7 | Asset Tracking & Monitoring Device Specification

Asset Tracking & Monitoring Devices are networked Components (hardware and embedded software) installed in the field that, following installation and commissioning, function together to locate, remotely monitor (and sometimes control) assets.

The suggested technical specifications for Asset Tracking & Monitoring Devices to be installed as part of the System are described in this section.

7.1 Asset Tracking & Monitoring Device Information

* 1. The Vendor shall supply the following Asset Tracking & Monitoring Device information:

1. Brand(s)
2. Type(s)
3. Model Number(s)

7.2 Physical Features and Requirements

A Asset Tracking & Monitoring Devices shall be capable of operation over an ambient temperature range of:

Select ONE of the following options:

1. -15 degrees C to +60 degrees C (hot environment)

2. -25 degrees C to +55 degrees C (medium environment)

3. -40 degrees C to +40 degrees C (cold environment)

* 1. Asset Tracking & Monitoring Devices installed external or remote to assets shall be housed in enclosures rated to a minimum of IP65
  2. Optional: During Offline Operation Asset Tracking & Monitoring Devices shall be capable of storing measurements of all Offline Parameters at the specified frequency for a storing period of greater than:

Select ONE Option:

1. 2 Days
2. 3 Days
3. 7 days
4. [Other User-specified duration]

**Note:** Requiring longer storing periods may increase unit cost.

* 1. Optional: If an Asset Tracking & Monitoring Device loses communication service due to an unforeseen event (eg loss of power), the Asset Tracking & Monitoring Device shall:

1. Be capable of communicating the loss of communication to the Central Management System (eg last gasp capability); and
2. Be capable of communicating any previously unsent Asset Tracking & Monitoring Device stored data to the Central Management System.

**Note:** This feature requires the integration of an additional battery or capacitor, which may increase unit cost.

* 1. Optional: Be capable of self-commissioning without user input.
  2. Method of attachment or integration[Specify particular method]

7.3 Logical Features and Requirements

1. During Online Operation, Asset Tracking & Monitoring Devices shall be capable of Reporting the following parameters:
2. Asset Tracking & Monitoring Device status (Online time, Offline time, Warning or Error codes)
3. GPS location (via integral sensor)
4. Additional parameters to be reported on are:
   1. **[Insert additional functional parameters to be reported on specific to the use case (eg fuel efficiency, engine temperature, operating hours, acceleration and speed for fleet telematics systems; temperature (and other climatic parameters), vibration, tilt, noise, fluid levels) for other types of asset tracking & monitoring sensors]**
   2. **[Insert additional rows as required]**

**Note:** Care is needed in specification and procurement to only request data collection and reporting functionality to cater for identified needs. Requesting additional functionality without an identified need or use may unnecessarily increase cost and complexity.

1. During Online Operation, Asset Tracking & Monitoring Devices shall be capable of reporting all parameters for all Asset Tracking & Monitoring Devices when these values change by more than **[Insert % change]** from the expected level:

Select ONE Option:

1. 5%

2. 10%

3. [Other User-specified duration]

1. And at a minimum Reporting Frequency of once per day **[or other interval as specified].**

**Note:** The Reporting Frequency performance will depend on the network size. Larger networks will generate longer time delays. Care is needed in specification and procurement to only request data collecting and reporting functionality/frequency to cater for identified needs. Requesting additional functionality/frequency without an identified need or use may unnecessarily increase cost and complexity and, may greatly shorten battery life for battery powered devices.

1. During Online Operation, Asset Tracking & Monitoring Devices shall be capable of answering any request for real-time reading of all Asset Tracking & Monitoring Device parameters for a single Asset Tracking & Monitoring Device at a maximum of:

Select ONE Option

1. 1 minute

2. 5 minutes

3. [Other User-specified duration]

**Note:** This specification establishes the maximum continuous update time during demonstration or troubleshooting, where a single Device is being operated or evaluated. For large networks or some network architectures, specifying a shorter time may (in some cases) result in higher cost.

1. Asset Tracking & Monitoring Devices shall execute any single command received from the Communication Network in less than:

Select ONE option:

1. 1 minute

2. 5 minutes

3. [Other User-specified duration]

**Note:** This specification establishes the maximum time for a single command to spread through the Communication Network and be received and executed by a Device.

1. Asset Tracking & Monitoring Devices shall automatically Report all data stored during Offline Operation, when Online Operation is restored.
2. Asset Tracking & Monitoring Devices shall include a method to verify the integrity of firmware to be executed, to prevent unauthorised or maliciously modified software from running on the Asset Tracking & Monitoring Device. This could, for example, use a secure Boot Loader scheme.
3. Radio Frequency Communications Compliance: The system shall comply with all relevant regulations for Radio Frequency Communications as they apply to the particular system used in [a country and/or region].
4. System Security: The system shall be manufactured, installed and commissioned so that appropriate levels of best practice system security are achieved [Insert specific minimum security requirements if applicable to the organisation].

7.4 Functional Features and Requirements

Asset Tracking & Monitoring Devices shall be capable of:

1. Optional: Calendar Control, from a set of Control Programs assigned to days of the year:
2. On a daily recurring basis;
3. Or on a weekday recurring basis;
4. Or on a weekend recurring basis;
5. Or on a special date/time period for special circumstances.
6. Optional: Monitoring and reporting:
7. Remaining battery life
8. Low battery alert

7.5 Interoperability

The system shall provide interoperability at various levels:

* 1. Optional: Between Central Management System and Communication Network the Central Management System shall be certified as compliant with [Insert one or more Options if an Interoperability Standard or protocol is to be met]
  2. Optional: Between Communication Network and Asset Tracking & Monitoring Devices the Communication Network shall accept, communicate with and interact with the following Asset Tracking & Monitoring Devices from independent Vendors [Insert products and Vendors].

**Note:** If interoperability on a network level is required to be achieved on a proprietary network, Vendors should be contractually obligated to licence their network technology to other vendors to avoid single supplier lock-in.

7.6 Rated Life & Reliability

1. The Rated Life of all Asset Tracking & Monitoring Devices at an ambient temperature of 25 degrees Celsius shall be:

Select ONE option:

1. 1 year or more

2. [1 - 3 years or more] [Typically selected for devices being used under very harsh conditions]

3. 5 years or more

4. [Other User-specified duration]

**Note:** Increased Rated Life requirements may lead to higher initial costs.

1. The Vendor shall report the predicted reliability of the Asset Tracking & Monitoring Devices, as calculated by Mean Time between Failures (MTBF) according to Telcordia SR-332.

7.7 Networked Standby Mode Power Disclosure

1. The Vendor shall disclose the Networked Standby Mode Power consumption (W) for Asset Tracking & Monitoring Devices. Networked Standby Mode Power is power consumption when connected to a supply voltage with all functions off, except for support functions using a trigger from a network. This is in accord with the forthcoming AS/NZS 63103.

8 | System Installation and Commissioning Specification

8.1 Introduction

The section covers the combined tasks of System Installation, System Start-up and System Commissioning.

8.2 System Installation Responsibility

Typical System installation activities include hardware mechanical mounting, electrical connections and provisioning for network communication or configuration of basic parameters and default settings. Installation on its own does not result in a state where all Components are operating as intended or where all System functions and capabilities are available to the User.

1. Installation shall be performed by the responsible party:

Select ONE option:

1. The Vendor or its nominated sub-contractor
2. The following third party: [Third party name]
3. Optional: System Installation tasks excludes the physical installation of the Asset Tracking & Monitoring Devices This task will be carried out by a User nominated installation contractor under a separate contract.
4. All hardware necessary for installation and provisioning for network communication shall be provided by the Vendor.

8.3 System Installation Training Requirements

1. If the Vendor is not the responsible party, the Vendor shall provide training on the installation of Gateways and other components (if applicable) to the responsible party and provide a reasonable estimate in Schedule C of the typical component installation time.
2. The responsible party shall provide installation training manuals and all supporting documentation in electronic format.

8.4 System Installation Requirements

The responsible party shall:

* 1. Specify whatever coordination is needed with the User's IT staff for all facets of system installation and implementation.
  2. Mount and electrically connect all Gateways and other Components (as applicable) in a location sufficiently removed from sources of electromagnetic radiation that are likely to interfere with System Performance. The Vendor shall specify minimum acceptable distances.
  3. Inspect the installed System following the installation of all Components and verify that the System is capable of operating as intended.
  4. Ensure that a licensed electrician from the responsible party shall inspect the installed System after it has been fully energised and submit the regionally appropriate electrical installation Certificate of Compliance (CoC) and/or SDoC as per the requirements of AS/NZS 3000 and applicable local requirements, and/or EMC Compliance Declaration.
  5. Submit a brief written report of any defective materials and workmanship issues found during inspections, as well as any unsatisfactory test results.
  6. Submit a brief written report containing a list of all installed components, tests performed, test results, as-built drawings and with a final signoff by the responsible party.

If applicable, the User shall provide:

1. Physical locations for the Gateways (including GPS location);
2. Electric power for the Gateways;
3. Physical location of CMS server hosting (if on-premise server hosting is required);
4. CMS server IT services as applicable (if on-premise server hosting is required); and
5. Access to existing Backhaul Communication network, such as fibre (if available and controlled by the User).

Arrange and facilitate coordination with any relevant third parties

8.5 System Start-Up (Pre-Commissioning)

The process of System Start-up results in all Components operating as intended and all System functions are available to the User. System Start-up activities include the configuration of System hardware, firmware, and software. System Start-up does not result in a state where all System functions and capabilities are configured according to User desires.

8.6 System Start-Up Responsibility

* 1. System Start-up (pre-commissioning) shall be performed by:

Select ONE option:

1. The Vendor or its nominated sub-contractor
2. The following third party: [Third Party name]
   1. All hardware, software and tools necessary for System Start-up shall be provided by the Vendor.

8.7 System Start-Up Training Requirements

* 1. The responsible party shall provide System Start-up training manuals and all supporting documentation.

8.8 System Start-Up Requirements

The responsible party shall:

* 1. Identify a manufacturer-authorised representative available to support System Start-up.
  2. Specify coordination needed with the User's IT staff in order to complete System Start-up.
  3. Configure any hardware, firmware, or software to enable all System Components to operate as intended.
  4. Ensure that the latest versions of all firmware and software are installed and perform any necessary updates or upgrades.
  5. Successfully demonstrate all System functions and capabilities System Start-up training.
  6. Ensure that following User acceptance of a successful demonstration of all System functions a System Start-up trial period shall commence.
  7. Ensure that the System Start-up proving period shall consist of:

Select ONE option:

1. 3 consecutive calendar days of System operation
2. 7 consecutive calendar days of System operation
   1. Ensure that all System functions shall operate normally for at least ninety-nine percent (99%) of the time.
   2. Remedy any issues discovered during the System Start-up trial period.
   3. Provide written documentation of all hardware, firmware, or software configurations and all modifications made in System Start-up and shall accurately represent the System following a successful System Start-up proving period.

8.9 System Commissioning

* 1. The process of System Commissioning results in a state where all System functions and capabilities are configured according to contracted User requirements. Typical System Commissioning activities include the modification of System software settings.

8.10 System Commissioning Responsibility

* 1. System Commissioning training shall be performed by:

Select ONE option:

1. The Vendor
2. The Vendor-specified agent or representative
   1. System Commissioning shall be performed by:

Select ONE option:

1. The Vendor
2. The Vendor-specified agent or representative
3. The following Third Party: [Third Party name]

8.11 System Commissioning Training Requirements

1. The responsible party shall provide Commissioning training manuals and all supporting documentation in electronic Format

8.12 System Commissioning Requirements

The responsible party shall:

* 1. Identify a manufacturer-authorised representative that will be available to support System Commissioning.
  2. Modify any System software settings as necessary to configure all System functions.
  3. Successfully demonstrate all that System functions are performing according to User desires.
  4. Ensure that following User acceptance of a successful demonstration of all System functions performing according to User desires, a System Commissioning trial period shall commence.
  5. Ensure that the System Commissioning period shall consist of:

Select ONE option:

1. 7 consecutive calendar days of System operation
2. 14 consecutive calendar days of System operation
   1. Ensure that all System functions shall operate according to User Specification for at least ninety-nine percent (99%) of the time (after commissioning).
   2. Remedy issues discovered during the System Commissioning trial period.
   3. Submit written documentation of all System software settings required to configure all System functions according to User desires. Written documentation of all System software settings shall include all modifications made over the course of System Commissioning and shall accurately represent the System following the completion of a successful System Commissioning trial period.
   4. Ensure that the system is Manufactured, Installed and Commissioned so that appropriate levels of best practice system security are achieved [Insert specific minimum security requirements if applicable to the organisation].

9 | System Maintenance Specification

The section covers the System maintenance requirements.

9.1 Maintenance Responsibility

1. The System shall be maintained by:

Select ONE option:

1. The Vendor
2. The following Third Party: [Third Party name]
3. The User
4. In the case that the Vendor is maintaining the System, the Vendor shall provide an overall description of its maintenance plan and its reactive and proactive service capabilities to meet that plan.

9.2 Maintenance Requirements

1. **If the System is maintained by a Third Party or the User:**
2. The Vendor shall provide comprehensive maintenance manuals and training at User premises, covering all aspects of the System;
3. The Vendor shall provide hardware and software maintenance and support according to the warranty terms for the duration of the warranty period. Any Maintenance term shall start following the end of the applicable warranty period;
4. The Vendor shall specify any mandatory maintenance required to maintain the terms of the warranty as well as provide an estimate of the annual number of hours required to maintain the System in Schedule C; and
5. Optional: Software and firmware upgrades, maintenance and support shall be provided for one year at no additional cost. The Vendor shall notify the User of any planned firmware updates, obtain User approval prior to making all changes and provide a process for reversing any changes if any faults or unwanted issues are identified.
6. Optional: The Vendor shall provide onsite assistance if remote support cannot resolve maintenance issues.
7. **If the System is maintained by the Vendor:**
8. The responsible party shall be responsible for the complete maintenance of the System, ensuring compliance with all terms of the Specification at all times;
9. If the Vendor is hosting the system, Vendor shall provide a comprehensive backup plan for software/system/server services, and stored data;
10. Optional: Monthly maintenance records and reports shall be submitted to the User. These shall include inspection reports, documentation of maintenance performed, and expected future maintenance requirements; and
11. Optional: The Vendor shall provide a mechanism to allow the User to submit requests for addressing any System malfunctions or maintenance issues.
12. The Vendor shall:
13. Hold a designated quantity of spares that is able to be despatched within 24 hours of notification. The Vendor shall provide a suggested spares list and quantities to be held, for client acceptance or modification; and
14. Provide a 24-hour facility to receive and address requests for technical support.
15. The Vendor shall achieve the following required minimum service levels [The User may wish to amend the suggested text below to suit their own organisational service level requirements or to nominate a standard framework of escalation that they follow]:
16. Handle fault reports via a 24 hour a day, 7 day a week call handling facility and via a website
17. Respond to customers within **[X]** days of their written communication with you.
18. Complete maintenance activities within **[Y]** business days of a fault being reported for a fault involving a single device outage
19. Complete maintenance activities within **[Z]** business days of a fault being reported involving multiple outages of devices or otherwise identified as urgent
20. Optional depending on the type of asset and locations: Respond (attend the site) within a maximum of **[W]** hours to any reported emergency situation and make safe as soon as practicable
21. Meet reporting requirements as outlined within the contract

10 | Appendix A: Terms and Definitions

Asset Tracking and Monitoring Terms and Definitions used in this Model Specification:

1. **AES-128 or AES-256** – The Advanced Encryption Standard is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) adopted by the U.S. government and now used worldwide.
2. **AMS** – An Asset Management System is a type of integrated software package to manage the technical and financial operation and maintenance of infrastructure assets.
3. **API** – Application Programming Interface is a piece of software that enables applications (such as a CMS managing an Asset Tracking & Monitoring System) to exchange data and functionality easily and securely with other applications (such as an AMS or smart city IoT Platform).
4. **Asset Database** – a computerised database to store structured technical, financial and operational details of infrastructure assets.
5. **Astronomical Clock** – a device that determines the expected time of sunrise and sunset for a given calendar date and geographical location.
6. **Boot Loader** – a program that loads an operating system when a computer is turned on.
7. **Backhaul Communication Network** – a communication system linking the Central Management System to one or more Communication Networks (i.e. to the Gateways).
8. **Central Management System (CMS)** – a computer environment that functions as the core of the System by providing all shared System services and consolidating and storing System data.
9. **Constrained Application Protocol** **(CoAP)** – A specialised web protocol for use with constrained nodes and networks in the Internet of things for machine-to-machine applications.
10. **Compatibility** – the ability of a device to operate on a network with another device without interfering with the operation of the other device.
11. **Component** – any installed, replaceable and/or upgradable item with a unique product number that is necessary to meet the requirements of this specification.
12. **Communication Network** – a communication system linking the Gateways to Asset Tracking & Monitoring Devices.
13. **FTP** – A File Transfer Protocol is a standard network protocol used for the transfer of computer files between a client and server on a computer network.
14. **Gateway (or Base Station, or Router**) – a communications device designed for interfacing between two communication networks that use different protocols.
15. **Graphical User Interface (GUI)** – a screen-based diagrammatic representation of a system.
16. **HMAC** – a specific type of Message Authentication Code involving a cryptographic hash function and a secret cryptographic key.
17. **Host Site** – the physical location of the Central Management System. Refers specifically to a site owned and operated by the User.
18. **http** – Hypertext Transfer Protocol is an application protocol for distributed, collaborative, and hypermedia information systems.
19. **ICT** – Information and Communications Technology
20. **International Electrotechnical Commission (IEC)** – The international standards development Organisation for electrical and electronic products and infrastructure.
21. **Ingress Protection (IP) -** AS/NZS 60529 Ingress Protection classifies and rates the degree of protection provided against intrusion by dust and moisture for mechanical casings and electrical enclosures.
22. **Internet Protocol (IP)** - Internet Protocol is the principal communications protocol in the Internet protocol suite for relaying data across network boundaries.
23. **Interchangeability** – the ability of a device to operate on a network in the same manner as a like device, where each device can be exchanged in the system.
24. **Interoperability** – the ability of a device to operate on a network in a consistent manner with a similar device.
25. **Latency** – the measure of time delay in a system.
26. **Management Station** – a user device that provides an interface to users to access the Central Management System e.g. mobile phone, laptop, tablet, desktop.
27. **Network** – a group of systems that function cooperatively or interdependently to provide a chain of command for asset control.
28. **Networked Standby Mode** - mode when connected to a supply voltage with all functions off, except for support functions using a trigger from a network
29. **On-shore Insurance Bond** – an indemnification tool providing project-related financial underwriting.
30. **Online Operation** – the normal operating condition whereby Gateways or Asset Tracking & Monitoring Devices are communicating with the Central Management System.
31. **Offline Operation** – any condition whereby Gateways or Asset Tracking & Monitoring Devices are not communicating with the Central Management System.
32. **Parent Company Guarantee** – a financial guarantee from a principal company (usually international) to a subsidiary company (usually local) providing project-related financial underwriting.
33. **Project Performance Insurance** – an indemnification tool providing project related financial underwriting of satisfactory technical performance.
34. **Protocol** – a set of standard rules for communicating over a computer network.
35. **Sensors** – Devices that may be installed on the same asset (or on the same Communication Network that enable measurement of physical parameters such as light, traffic, air quality, climate, or sound.
36. **SHA-256** – The Secure Hash Algorithm is one of a number of cryptographic hash functions. Like a signature for a text or a data file.
37. **SMTP** – The Simple Mail Transfer Protocol is an Internet standard for electronic mail transmission.
38. **SNMP** – The Simple Network Management Protocol is a protocol for network management used for collecting information and configuring network devices on an Internet Protocol network.
39. **Standby Mode** - mode when connected to a supply voltage with all functions off, except for support functions using a sensor, timer or external trigger not being a trigger from a network.
40. **System** – the entire set of networked Components. Hardware and software, typically consisting of Asset Tracking & Monitoring Devices, Gateways, Backhaul, a Central Management System, and Management Stations, that function together to adaptively control and remotely monitor tracking devices.
41. **TCP** – The Transmission Control Protocol is one of the main protocols of the Internet protocol suite. The entire suite is commonly referred to as TCP/IP.
42. **UDP** – The User Datagram Protocol is a simple OSI transport layer protocol for client/server network applications based on Internet Protocol.
43. **X.509 Certificate** – a digital certificate that uses the international X.509 public key infrastructure standard that defines the format of public key certificates. X.509 certificates are used in many Internet protocols.

11 | Appendix B: Standards References

11.1 Normative References

1. **International Electrotechnical Commission (IEC)**
2. IEC 60529 Degrees of protection provided by enclosures (IP Code)
3. **Telcordia**
4. SR-332 Reliability Prediction Procedure for Electronic Equipment
5. **Australia/New Zealand Standards**
6. AS/CA S042 Requirements for connection to an air interface of a telecommunications network – Part 1: General
7. AS/NZS CISPR 15 Limits and methods of measurement of radio disturbance characteristics of electrical lighting and similar equipment
8. AS/NZS 3000 Electrical Installations (Australian/New Zealand Wiring Rules)
9. AS/NZS 3820 Essential safety requirements for electrical equipment
10. AS/NZS 4268 Radio equipment and systems - Short range devices - Limits and methods of measurement

12 | Appendix C: Returnable Schedules

In responding to this tender, tenderers need to provide the following completed schedules:

**SCHEDULE A** - Vendor Information & Referees

**SCHEDULE B** - Asset Tracking & Monitoring System Technical Specification Compliance Response for:

* 1. Central Management System
  2. Communication Networks
  3. Asset Tracking & Monitoring Devices Installation & Maintenance

**SCHEDULE C** - Pricing

**SCHEDULE D** - Warranty Information

**SCHEDULE E** - Vendor or Project Performance Guarantees, Bonds, Insurances (Optional)

**SCHEDULE F** - Statutory Declaration (Optional)

12.1 SCHEDULE A: Vendor Information & Referees

Please provide the following details separately for both the Tenderer (typically a local distributor as Vendor) and the Manufacturer (if not the same company) for the purpose of evaluating tenders:

**Tenderer's Information**

|  |  |
| --- | --- |
| **ITEM** | **RESPONSE** |
| 1. Tenderer Name |  |
| 1. Location (Physical address) |  |
| 1. ABN or NZ Company No. |  |
| 1. Website |  |
| 1. Number of Employees |  |
| 1. Approximate Annual Financial Turnover | [Like all other information submitted, this will remain confidential to the Evaluation Panel and its advisers] |
| 1. Relationship to Manufacturer (if not the same company) | [Clarify whether distribution rights are exclusive, whether the manufacturer has shareholding in the distributor etc] |
| 1. Competencies in Asset Tracking & Monitoring Devices and wireless communications | [Brief company CV – Max half page] |
| 1. List of reference sites / customers | [List recent relevant reference sites/customers and approximate number of Asset Tracking & Monitoring Devices for each. Local reference sites preferred but international reference sites may also be relevant] |
| 1. Competencies of key ANZ-based staff | [Brief one-paragraph CVs of key technical  or customer-facing personnel] |
| 1. Ability to support site visits | [Name of customer service representative and location] |

[Tenderer to delete table below if tenderer and manufacturer are the same company]

**Manufacturer’s Information**

|  |  |
| --- | --- |
| **ITEM** | **RESPONSE** |
| 1. Manufacturer Name |  |
| 1. Location (Physical address) |  |
| 1. ABN / NZ Company No. |  |
| 1. Website |  |
| 1. ISO 9001 Certification No. |  |
| 1. Number of Employees |  |
| 1. Approximate Annual Financial Turnover | [Like all other information submitted, this will remain confidential to the Evaluation panel and its advisers] |
| 1. Competencies in Asset Tracking & Monitoring Devices and wireless communications | [Brief company CV – Max half page] |
| 1. Competencies of key ANZ-based staff (if applicable) | [Brief one-paragraph CVs of key technical  or customer-facing personnel] |
| 1. Ability to support site visits | [Name of customer service representative and location if applicable] |

**Referee’s Information**

The Tenderer shall provide [Insert No. of referees required] from recent projects. Tenderers shall provide a contact for each who is able to act as a referee for this tender and has given their permission to be contacted.

For most Vendors of Asset Tracking and Monitoring Systems there may be few suitable local referees with application experience of sufficient scale, at this time. In this case, Vendors may provide (English speaking) referees from international projects.

The Tenderer shall provide a minimum of:

For local or international reference projects, other than trials. Select ONE of the following options:

1. Two referees
2. Three referees

Information about referees and their projects shall be provided in the tables below:

**Note:** Actual projects are required to obtain meaningful reference information. Trial or demonstration projects do not convey the nature of the typical support and backup patterns required of a Vendor. Vendors and Manufacturers operate in a world market and local procurement organisations need to access third party viewpoints on the nature of the system performance and support provided by the Vendor or Manufacturer. Setting a high quantity may unreasonably limit the field.

**Referee 1**

|  |  |
| --- | --- |
| **ITEM** | **RESPONSE** |
| 1. Referee Name |  |
| 1. Organisation |  |
| 1. Location of Referee (Physical address) |  |
| 1. Telephone |  |
| 1. Email |  |
| 1. Project Description | [Brief description of project] |
| 1. Project Size and Nature | [Type of CMS Software, Type of Asset Tracking & Monitoring Devices, Type of Communication Network, Number of Asset Tracking & Monitoring Devices, Date of first installation, Date of last installation.] |
| 1. Project Objective and Achievements | [Goals of the project, Measurable benefits of the project, Non-measurable benefits of the project] |

**Referee 2**

|  |  |
| --- | --- |
| **ITEM** | **RESPONSE** |
| 1. Referee Name |  |
| 1. Organisation |  |
| 1. Location of Referee (Physical address) |  |
| 1. Telephone |  |
| 1. Email |  |
| 1. Project Description | [Brief description of project] |
| 1. Project Size and Nature | [Type of CMS Software, Type of Asset Tracking & Monitoring Devices, Type of Communication Network, Number of Asset Tracking & Monitoring Devices, Date of first installation, Date of last installation.] |
| 1. Project Objective and Achievements | [Goals of the project, Measurable benefits of the project, Non-measurable benefits of the project] |

12.2 SCHEDULE B: Asset Tracking & Monitoring System Technical Documentation

**Note:** Tendering organisation to insert additional tables below if additional referees are required.

Tender submission documentation shall be provided in [Tending organisation to insert form of returnable schedules] and supported by the following attachments:

1. Technical Specifications for all Components:
2. Brochures, specifications, technical data sheets, drawings and other technical information describing the Components to be used in the proposed System including explicit identification of model/catalogue numbers
3. Asset Tracking & Monitoring Devices and Gateway regulatory safety and EMC compliance certifications and/or test reports and Supplier Declarations of Conformity (SDoCs)
4. Documentation of System topology and layout:
5. Proposed Asset Tracking & Monitoring Devices and Gateway topology (e.g. Star, Mesh or Mobile communication), layout and proposed Gateway locations (if applicable)
6. Representative system communication paths between Asset Tracking & Monitoring Devices, Gateways and Backhaul communication network(s)
7. A description of the modelling or analysis methods used to support the proposed Asset Tracking & Monitoring Devices, Gateway and Backhaul topology and layout, System communication paths, and confidence in System performance

12.3 SCHEDULE C: Price Information

A tender submission may be based on a traditional capital asset acquisition model or, for the supply of an Asset Tracking & Monitoring system based on a Network-as-a-Service (NaaS) model, submissions can be based on on-going operating charges. The tender submission shall include pricing (initial) and fees (recurring) for a System that fully meets this specification and does not require any additional options or upgrades.

The pricing is to be stated separately for each of the categories, as in the [Tending organisation to insert form of returnable pricing Schedule C].

**Note:** This model specification is designed to align with Best Value (BV) public sector procurement processes that use evaluation methods that include price comparison on the basis of whole of life costing over the full asset lifespan and including the use of Discounted Cash Flow (DCF) techniques such as Net Present Value (NPV) calculations. Procurement and tender evaluation methods that use simple comparison of lowest initial pricing are not suitable.

12.3.1 Hardware Pricing Notes:

Hardware tender pricing as quoted in the attached Schedule C shall be for goods Free-Into-Store (FIS) at the following location:

[Insert location of User or local installation contractor’s nominated store]

12.3.2 Payment Terms

The tender submission should include any Vendor-desired Payment Terms and identify any Vendor-desired payment timing for the specified project steps.

12.3.3 Financing Options

The tender submission shall:

Select one or more, as desired

1. Include Vendor financing options
2. Include Vendor specified Third Party financing options
3. Not include financing options

12.4 SCHEDULE D: Warranty Information

12.4.1 Hardware Warranty

All Hardware Components shall be covered by a single-source written replacement warranty covering materials and workmanship for a period of:

Select ONE option:

1. 5 years
2. 10 years
3. [Other User-specified duration]

This shall provide a full replacement Component product warranty from the date of the purchase invoice on a Component “return-to-base” labour and transport basis.

A full replacement return-to-base warranty shall include Component repair or replacement of (at a minimum):

1. Failure of any electrical, electronic, optical or mechanical components.
2. Failure of any ingress protection resulting in moisture or dirt degradation.
3. Vendor transport costs to and from a User nominated local store.

A full replacement return-to-base warranty does not include:

1. Site removal or reinstallation by Vendor, including transport and labour.
2. Component failure caused by improper handling, misuse, abuse, vandalism or negligence.
3. Any failed Component pro-rata usage cost recovery by the Vendor.

The User may perform field measurements and/or send Components to independent laboratories for testing (at User cost) to enforce warranty provisions at any time during the warranty period.

12.4.2 Software Warranty

All software shall be covered by a written replacement warranty and maintained via a firmware update mechanism for a period of:

Select ONE option:

1. 1 year
2. 2 years
3. 3 years
4. 5 years
5. 10 years
6. [Other User-specified duration]

12.4.3 Warranty Certificates

Signed warranty certificates shall be provided to the client immediately upon completion of installation and commissioning. Unless specifically agreed with the User, these warranty conditions take precedence over any standard supplier warranty provisions or terms and conditions of sale.

12.5 SCHEDULE E: Vendor or Project Performance Guarantees, Bonds, Insurances

**Note:** Vendor Company financial security instruments such Parent Company Guarantees, Bank Guarantees, On-shore Insurance Bonds or Project Performance Insurance are various methods of indemnifying the User against deficiencies in performance of the System and/or of the Vendor during the Warranty period. These instruments may be a useful method of risk mitigation for larger projects. Note that these measures may have cost implications and should not be applied unless there are specific reasons for doing so. In the case of Project Performance Insurance it should be stated in the Tender Specification whether the insurance premium costs will be borne by the User or by the Vendor.

1. Optional: The following Vendor and/or project performance risk mitigating instruments shall be provided by the Vendor:

Select ONE or MORE, as desired

* 1. Parent Company Guarantee [Insert all required details]
  2. Bank Guarantee [Insert all required details]
  3. On-shore Insurance Bond [Insert all required details]
  4. Project Performance Insurance [Insert all required details]

1. Optional: The Vendor and/or project performance risk mitigating instruments required as above shall have a duration of:

Select ONE or MORE, as desired

* 1. 3 Year
  2. 5 Year
  3. 10 Year
  4. Same duration as Hardware Warranty

* 1. SCHEDULE F: Statutory Declaration **(Optional)**

**Note:** Tendering organisations have the option of inserting a standard form of statutory declaration relevant to the jurisdiction of the tendering organisation allowing the vendor to attest to the truthfulness of their tender submission. Perhaps most importantly, vendors would be attesting to that the list of substantiating documentation is available in precisely the format requested and with appropriate certifications from accredited independent laboratories.

A picture containing text, electronics, businesscard

Description automatically generated