RIoT Secure Partner Pack for Horizon Cluster 4 IA (HORIZON-CL4-2026)

Version: Q1 2026 | For consortium building + partner onboarding forms

We are a partner seeking for a consortium.
We are providing Product, Technology, Services, Use Case and Expertise

1) Partner role

RIoT Secure provides the **secure lifecycle control plane** for edge/industrial data and AI artifacts: **secure onboarding, policy-based deployment, versioned releases, staged rollout, safe rollback, and compliance evidence** (CRA-aligned), including **lightweight secure connectivity (µTLS)** and **sandboxed execution (WASM/Brawl)**.

2) Why RIoT Secure

- **Lifecycle governance is the product** (not a bolt-on): versioning, rollout/rollback, fleet coherence, audit logs, and operational guardrails engineered for long-lived deployments.
- **Constrained + disconnected-first security:** µTLS enables secure comms with **very low overhead**, designed for low bandwidth, power, and intermittent connectivity.
- **Safe change without recertifying the whole device: WASM/Brawl** modular execution enables updating application logic / AI workflows independently from stable firmware layers.
- **Compliance evidence by design (CRA-ready posture):** traceability from **artifact → config → device → deployment event**, supporting audits, incident response, and secure-by-design claims.
- **Industrial proof orientation:** designed to produce **repeatable evidence packages** (deployment reports, rollback drill results, security posture dashboards), not just demos.

3) Suggested Work Package

WPX - Security, Trust & Lifecycle Governance for Edge/Industrial Data & AI (Lead: RIoT Secure)

Objective: Provide end-to-end security and operational lifecycle governance so that data and AI artifacts can be deployed, updated, monitored, and rolled back safely across distributed edge/industrial environments, while generating compliance evidence aligned with emerging regulation (e.g., CRA).

Main activities:

1. **Security architecture & trust boundaries:** threat model, asset inventory, trust assumptions, secure-by-design requirements mapped to system components and data flows.
2. **Identity, onboarding & policy enforcement:** secure provisioning, device identity, authorization model, and policy-based deployment controls.
3. **Artifact governance:** signed/attested releases for models, configs, and edge modules; provenance tracking and version coherence across fleets.
4. **Staged rollout & safe rollback:** canary/staging strategies, rollback criteria, recovery playbooks, and **rollback drill evidence**.
5. **Telemetry, auditability & compliance evidence:** security events, lifecycle state, deployment logs, and “evidence packs” for audits and operational sign-off.
6. **Demonstrator integration:** integrate lifecycle controls into at least one project use case (industrial/transport/public infrastructure), validating operational constraints (connectivity, maintenance windows, safety requirements).

Deliverables (examples):

- D-WPX.1 Security architecture + threat model + requirements mapping (incl. CRA-relevant controls)
- D-WPX.2 Lifecycle governance specification (identity, policy, artifact signing, rollout/rollback)
- D-WPX.3 Evidence pack template + audit log schema + operational guardrails
- D-WPX.4 Demonstrator integration report + rollout/rollback drill results + fleet coherence report

4) Expected outcomes

- **Operationally validated lifecycle governance** for edge/industrial deployments: controlled updates, rollback, and measurable fleet coherence.
- **Trustworthy deployment of AI/data artifacts** with provenance and integrity: verifiable “what is running where” across distributed nodes.

- **Reduced risk and cost of field operations:** fewer site visits, faster safe iteration, less downtime via staged rollout + recovery workflows.
- **Compliance-ready evidence generation:** auditable logs and security posture artifacts that strengthen CRA-aligned claims and procurement readiness.

5) Short paragraph for Part B form (Horizon format)

RIoT Secure will provide the project's **security and lifecycle governance layer,** enabling trustworthy deployment of data and AI artifacts across distributed edge and industrial environments. We will implement **secure onboarding and policy-based deployment**, versioned releases with **staged rollout and safe rollback**, and continuous monitoring with **audit-grade compliance evidence** aligned with secure-by-design expectations (including CRA). By combining **lightweight secure connectivity (µTLS)** for constrained /disconnected operation and **sandboxed execution (WASM/Brawl)** for modular updates, RIoT Secure ensures the consortium can demonstrate not only technical performance, but also **operational robustness, traceability, and regulatory readiness** in at least one real industrial/use-case demonstrator.

6) What we need from the coordinator

- Target use cases + data flows (who provides data, who consumes, where decisions happen)
- High-level system architecture/integration points for identity, artifact delivery, and telemetry
- Expected TRL range + demonstrator environments
- Draft consortium roles so we can align WP ownership, deliverables, and budget share