Minimum Viable Secure Product (MVSP) Implementation Overview

This document outlines how the Unicis platform implements the MVSP (Minimum Viable Secure Product) controls across key domains including business, application design, implementation, and operations.

Unicis is a privacy-focused, open-source platform designed for secure digital collaboration and communication. It adheres to modern cybersecurity standards through built-in security features, open-core governance, and integration with trusted open-source tools. The implementation strategy leverages the Unicis Cybersecurity Controls module for audit tracking, and integrates with tools like IRIS (for incident management), Wazuh (for SIEM and vulnerability management), and the Unicis Awareness module (for security training and compliance).

This table provides a breakdown of how each MVSP requirement is met using Unicis-native tools or vetted third-party open-source components.

MVSP Area	SP Area Control			Implementation				
Business Controls	External vulnerability reports		Reports accepted via `security.txt` page, tracked in IRIS, linked to Git issues.					
Business Controls	Customer testing			Clients may request sandbox environments; tests are isolated and monitored. Guidelines provided.				
Business Controls	Self-assessment		nt	Annual MVSP audit tracked in Unicis Cybersecurity Controls module. Responsible roles managed in OpenProject; evidence stored in Nextcloud.				
Business Controls	External testing		g	Annual pentests performed. Findings tracked in Unicis Cybersecurity Controls and resolved in OpenProject. Results referenced in IRIS.				
Business Controls	Training			Awareness and secure dev training delivered via Unicis Awareness Module. Participation tracked per user.				
Business Controls	Compliance		ISO 27001, GDPR, MVSP mapped in Unicis Cybersecurity Controls . Regional segmentation enforced via Mautic.					
Business Controls		ng	All incidents logged and resolved in IRIS. Escalation flows managed with SLAs (e.g. 72h for breaches). n8n used for automated notifications.					
Business Controls	Data handling			End-of-life handling logged in OpenProject. Data deletion procedures follow checklist in Unicis Cybersecurity Controls .				
Application Design Controls		Single Sign-On (SS		SSO)		e.g., Keycloak) enforced across platform. Self-hosted can connect to external IdP.		
Application Design Controls		Multi-Factor Authentication (M		ЛFA)	MFA required for all critical systems using TOTP or YubiKey Enforced at SSO level.			
Application Design Controls		HTTPS-only			HTTPS enforced sitewide with HSTS; Let's Encrypt certs autorenewed.			
Application Design Controls		Security Headers		i	CSP, X-Frame, HSTS, etc. enforced by server and app; tested on CI/CD deploys.			
Application Design Controls		Password policy			SSO enforces 12+ character passwords; passphrases supported; Zxcvbn used. No passwords stored locally.			
Application Design Controls		Security libraries		Shared internal security modules reviewed periodically.				
Application Design Controls		Dependency patching		Monitored via Dependabot/Renovate. Wazuh flags CVEs. Fix SLA: <72h for critical.				
Application Design Lo		_ogging		Wazuh collects auth and admin logs. Logs retained ≥180 days. Alerts forwarded to IRIS.				
Application Design Controls		Encrypt	ption		AES-256 at rest, TLS 1.3 in transit. Secrets handled securely; API keys scoped and rotated.			
Application Implementation Controls		on	List of data			Data types (PII, etc.) documented in EspoCRM. Models versioned in Git and listed in Nextcloud.		

Last update:	15.06.2025	22:05
--------------	------------	-------

Application Implement Controls	Data flow di	iagrams	Maintained in diagrams.net, stored in Nextcloud, referenced in Unicis Cybersecurity Controls .		
Application Implement Controls	Vulnerability prevention	y	Devs trained on OWASP Top 10 via Unicis Awareness. Code reviews require static scans.		
Application Implement Controls			IRIS and Wazuh alert triage with OpenProject task linkage. Critical fixes in <72h.		
Application Implementation Controls				CI/CD pipelines enforce clean builds, no hardcoded secrets. Provenance signed and tracked.	
Operational Controls	Physical ac	cess	Data centers via Hetzner/Scaleway (ISO 27001). On-prem setups provided with compliance templates.		
Operational Controls	Logical acc	ess	RBAC + SSO + MFA enforced. Access reviews quarterly using Unicis Cybersecurity Controls . Inactive accounts deactivated by n8n.		
Operational Controls	Sub-proces	sors	Public DPA maintained. Sub-processors reviewed annually and stored in Nextcloud. Linked to Unicis Cybersecurity Controls .		
TONEIALIONAL CONTINIC	Backup & D Recovery	isaster	Daily encrypted backups, restore tests monthly. Logged in OpenProject, tracked in audit module.		

From:

https://handbook.unicis.tech/ - Unicis Handbook

Permanent link:

https://handbook.unicis.tech/pub/trust_center/controls?rev=1750025101

Last update: **15.06.2025 22:05**