

TECHNOLOGY PARTNER AGREEMENT

Template Version: 1.0 | Last Updated: August 2026

1. PARTNER DETAILS

Partner Name	[INSERT]
Company Registration	[INSERT]
Product/Service Name	[INSERT]
Technical Lead	[INSERT]
Email	[INSERT]
Integration Type	[REST API / Webhooks / MCP Server / Custom]
Agreement Start Date	[INSERT]
Agreement End Date	[INSERT: Typically 24 months]

2. PROGRAM OVERVIEW

Program Type: Technology Partner **Program Code:** TECH

Unicis Tech OÜ (“Unicis”) engages [Partner Name] (“Partner”) as a Technology Partner under the Unicis Partner Programme. As a Technology Partner, you integrate your product with Unicis via our open REST API, build connectors, develop automations, or create compliance workflows that extend the Unicis platform.

3. INTEGRATION SCOPE

3.1 Integration Type

Select integration method(s):

- ☐ REST API (REST calls to/from Unicis)
- ☐ Webhooks (Event-driven notifications)
- ☐ MCP Server (Model Context Protocol - AI integration)
- ☐ Custom Integration (specify: [INSERT])

3.2 Use Cases

Describe primary use cases for the integration:

- [INSERT: e.g., “Automated SBOM ingestion from Snyk”, “Jira issue to Unicis control mapping”]
- [INSERT]
- [INSERT]

3.3 API Access Level

Partner is granted access to the following Unicis APIs:

- ☐ Read-only (read controls, frameworks, compliance data)

- ☐ Write/Create (create tasks, risks, assessments)
- ☐ Admin (manage users, teams, organization settings)
- ☐ Webhook (receive notifications on data changes)

Note: MCP Server access allows AI models to interact with Unicis tools.

4. TECHNICAL REQUIREMENTS

4.1 API Documentation

Unicis provides:

- Full OpenAPI 3.0 specification
- Code examples (cURL, Python, JavaScript, Go)
- Rate limits: [INSERT: e.g., 100 req/min, 10,000 req/day]
- Sandbox environment for testing
- API v1 & v2 support (v1 deprecated after [DATE])

4.2 Security Requirements

Partner's integration must:

- Use OAuth 2.0 or API keys for authentication
- Encrypt all data in transit (HTTPS/TLS 1.2+)
- Implement rate limiting to avoid abuse
- Handle error responses gracefully
- Store API credentials securely (never in client-side code)
- Comply with OWASP Top 10 security standards

4.3 Data Handling

Partner agrees to:

- Not cache customer data longer than [INSERT: e.g., 24 hours]
- Encrypt data at rest if stored
- Delete data within 30 days of customer request
- Not share customer data with third parties
- Execute Unicis Data Processing Agreement (DPA)

5. GO-TO-MARKET & LISTING

5.1 Integration Directory

Upon launch, Partner's integration will be listed in **Unicis Integration Directory** with:

- Integration name & description
- Logo & screenshots
- Use case overview

- Link to Partner's documentation
- Star rating (user reviews)

Listing Criteria:

- Integration is production-ready
- Documentation is complete
- At least one customer reference (optional)

5.2 Co-Marketing Opportunities

Unicis supports Technology Partners through:

- Blog post featuring the integration ("Unicis + [Partner] Integration")
- Social media announcement
- Joint webinar/demo session
- Co-branded case study (if customer agrees)
- Shared booth at trade events

5.3 Revenue Share

Model: Co-sell arrangement (case-by-case)

For deals involving both Unicis AND Partner's platform:

- Partner receives [INSERT: 10-20%] commission on referred Unicis deals
- Unicis receives reciprocal terms for referred Partner deals

6. PARTNER RESPONSIBILITIES

- Maintain API integration (fix bugs, handle deprecations)
- Provide support to end-users on integration issues
- Test integration against latest Unicis API versions
- Publish integration on Partner's marketplace/app store
- Respond to Unicis within 48h on critical issues
- Update integration when API changes (6 month notice given)
- Maintain documentation & setup guides

7. UNICIS RESPONSIBILITIES

- Provide stable, documented REST API
- Maintain 99.5% API uptime (SLA)
- Provide 30-day deprecation notice for API changes
- Offer sandbox environment for testing
- List integration in public directory
- Provide co-marketing support
- Assign technical partner manager
- Early access to new API features (optional beta program)

8. EARLY ACCESS & BETA FEATURES

8.1 Beta Program

Technology Partners may request early access to:

- New API endpoints & methods
- Upcoming features & frameworks
- Performance improvements

Requirements:

- Sign beta NDA
- Provide feedback to Unicis
- Report bugs found during testing

8.2 API Versioning

- Current stable: [INSERT: e.g., v2]
- Previous stable: [INSERT: e.g., v1] (deprecated [DATE], sunset [DATE])
- Beta: [INSERT: e.g., v3-beta]

9. SUPPORT & ESCALATION

Issue Type	Response Time	Contact
Critical (API down)	2 hours	partners@unicis.tech
High (Integration broken)	24 hours	partners@unicis.tech
Medium (Bug/feature question)	48 hours	partners@unicis.tech
Low (Documentation)	1 week	partners@unicis.tech

10. INTELLECTUAL PROPERTY

- Partner retains IP rights to Partner's integration code
- Unicis retains IP rights to REST API, webhooks, MCP server
- Neither party may reverse-engineer the other's technology
- Partner may not claim to “own” Unicis API
- Partner may market integration as “Built for Unicis” (with approval)

11. COMPLIANCE & DATA PROTECTION

Partner agrees to:

- Comply with GDPR, CCPA, and local data protection laws
- Execute Unicis Data Processing Agreement (DPA)
- Implement security standards (OWASP, NIST CSF minimum)
- Report security incidents within 24 hours
- Pass annual security audit or SOC 2 attestation (recommended)

12. TERMINATION & TRANSITION

12.1 Termination

Either party may terminate with 60 days written notice.

12.2 Post-Termination

- API access revoked immediately upon termination
- Partner's integration will be removed from directory
- Customer data exported in standard format within 30 days
- Partner may retain documentation of completed integrations

13. MCP SERVER SPECIFIC TERMS

(If applicable)

13.1 MCP Server Registration

Partner's MCP server will be listed in Unicis MCP registry for AI model access.

13.2 Rate Limits & Cost

- MCP calls are rate-limited to [INSERT: e.g., 1000/day] per user
- Partner is responsible for any infrastructure costs
- Unicis provides monitoring dashboard for usage

13.3 AI Safety

Partner agrees:

- MCP server will not output harmful, malicious, or confidential content
- Partner will implement appropriate access controls
- Partner will monitor for abuse and report to Unicis

14. SIGNATURE & ACCEPTANCE

Partner Name	
Authorized Signatory	
Title	
Date	
Unicis Representative	
Date	

15. NOTES & SPECIAL TERMS

[INSERT ANY CUSTOM API ACCESS LEVELS, REVENUE SHARE TERMS, TERRITORY RESTRICTIONS, OR SPECIAL ARRANGEMENTS]

—

Integration Launch Checklist:

- ☐ API documentation complete
- ☐ Integration tested in sandbox
- ☐ Security audit passed
- ☐ DPA executed
- ☐ Production-ready demo prepared
- ☐ Customer documentation written
- ☐ Support plan defined

—

Document Status: Draft | **Last Reviewed:** [DATE]

From:
<https://handbook.unicis.tech/> - **Unicis Handbook**

Permanent link:
<https://handbook.unicis.tech/partnerships/templates/technology-partner-agreement>

Last update: **18.08.2026 10:58**