V-IMS

Terms of service for the VIMS platform

Version: 1.3 · Last updated: 2026-10-01

These terms govern the use of the VIMS platform delivered as an online service at app.v-ims.pl and of the informational website v-ims.pl. The document is addressed to businesses and organizations using the system in the course of their professional activity.

1. Definitions

- Provider — Vesta Usługi i Szkolenia Marcin Makowski, ul. Wrzosowa 33, 84-300 Lębork, Poland, VAT ID (NIP) 841-161-18-09, Polish business registry number (REGON) 771244908, contact address: kontakt@v-ims.pl.
- VIMS platform (System) — the Varilo Integrated Management System software made available by the Provider as a browser-based service at app.v-ims.pl.
- Website — the informational site at v-ims.pl together with its subpages.
- Customer — a business, organizational unit or other entity entering into an agreement with the Provider for the use of the System in the course of its activity.
- User — a natural person granted access to the System by the Customer within its Organization (employee, contractor, subcontractor).
- Organization — the Customer's separated data space in the System, containing its registers, documents and tasks.
- Account — an individual set of User data enabling access to the System after authentication.
- Customer Data — all data and content entered into the System by the Customer or its Users, including incident registers, risk assessments, documents and attachments.
- Agreement — the agreement for the provision of access to the System concluded between the Provider and the Customer, of which these terms form an integral part.
- Terms — this document.

2. General provisions and scope of the service

The Provider grants the Customer access to the System through a web browser, without the need to install software on the Customer's infrastructure. The service covers hosting and maintenance of the System, its updates and support handling to the extent described in these Terms and in the Agreement.

The System supports the management of occupational safety, environmental protection, fire safety, quality and compliance processes. The System does not replace statutory obligations or decisions made by the Customer's own functions, and it does not constitute legal advice or occupational safety consultancy.

The Lone Worker module is provided in beta as a tool supporting lone-working safety procedures. It is not a medical device, rescue system or monitoring service provided by an alarm receiving centre, and it does not replace the Customer's supervision, organizational procedures or the need to call the emergency services.

The effectiveness of Lone Worker notifications depends on factors beyond the Provider's control, including cellular or Wi-Fi coverage and quality, battery level, GPS signal availability, permissions granted to the application by the User, power-saving settings and background-operation restrictions imposed by the device manufacturer. The Customer must account for these limitations in its own lone-working procedure and provide a fallback solution if the module is unavailable.

Monitoring in the Lone Worker module starts only through the User's informed action after information about the scope of data collected has been displayed, and ends when the session is disarmed. The Customer is responsible for informing Users about the monitoring rules and for designating emergency contacts and an alarm response procedure.

The service is addressed to entities conducting business or professional activity. The Agreement is not a consumer contract and the System is used in connection with the Customer's activity.

If the Customer is a natural person entering into an Agreement directly connected with their business activity, but the Agreement is not of a professional nature for that person, these Terms do not exclude rights granted by mandatory law. In particular, limitations of liability and exclusion of statutory warranty apply only to the extent permitted by law.

The scope of modules made available, the number of Users and the commercial terms are agreed individually and confirmed in the Agreement, an offer or an order accepted by the Provider.

3. Technical requirements

Using the System requires a device with internet access, a current web browser with JavaScript and browser storage enabled, and an active e-mail address assigned to the Account.

Signing in requires two-step authentication. After the e-mail address and password are provided, the System sends a one-time code to the Account's e-mail address. The code is valid for ten minutes, the number of attempts is limited, and a new code can be requested after a short cooldown. A User may mark a device as trusted, which reduces how often the code is required for a defined period.

Disabling essential cookies or local storage in the browser prevents signing in and using the service.

4. Conclusion of the Agreement, registration and access

The Agreement is concluded when the Provider confirms that an Organization has been made available to the Customer — on the basis of a signed Agreement, an accepted order or an accepted offer, depending on the agreed mode of cooperation.

Registering an Account requires acceptance of these Terms and acknowledgement of the personal data processing information. The acceptance is recorded in the System together with the document version and date.

Creating an Account does not automatically grant access to Organization data. Joining an Organization requires approval by its owner or administrator. Until approval is granted, the User has no access to operational data.

The Customer is responsible for granting and revoking permissions for its Users, including prompt revocation of access for individuals who have ended their cooperation with the Customer.

5. Rules for using the System

The Customer and its Users must use the System in accordance with the law, these Terms and the intended purpose of the service, protect their authentication credentials and refrain from sharing Accounts with third parties. Each Account is assigned to one natural person.

It is prohibited to interfere with the operation of the System, in particular to attempt unauthorized access to data of other Organizations, to circumvent access controls, to perform automated bulk data extraction, or to conduct load or security testing without the Provider's prior written consent.

The Customer undertakes not to enter unlawful content into the System, nor data exceeding the purpose of the processes carried out in it. The Customer decides independently on the scope of personal data entered into the System and is responsible for its adequacy.

The Provider may temporarily restrict access to a User's Account where there is a justified suspicion of a security breach, informing the Customer without undue delay.

VIMS Intelligence functions using artificial intelligence are supportive only: they assist with technical documentation, data imports and draft record entries. Output is marked as requiring verification and does not become a final record or a decision producing legal effects without approval by an authorized User.

The occupational risk assessment creator and other content generators produce draft material only. Output becomes an effective document only after it has been reviewed and approved by an authorized

User, in particular by the Customer's occupational health and safety function, which remains responsible for the content of the documentation.

Customer Data included in an AI request and generated responses are not used by the Provider to train, fine-tune or improve public or generally available AI models. The Provider uses API access intended for business processing and requires model providers not to use request or response content to train their models, subject to the provider's statutory obligations.

In BYOK (Bring Your Own Key) mode, the Customer selects the model provider and uses its own API key. Processing by that provider is governed by the agreement between the Customer and the provider. The Customer is responsible for privacy settings, the legal basis for the transfer and ensuring that the selected provider meets its requirements.

The Customer should limit AI requests to data necessary for the task and should not enter special-category data or confidential information unless necessary and appropriately safeguarded. Availability and the option to disable AI functions depend on the purchased plan and Organization configuration.

6. Fees, invoices and payments

Use of the System is subject to fees agreed with the Customer in the Agreement, an offer or an order. Value added tax at the applicable rate is added to the agreed amounts.

The amount of fees, the scope of plans, prices of individual modules and add-ons, and the technical limits are set out in the V-IMS licensing, plans and limits document (Edition 3.3), which forms Annex 1 to these Terms. Employee, account and resource limits apply to the whole organisation across all sites; an extra site does not increase them. It is published at v-ims.pl/en/pricing and available for download in PDF and DOCX. All amounts in the price list are net amounts.

The price list sets out regular prices and launch-offer prices. The launch offer covers the first 30 workplaces and the first 20 OHS firms that conclude the Agreement and reduces the plan price by approximately 30% against the regular price for 12 months from subscription start. After that period the Client keeps the launch price with annual prepayment, or receives a loyalty discount of 15–20% off the regular price with monthly billing. The discount does not apply to single modules, V-IMS Core, site surcharges or add-ons, in particular the Lone Worker module and AI task top-ups. A new Client may use a free 30-day trial without providing payment card details.

Artificial intelligence functions are billed against the monthly task allowance assigned to the plan. Any unused monthly allowance does not carry over to the next billing period, while separately purchased top-ups remain valid until used. Use of the Customer's own model-provider key in BYOK mode does not reduce the allowance.

The Lone Worker module is billed according to the number of devices monitored concurrently. Disarming a session releases capacity for another User. If the purchased limit is reached, another session cannot be started until capacity is released or the plan is extended.

Settlement is based on an invoice issued by the Provider. Invoices are delivered electronically to the billing e-mail address indicated by the Customer, to which the Customer consents by concluding the Agreement.

Payments should be made to the Bank Erste account: 79 1090 1102 0000 0001 3149 8962, unless the invoice or an individual agreement between the parties specifies another account. Access to the System for the paid billing period is activated or maintained once payment has been credited.

Where payment is delayed by more than fourteen days, the Provider may suspend access to the System until the arrears are settled, after sending a prior reminder to the Customer's e-mail address. Suspension of access does not mean deletion of Customer Data.

The Provider may change the fees for a subsequent billing period, informing the Customer at least thirty days before the planned change. A Customer who does not accept the change may terminate the Agreement as described in these Terms.

7. Term, termination and end of cooperation

The Agreement is concluded for an indefinite period, unless the parties agree on a fixed term.

Either party may terminate the Agreement with one month's notice, effective at the end of the calendar month following the month in which notice was given. Notice must be given in writing or sent to the other party's e-mail address.

The Provider may terminate the Agreement with immediate effect in the event of a gross breach of these Terms by the Customer or its Users, in particular actions endangering the security of other Organizations' data, after an unsuccessful request to cease the breach.

Before the Agreement ends, the Customer may download an archive of its Organization data directly from the System. This right is available to the Organization owner and administrator, and each export is recorded in the security event log.

After the Agreement ends, Customer Data is deleted or returned in the manner and within the period set out in the data processing agreement. The Provider does not retain data as leverage for renewing the cooperation.

At the Customer's request or after the Agreement ends, the Organization may be permanently deleted. Deletion is preceded by suspension of the Organization and requires additional confirmation by an authorized person on the Provider's side. Permanent deletion covers the Organization's operational data, attachments and backups, is irreversible and is recorded in the security event log. Accounts of Users belonging exclusively to the deleted Organization are deleted with it.

A User may independently request deletion of their Account at app.v-ims.pl/usun-konto. Account deletion does not erase data that the Customer, as controller, is required to retain under applicable law.

8. Availability, maintenance and changes to the System

The Provider aims to keep the System continuously available, subject to interruptions resulting from maintenance, updates and events beyond the Provider's control, including failures at infrastructure and telecommunications suppliers.

The Provider does not publish a guaranteed availability level as a commercial standard. Where the Customer requires a contractual commitment in this respect, its terms are agreed individually in the Agreement.

The Provider may develop the System, add and modify functions and withdraw functions replaced by newer solutions. Changes may not materially reduce the agreed scope of the service without informing the Customer at least thirty days in advance.

9. Intellectual property and Customer Data

All rights to the System, including its software, interface, documentation, the VIMS and Varilo trademarks and materials published on the Website, remain with the Provider or the entities from which the Provider obtained the relevant rights.

For the term of the Agreement the Customer receives a non-exclusive, non-transferable right to use the System to the extent necessary to run its own processes. This right does not include copying, decompiling, resale or making the System available to third parties, except for serving the Customer's own clients under the model provided for occupational safety service providers, where such scope has been agreed in the Agreement.

Customer Data remains the property of the Customer. The Provider uses it solely to deliver the service, handle support requests and meet statutory obligations.

The Provider may use aggregated, anonymized technical information about how the System is used in order to develop it, provided that such information does not allow identification of the Customer or of natural persons.

10. Liability

The Provider is responsible for the proper provision of the service in accordance with these Terms and the Agreement. The Provider is not responsible for the consequences of decisions taken by the

Customer on the basis of data held in the System, nor for the compliance of the Customer's processes with the law.

The Provider is not liable for the consequences of authentication credentials being disclosed to unauthorized persons by the Customer or a User, for the content and scope of data entered into the System, or for lack of access caused by circumstances attributable to the Customer, including its network and device configuration.

The Provider's liability for damage caused to the Customer is limited to the fees paid by the Customer for the twelve months preceding the event giving rise to the claim. This limitation does not apply to damage caused intentionally or where limitation of liability is not permitted by law.

The parties exclude liability for lost profits to the extent permitted by law.

In relations with Customers acting as businesses, the parties exclude the Provider's liability under the statutory warranty for defects pursuant to Art. 558 § 1 of the Polish Civil Code to the fullest extent permitted by law. This exclusion does not apply where the Provider fraudulently concealed a defect or where exclusion is otherwise prohibited by mandatory law.

11. Security and personal data protection

The Provider applies the technical and organizational measures described in the Privacy policy and in the data processing agreement, in particular database-level isolation of each Organization's data, encryption in transit, access control and a security event log.

With regard to personal data entered into the System, the Customer acts as controller and the Provider as processor. The processing conditions are set out in the data processing agreement annexed to the Agreement.

System data is processed in infrastructure located within the European Economic Area.

12. Complaints and incident reporting

Complaints and reports of malfunctions should be sent to kontakt@v-ims.pl, indicating the Organization, a description of the problem, when it occurred and, where possible, a screenshot.

The Provider handles a report within fourteen days of receipt and, in matters requiring further investigation, informs the Customer of the expected resolution date.

Reports concerning critical unavailability of the System are handled first, regardless of the order of receipt.

13. Changes to these Terms

The Provider may amend these Terms in the event of changes in the law, changes to the scope or manner of providing the service, the introduction of new System functions, or organizational changes at the Provider.

The Customer is informed of amendments by e-mail to the address assigned to the Organization or by a notice in the System, at least fourteen days before the changes take effect.

If the Customer does not accept the amendments, it may terminate the Agreement with one month's notice. Continued use of the System after the changes take effect constitutes their acceptance.

14. Final provisions

These Terms and the Agreement are governed by Polish law. Disputes arising from the Agreement are submitted to the court having jurisdiction over the Provider's registered seat.

If any provision of these Terms is invalid, the remaining provisions remain in force and the parties will replace the invalid provision with one of similar economic effect.

The relationship between the parties is governed jointly by: these Terms, the Privacy and cookie policy, and the data processing agreement.

Version 1.3 of these Terms applies from 2026-10-01. The current version is published at v-ims.pl/en/terms.