

Hardware, Software and Services End-User License Agreement (EULA)



IMPORTANT—READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and the Licensor, **a Person** ("Licensor"), for the software product identified above, which includes computer software and associated media, printed materials, and "online" or electronic documentation ("Software"). By installing, copying, or otherwise using the Software, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the Software.

1. Grant of License

Licensor grants you a non-exclusive, non-transferable, revocable license to install and use the Software on a single device, owned or leased by you, solely for your internal business or personal use, subject to the terms and conditions set forth in this EULA.

A. Trial/Evaluation License

If the Software is designated as a trial, evaluation, not-for-resale (NFR), or promotional version, you may use it solely for the purpose of testing and evaluating the Software for a limited period of **☐ Date**, and the license is automatically terminated upon the expiration of this period or when you cease to use the Software, whichever occurs first.

2. Restrictions

You may not, and you agree not to permit others to:

- Modify, adapt, translate, or create derivative works based upon the Software.
- Decompile, disassemble, reverse engineer, or otherwise attempt to discover the source code or underlying ideas or algorithms of the Software.
- Rent, lease, lend, sell, sublicense, distribute, or otherwise transfer the Software to any third party.
- Use the Software for any purpose other than as expressly permitted herein.
- Remove, alter, or obscure any proprietary notices, labels, or marks from the Software.

3. Intellectual Property

The Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Software is licensed, not sold. All right, title, and interest in and to the Software (including without limitation any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the Software), and any copies of the Software, are owned by Licensor or its suppliers.

4. Term and Termination

This EULA is effective upon your acceptance and use of the Software and shall continue until terminated. Licensor may terminate this EULA immediately and without prior notice if you fail to comply with any of the terms and conditions set forth in this EULA. Upon termination, you must immediately cease all use of the Software and destroy all copies, in whole or in part, of the Software.

5. Disclaimer of Warranty

The Software is provided "AS IS" without warranty of any kind. Licensor and its suppliers disclaim all warranties, either express or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose, with respect to the Software.

6. Limitation of Liability

In no event shall Licensor or its suppliers be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitation, damages for loss

of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use the Software, even if Licensor has been advised of the possibility of such damages.

7. Governing Law

This EULA shall be governed by and construed in accordance with the laws of the jurisdiction of 📍 Place, without regard to its conflict of laws principles.

8. Entire Agreement

This EULA constitutes the entire agreement between you and Licensor regarding the use of the Software and supersedes all prior and contemporaneous agreements, discussions, and understandings, whether written or oral.

9. Contact Information

If you have any questions about this EULA, please contact Licensor at:

- **Company Name:** Provider or Ionity (Pty) Ltd
- **Address:** Centurion South Africa
- **Email:** Johan Wilhelm Van Antwerp
- **Phone:** +27 9

By installing or using the Software, you confirm that you have read and understood this EULA and agree to be bound by its terms and conditions.

Hardware-as-a-Service (HaaS) & Software

Licensing Document Code: ION-EULA-HAAS-001

Compliance Framework: Policy 986 AED (Security & Fines)

Effective Date: [Insert Date]

This End User License and Hardware Agreement ("Agreement") is a legally binding contract between Ionity (Pty) Ltd ("Ionity", "We", "Our") and the Client ("User", "You"). By installing, powering on, or accessing the AEDi™ ecosystem or AI-M hardware, You agree to be bound by these terms.

1. The "Gas Bottle" Principle: Hardware Ownership & Usage Rights

Ionity operates on a strict Hardware-as-a-Service (HaaS) model.

1. **Absolute Ownership:** Similar to an industrial gas cylinder lease, all physical hardware—including the AI-M (Artificial Intelligent Motherboard), Project Root System [PRS01] edge nodes, and associated sensor arrays—remains the sole, exclusive property of Ionity (Pty) Ltd at all times.
2. **Perpetual Usage Right:** As long as Your subscription, SLA, or authorized use agreement remains active and in good standing, You are granted a non-exclusive, non-transferable right to use the hardware and software indefinitely to monitor and optimize Your industrial operations.
3. **Return of Hardware:** Upon termination of the service agreement by either party, all Ionity hardware must be surrendered and returned to Ionity.

2. Strict Anti-Tampering & Physical Security (Policy 986 AED)

The AI-M hardware is engineered for True Edge AI at an ultra-low power threshold (5V 20W). To protect our intellectual property and your operational safety, strict physical boundaries apply:

1. **No Tampering or Opening:** You are strictly prohibited from opening the hardware enclosure, breaking the security seals, or attempting to physically access the internal PCB, circuitry, or cryptographic modules.
2. **No Reverse Engineering:** You may not decompile, disassemble, or reverse-engineer the physical hardware, the embedded firmware, or the Over-The-Air (OTA) update mechanisms.
3. **No Unauthorized Destruction:** You may not deliberately destroy, dismantle, or dispose of the hardware under any circumstances. If a unit is slated for decommissioning, it must be returned to Ionity for secure cryptographic wiping and recycling.

3. Standards Adherence, Notification & Replacement

Ionity guarantees the performance of the AEDi™ ecosystem by adhering to strict internal Quality Management System (QMS) standards.

1. **Mandatory Notification:** If a hardware unit fails, shows signs of physical damage, or drops offline, You must immediately notify Ionity Support via the CMMS dashboard or at support@ionity.today.
2. **Guaranteed Replacement:** Ionity takes full responsibility for maintaining system integrity. Upon receiving a valid failure notification, Ionity will dispatch a replacement AI-M unit or sensor array to ensure your predictive maintenance (PdM) capabilities remain uninterrupted. You are not authorized to attempt repairs yourself.

4. Software & CMMS Dashboard Licensing

1. **Zero Trust Network:** The software provided—including the customized Graphical User Interfaces (GUIs), Smart Notify alerts, and DaQ pipelines—operates on a Zero Trust architecture. You may not bypass the established VPN or VLAN tunnels.
2. **Data Ownership:** While Ionity owns the hardware and the AI algorithms, You retain full ownership of the raw telemetry and operational data generated by Your facilities.

5. Policy 986 AED Fines & Penalties

Because Ionity bears the capital cost of the hardware and the risk of intellectual property exposure, violations of the anti-tampering clauses are met with severe financial penalties.

Under Policy 986 AED, if an Ionity audit or automated physical tamper-switch detects that a unit has been opened, compromised, reverse-engineered, or destroyed by the User or the User's unauthorized contractors:

1. **Immediate Penalty:** The User will be liable for an immediate Tamper & IP Compromise Fine of min R 50,000 per compromised unit or service.
2. **Service Suspension:** Ionity reserves the right to immediately suspend all cloud access, CMMS dashboard functionality, and OTA updates until the fine is paid and the compromised hardware is recovered.
3. **Legal Action:** In cases of suspected intellectual property theft, Ionity reserves the right to pursue further damages under international trade secret laws.

EXPANSION: MISSING ELEMENTS FOR IONITY EULA & HAAS AGREEMENT

Below are the critical additions and expansions to strengthen your Hardware, Software and Services End-User License Agreement (EULA) and Hardware-as-a-Service (HaaS) document. These address gaps specific to your AEDi™ ecosystem, Cerberus-4 architecture, and global enforcement posture.

A. DEFINITIONS SECTION (ADD TO SECTION 1 OR CREATE NEW SECTION 0)

Add precise, legally operative definitions for technical and commercial terms:

- "AEDi™" means the Automated Ecosystem Design Intelligence platform, including its AI/ML models, data pipelines, and orchestration logic, owned exclusively by Ionity (Pty) Ltd.
- "AI-M" means the Artificial Intelligent Motherboard hardware unit, including all embedded firmware, cryptographic modules, and sensor interfaces.
- "Cerberus-4" means the multi-layered security gateway architecture comprising four (4) ESP32-S3 modules interfaced with a Raspberry Pi 5 core via hardware-isolated UART channels, as specified in Exhibit A.
- "Project Root System [RPS01]" means the 9-channel edge measurement node supporting energy monitoring sensors, SD card logging, RTC time-stamping, SIM cellular fallback, GPS geo-tagging, and ADXL accelerometer integration, as specified in Exhibit B.
- "OTA" means Over-The-Air update mechanisms for firmware, configuration, and AI model deployment, requiring cryptographic signature verification and rollback capability.
- "Zero Trust Architecture" means the security model wherein no device, user, or network segment is implicitly trusted; all communications require authentication, authorization, and encryption per Policy AED 986.
- "Tamper-Switch" means the hardware-integrated physical intrusion detection system that logs and reports unauthorized enclosure access to Ionity's CMMS dashboard.
- "Telemetry Data" means operational metrics, sensor readings, system health logs, and diagnostic information generated by Ionity hardware, excluding Client's proprietary process data.

B. DATA PRIVACY, COMPLIANCE & CROSS-BORDER TRANSFER (ADD AS NEW SECTION)

Given global deployments and POPIA/GDPR obligations:

- Data Processing Roles: Ionity acts as a Data Processor for Telemetry Data required for system maintenance, predictive analytics, and OTA

integrity. Client remains the Data Controller for operational/process data generated by their facilities.

- **Cross-Border Transfers:** Where Telemetry Data is transmitted outside the Republic of South Africa, Ionity ensures compliance with POPIA Section 72, GDPR Chapter V, or equivalent frameworks via Standard Contractual Clauses or Binding Corporate Rules.
 - **Data Retention & Deletion:** Telemetry Data is retained only for the duration necessary for system performance, security auditing, and model improvement. Upon written request and contract termination, Ionity will securely delete Client-identifiable Telemetry Data within 90 days, except where retention is required by law.
 - **Client Data Ownership:** Client retains exclusive ownership of raw operational data generated by their industrial processes. Ionity's AI models trained on aggregated, anonymized Telemetry Data remain Ionity's exclusive Intellectual Property.
-

C. FIRMWARE INTEGRITY, OTA UPDATES & ROLLBACK PROTOCOLS (EXPAND SECTION 2 OR ADD NEW)

Critical for your ESP32-S3 + RPi5 multi-module architecture:

- **Signature Verification:** All OTA updates must be cryptographically signed by Ionity. Hardware will reject unsigned or tampered firmware packages.
 - **Atomic Updates:** Firmware updates are applied atomically per module (ESP32#1-#4, RPi5 core) to prevent partial-state failures.
 - **Rollback Capability:** If an update fails integrity checks or causes system instability, hardware will automatically revert to the last known-good firmware version.
 - **Update Windows:** OTA deployments occur during Client-approved maintenance windows unless classified as a Critical Security Patch (e.g., CVE remediation), which may be deployed immediately with prior notice where feasible.
 - **No User-Initiated Flashing:** Client is prohibited from manually flashing firmware, modifying bootloaders, or altering partition tables. All firmware changes must occur via Ionity's authenticated OTA pipeline.
-

D. NETWORK SECURITY & ZERO TRUST REQUIREMENTS (ADD AS NEW SECTION)

Align with your documented architecture:

- Network Segmentation: Client must ensure Ionity hardware operates on a logically segmented network (VLAN) isolated from general corporate IT infrastructure, unless otherwise approved in writing.
 - Firewall Rules: Outbound connections are permitted only to Ionity-approved cloud endpoints (documented in Exhibit C). Inbound connections to Ionity hardware are prohibited except for authenticated OTA and CMMS management traffic.
 - VPN/Tunnel Requirements: Where public internet is used for cloud connectivity, Client must support IPsec or WireGuard tunnels as configured by Ionity.
 - Wireless Interface Restrictions: Client shall not enable, modify, or interfere with hardware wireless interfaces (Wi-Fi, BLE, Cellular) beyond Ionity-provided configuration profiles.
-

E. AUDIT, MONITORING & COMPLIANCE TELEMETRY (ADD AS NEW SECTION)

Enable remote enforcement of Policy 986 AED:

- Remote Integrity Checks: Ionity may remotely query hardware for tamper-switch status, firmware version hashes, secure boot logs, and UART communication integrity.
 - Compliance Telemetry: Hardware periodically transmits anonymized compliance metadata (e.g., "enclosure sealed: true", "firmware signature: valid") to Ionity's CMMS for audit purposes.
 - Audit Rights: Upon reasonable notice, Ionity may request Client to facilitate a remote or on-site audit to verify compliance with anti-tampering, network security, and usage terms.
 - Non-Interference: Client shall not block, filter, or modify compliance telemetry transmissions. Doing so constitutes a material breach triggering Policy 986 AED penalties.
-

F. FORCE MAJEURE, OFFLINE RESILIENCE & SERVICE CONTINUITY (EXPAND SECTION 5 OR ADD NEW)

Address your hardware's offline capabilities (SD logging, SIM fallback):

- **Offline Operation:** In the event of network outage, hardware will continue local data acquisition and store Telemetry Data on the integrated SD card module with RTC time-stamping. Data will sync automatically upon connectivity restoration.
 - **Cellular Fallback:** When equipped with a SIM module, hardware will attempt automatic failover to cellular networks. Client is responsible for ensuring cellular coverage or approving alternative connectivity arrangements.
 - **Force Majeure:** Neither party is liable for failure to perform due to causes beyond reasonable control (e.g., natural disasters, war, government action, widespread internet outage). Ionity will use commercially reasonable efforts to restore service promptly.
 - **Data Loss Disclaimer:** Ionity is not liable for data loss resulting from Client's failure to maintain power, network connectivity, or environmental conditions within hardware specifications.
-

G. MULTI-JURISDICTIONAL ENFORCEMENT & IP PROTECTION (EXPAND SECTION 7 OR ADD NEW)

Strengthen global IP enforcement posture:

- **Applicable Law Election:** Ionity reserves the right to elect governing law per dispute: (a) Republic of South Africa for contractual breaches; or (b) State of Delaware, USA, for intellectual property misappropriation claims.
 - **International Treaties:** Client acknowledges Ionity's IP is protected under the Defend Trade Secrets Act (US), TRIPS Agreement, WIPO Copyright Treaty, and South African Copyright/Patents Acts.
 - **Injunctive Relief:** Client consents to Ionity seeking immediate injunctive relief in any competent court globally to prevent irreparable harm from IP misappropriation or hardware tampering.
 - **Costs & Fees:** In any enforcement action arising from Client's breach, prevailing Ionity shall be entitled to recover reasonable attorneys' fees, forensic investigation costs, and expert witness fees.
-

H. EXHIBITS & TECHNICAL REFERENCES (ADD STRUCTURE)

Reference detailed specs without cluttering the main agreement:

- Exhibit A: Cerberus-4 Technical Specifications (GPIO matrix, UART assignments, power thresholds, performance benchmarks)
- Exhibit B: Project Root System [RPS01] Hardware Features (9-channel measurement, SD/RTC/SIM/GPS/ADXL specifications)
- Exhibit C: Approved Cloud Endpoints & Network Configuration (IP ranges, ports, TLS requirements)
- Exhibit D: Policy 986 AED – Security, Tamper Detection & Penalty Schedule (detailed fine structure, audit procedures)

Note: Exhibits are incorporated by reference and form part of this Agreement.

I. SUBSCRIPTION, BILLING & TERMINATION MECHANICS (EXPAND SECTION 4 OR ADD NEW)

Clarify HaaS commercial terms:

- Billing Cycle: Fees are billed [monthly/quarterly/annually] in advance. Late payments incur interest at 1.5% per month or the maximum rate permitted by law.
 - Suspension for Non-Payment: Ionity may suspend CMMS dashboard access and OTA services after 15 days' written notice of overdue payment. Hardware will continue local logging but cease cloud synchronization.
 - Termination for Cause: Either party may terminate for material breach upon 30 days' written notice if uncured. Ionity may terminate immediately for tampering, reverse engineering, or IP theft.
 - Post-Termination Obligations: Upon termination, Client must: (a) cease all use of Software; (b) return all hardware per Section 1; (c) provide written certification of destruction of local copies; and (d) pay all outstanding fees and applicable Policy 986 AED penalties.
-

J. ASSIGNMENT, CHANGE OF CONTROL & SUCCESSION (ADD AS NEW SECTION)

Address business continuity scenarios:

- Client Assignment: Client may not assign this Agreement or transfer hardware usage rights without Ionity's prior written consent, except in connection with a merger, acquisition, or sale of substantially all assets, provided the successor assumes all obligations herein.
 - Ionity Assignment: Ionity may assign this Agreement in connection with corporate reorganization, merger, or sale of assets, provided Client's usage rights and data protections remain substantially unchanged.
 - Notification Requirement: Client must notify Ionity within 30 days of any change in controlling ownership, legal entity name, or primary operational address affecting hardware deployment.
-

K. SURVIVAL, ELECTRONIC ACCEPTANCE & MISCELLANEOUS (ADD TO SECTION 8 OR NEW)

Finalize enforceability mechanics:

- Surviving Provisions: Sections on Intellectual Property, Confidentiality, Data Ownership, Audit Rights, Limitation of Liability, Governing Law, and Policy 986 AED Penalties shall survive termination or expiration of this Agreement.
 - Electronic Acceptance: By powering on Ionity hardware, accessing the CMMS dashboard, or clicking "I Agree" in the provisioning workflow, Client manifests assent to this Agreement. Telemetry logs of first boot and dashboard login serve as evidence of acceptance.
 - Severability: If any provision is held unenforceable, the remainder of the Agreement remains in full force, and the invalid provision shall be reformed to the minimum extent necessary to achieve its original intent.
 - Waiver: No waiver of any breach shall be deemed a waiver of any subsequent breach. Waivers must be in writing and signed by Ionity's authorized representative.
 - Notices: All formal notices shall be sent to the addresses on file in Ionity's CMMS or to legal@ionity.today, with reference to Document Code ION-EULA-HAAS-001.
-

L. CONTACT & SUPPORT CLARIFICATION (UPDATE SECTION 9)

Ensure clear escalation paths:

- Technical Support: support@ionity.today | CMMS Dashboard Ticketing | Response SLA per subscribed tier
- Legal & Compliance: legal@ionity.today | For EULA interpretations, audit requests, or policy clarifications
- Security Incidents: security@ionity.today | 24/7 for tamper alerts, suspected breaches, or critical vulnerabilities
- Documentation Portal: <https://ionity.today/privacy> | For firmware notes, configuration guides, and Exhibit references

BY USING THE IONITY HARDWARE AND SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTOOD, AND AGREE TO BE BOUND BY THIS EULA AND THE FINES STIPULATED UNDER POLICY 986 AED.

DATE: 2026/01/10

AUTHORIZED BY: Johan Wilhelm van Antwerp