# Third-Party & Contractor Infrastructure Security (TPSRM)

This page defines how Unicis monitors and controls infrastructure and tooling introduced by contractors, freelancers, and external partners. It applies to anyone outside the core team who introduces, manages, or accesses Unicis systems on our behalf.

## Scope

This policy applies to any contractor, freelancer, or external partner who:

- Introduces a new tool, SaaS service, or cloud resource on behalf of Unicis
- Has access to Unicis infrastructure, code repositories, or production data
- Deploys, configures, or manages any component in a Unicis environment
- Handles Unicis customer or operational data as part of their engagement

## Approval Before Introduction

No contractor may introduce a new tool, integration, or infrastructure component without completing all of the following steps:

1. Complete the Vendor Questionnaire for the proposed tool or service
2. Obtain written approval from the CEO (Predrag) via Matrix message or email
3. Add the approved tool to Tech Stack Applications with the contractor's name and date noted
4. Document the business justification in the relevant OpenProject task

Unapproved tools must not be used for any Unicis work, even temporarily.

## Access Controls

- All contractor access follows the principle of **least privilege** — only the minimum permissions required for the task
- Accounts are created with a **defined expiry date**, not to exceed the end of the engagement (maximum 6 weeks unless formally renewed in writing by the CEO)
- Contractors do **not** receive production database credentials unless explicitly approved by the CEO (Predrag) in writing
- Contractors do **not** use personal cloud accounts (Google Drive, Dropbox, personal GitHub, etc.) for any Unicis-related work or data
- All GitLab and infrastructure access is reviewed monthly by the CEO (Predrag)

## Infrastructure Monitoring

- All infrastructure changes introduced by contractors must be tracked in OpenProject under the relevant project or task
- Contractors must not make changes outside the agreed scope without prior written approval from the CEO (Predrag)
- The SOC Plan covers monthly security reviews, which include a check for unexpected infrastructure or

access
- Any tool or service accessible from the internet that a contractor introduces must be listed in the Subprocessors & Infrastructure Overview

## Contractor Offboarding

When a contractor engagement ends, the following must be completed **within 24 hours**:

1. Revoke access to: GitLab, Nextcloud, Element/Matrix, OpenProject, and any other tool they were granted
2. Review and archive any infrastructure, repositories, or configurations they owned or managed
3. Confirm no Unicis data remains in personal accounts or personal cloud storage
4. Update Tech Stack Applications if any tools they introduced are being retired
5. Log the offboarding completion in the relevant OpenProject task

See also Departure Communication for the full offboarding checklist.

## Responsibility

| Role | Responsibility |
|---|---|
| **CEO (Predrag)** | Approves all contractor tool and access requests; reviews all infrastructure changes; performs monthly access review across all tools |
| **Contractor** | Responsible for complying with this policy and proactively disclosing any tools or services used |

## Related Pages

- Vendor Questionnaires
- Trusted Subprocessors and Infrastructure Overview
- IT Security Policy
- SOC Plan
- Contractor Hiring Guidelines
- Tech Stack Applications

*Last reviewed: June 2026 — Predrag*

security, contractor, third-party, infrastructure, risk, compliance, tpsrm