CLEARHOLD

Registration Number: 2026/035423/07
Strategic Capital, Infrastructure & Diversified Group Enterprises
Contact: info@CLEARHOLD.CO.ZA | +27 (0)68 337 6816

VYLER USER OBLIGATIONS AND ACCEPTABLE USE POLICY

Platform: Vyler
Operating company: CLEARHOLD (Pty) Ltd
Company registration number: 2026/035423/07
Website: https://vyler.co.za
Contact: support@vyler.co.za

1. PURPOSE AND APPLICATION

This User Obligations and Acceptable Use Policy establishes the responsibilities and standards of conduct applicable to individuals and businesses accessing or using Vyler.

Vyler facilitates transactions between buyers and sellers through structured transaction agreements, protected-payment arrangements, fulfilment requirements, inspection procedures and dispute-resolution mechanisms.

Every user is responsible for using the Platform honestly, lawfully, securely and in accordance with the terms agreed for each transaction.

This Policy applies to buyers, sellers, business representatives and any other person using the Platform. Where an obligation applies specifically to a buyer, seller or business representative, it applies to that person's role in the relevant transaction.

By registering for, accessing or using Vyler, users agree to comply with this Policy and the applicable Terms and Conditions.

2. ACCURATE INFORMATION AND HONEST REPRESENTATION

Users must provide accurate, complete and current information when registering, completing verification, creating transactions or communicating with other users.

Users must not:

- **Provide false, misleading, fabricated or materially incomplete information.**
- **Impersonate another person or falsely claim to represent a business.**

- **Use another person's identity documents, account credentials or verification results without lawful authority.**
- **Misrepresent their age, identity, business registration, ownership, authority or transaction history.**
- **Submit altered, forged or misleading documents to obtain verification or access to the Platform.**
- **Knowingly conceal information material to a transaction or required verification.**
- **Misrepresent the status, availability, condition, ownership or authenticity of goods or services.**

Users must promptly correct material inaccuracies in their account information and notify Vyler where a change affects an active transaction or the user's ability to fulfil an obligation.

3. IDENTITY VERIFICATION AND BUSINESS VERIFICATION

Users must complete the identity or business verification procedures applicable to their accounts and intended activities.

Verification may be conducted through Didit and may include identity-document verification, facial liveness checks, company-registration checks, beneficial-ownership checks and relevant screening.

Users must:

- **Supply information and documents that genuinely relate to the person or entity being verified.**
- **Participate honestly in required verification procedures.**
- **Provide additional information where reasonably necessary to resolve a verification discrepancy or satisfy a lawful requirement.**
- **Ensure that business information and ownership details supplied are accurate to the best of their knowledge.**
- **Refrain from manipulating, bypassing or attempting to defeat identity-verification or liveness checks.**
- **Refrain from using another person's identity or attempting to create an account under a false identity.**

Vyler may restrict access to relevant features or decline to facilitate a transaction where required verification remains incomplete, fails or raises a legitimate concern.

Any restriction or request for additional information must be handled in accordance with applicable law and the Platform's contractual procedures.

4. ACCOUNT SECURITY AND ACCESS

Users are responsible for taking reasonable precautions to protect their accounts and authentication credentials.

Users must:

- **Keep passwords, authentication codes and other security credentials confidential.**
- **Avoid knowingly allowing unauthorised persons to access their accounts.**
- **Notify Vyler promptly if they suspect account compromise, unauthorised access or identity misuse.**
- **Use the Platform only through accounts they are authorised to access.**
- **Avoid attempts to bypass access controls, exploit vulnerabilities or interfere with another user's account.**

Users must not sell, rent, transfer or otherwise provide access to their accounts to another person except where the Platform expressly supports the relevant arrangement.

A user must not continue using an account in a manner that misrepresents who is conducting a transaction.

5. BUYER OBLIGATIONS

A buyer is responsible for understanding and complying with the transaction terms accepted before committing to a transaction.

Buyers must:

- **Review the description of the goods or services, transaction value, milestones, delivery arrangements and applicable inspection requirements.**
- **Ensure that the transaction details reflect the intended purchase before confirming the transaction.**
- **Provide accurate delivery addresses, collection details and other information required for fulfilment.**
- **Make the agreed payment through the applicable payment or protected-funds process.**
- **Cooperate reasonably with delivery, inspection, verification and dispute procedures.**
- **Inspect delivered goods or completed services within the agreed inspection period.**
- **Raise genuine concerns within the applicable timeframe and provide a reasonably clear explanation of the alleged defect, discrepancy or non-fulfilment.**
- **Provide relevant supporting evidence where reasonably available.**
- **Avoid making false claims about delivery, quality, authenticity, condition or fulfilment.**
- **Avoid intentionally obstructing a transaction to obtain an unjustified refund or prevent a legitimate payment release.**

A buyer must not assume that funds will automatically be refunded merely because they change their mind, become dissatisfied for an unrelated reason or wish to withdraw from an otherwise binding transaction.

Cancellation and refund rights remain subject to the transaction terms and applicable law, including any mandatory consumer rights.

6. SELLER OBLIGATIONS

A seller is responsible for supplying the goods or services agreed to in the transaction.

Sellers must:

- **Accurately describe the goods or services being offered.**
- **Disclose material defects, limitations, exclusions or other facts that could reasonably affect the buyer's decision.**
- **Ensure that they have the legal right and authority to sell or provide the relevant goods or services.**
- **Ensure that the goods or services supplied correspond materially with the agreed transaction description.**
- **Meet the agreed delivery dates, milestones and fulfilment requirements, subject to any permitted changes or circumstances recognised under the applicable terms.**
- **Provide genuine delivery records, completion evidence and supporting documentation where required.**
- **Cooperate reasonably with inspection and dispute-resolution procedures.**
- **Communicate material delays, supply problems or other circumstances affecting fulfilment promptly.**
- **Refrain from misrepresenting the authenticity, condition, ownership, origin or functionality of goods.**
- **Refrain from falsely claiming that goods have been dispatched, delivered, installed or accepted.**
- **Avoid deliberately circumventing the agreed transaction conditions to obtain payment improperly.**

A seller must not knowingly supply counterfeit, stolen, unlawfully obtained or prohibited goods or provide unlawful services.

Where a seller acts on behalf of a business, the seller must have the authority necessary to make the relevant representations and enter into the transaction.

7. TRANSACTION TERMS AND AGREEMENTS

Users must honour the terms they accept for each transaction.

These may include:

- The description and quantity of goods or services.
- The agreed transaction price.
- Delivery, collection or service-completion arrangements.
- Milestone requirements and deadlines.
- Inspection periods and acceptance criteria.
- Required documentation or evidence.
- Agreed cancellation and refund conditions.
- Any other conditions expressly incorporated into the transaction.

Users must not knowingly misrepresent the agreed terms or attempt to alter transaction records improperly.

Changes to a transaction must be made through the applicable Platform process and accepted by the relevant parties where required.

A user must not assume that an informal message, verbal understanding or unilateral change automatically overrides the recorded transaction terms.

Nothing in this section excludes any variation, remedy or right that may be available under applicable law.

8. PAYMENT AND PROTECTED-FUNDS REQUIREMENTS

Users must follow the payment instructions and transaction procedures presented through Vyler.

Users must not:

- Falsely claim to have paid when payment has not been completed.
- Submit fabricated payment confirmations or altered proof of payment.
- Knowingly use stolen payment credentials or payment methods without lawful authority.
- Attempt to manipulate payment-status records or interfere with the protected-funds process.
- Misrepresent their entitlement to a payment, refund or payout.
- Use the Platform to facilitate unlawful payments or conceal the proceeds of unlawful activity.
- Attempt to obtain duplicate refunds or payments for the same transaction through deception.
- Knowingly engage in collusion designed to misuse the Platform's payment or refund procedures.

Protected funds are handled through the relevant third-party service provider in accordance with the applicable arrangements.

Users must comply with the payment, inspection, fulfilment and dispute conditions applicable to their transactions.

No user may represent that funds have been released, secured or refunded unless that status is supported by the applicable transaction records or provider confirmation.

9. DELIVERY, INSPECTION AND ACCEPTANCE

Buyers and sellers must cooperate with the delivery, inspection and acceptance procedures agreed for a transaction.

Buyers must not deliberately avoid delivery, refuse reasonable access required for agreed inspection or fabricate defects to obtain an unjustified financial advantage.

Sellers must not falsely represent that delivery or fulfilment has occurred or prevent a buyer from exercising applicable inspection rights.

Both parties must:

- **Keep relevant delivery and fulfilment information accurate.**
- **Preserve reasonably available supporting evidence.**
- **Notify the other party of material problems affecting fulfilment.**
- **Observe applicable deadlines.**
- **Use the agreed channels to communicate material concerns.**

Where a transaction includes multiple milestones, the parties must comply with the requirements applicable to each milestone.

Failure to respond within an inspection period may result in consequences specified by the transaction terms, but it does not automatically extinguish any non-waivable statutory rights.

10. DISPUTES, COMPLAINTS AND EVIDENCE

Users must act honestly when raising, responding to or participating in a dispute.

A user must not knowingly:

- **Fabricate evidence.**
- **Alter records to misrepresent what occurred.**
- **Submit false allegations to obtain a refund or prevent payment.**
- **Conceal material information in a manner intended to mislead the review process.**
- **Impersonate another party or submit evidence falsely attributed to someone else.**

- **Repeatedly initiate substantially identical disputes in an attempt to manipulate an outcome.**
- **Threaten, harass or intimidate another party to influence a transaction decision.**

Users must provide relevant information reasonably requested through the applicable dispute process, subject to their legal rights and obligations.

Vyler may review relevant transaction records and submitted evidence to administer its own procedures. The handling and determination of protected funds remain subject to the applicable third-party arrangements and the parties' contractual rights.

Submitting a complaint or dispute in good faith is not prohibited merely because the claim is ultimately unsuccessful.

11. PROHIBITED GOODS, SERVICES AND ACTIVITIES

Users must not use Vyler to facilitate unlawful activity or transactions involving goods or services prohibited by applicable law or by the Platform's published restrictions.

Prohibited conduct includes, where applicable:

- **Trading in stolen or unlawfully obtained property.**
- **Selling counterfeit goods while misrepresenting them as genuine.**
- **Fraud, identity theft, payment fraud or impersonation.**
- **Money laundering or attempts to conceal the origin or destination of unlawful funds.**
- **Transactions intended to evade applicable sanctions or legal restrictions.**
- **Offering unlawful services or facilitating criminal conduct.**
- **Exploiting minors or engaging in unlawful exploitation.**
- **Attempting to use Vyler to transfer or conceal proceeds of crime.**
- **Transactions involving prohibited items or services identified in the Platform's applicable rules.**

Vyler may refuse, restrict or suspend transactions that reasonably appear to involve prohibited activity, subject to applicable law and the relevant contractual arrangements.

12. FRAUD PREVENTION AND COMPLIANCE COOPERATION

Users must not knowingly use Vyler to facilitate fraud, financial crime, impersonation or other unlawful conduct.

Where reasonably necessary and lawful, Vyler may conduct or facilitate verification, screening, account reviews, transaction reviews, security checks and compliance assessments.

Users may be required to provide additional information or complete further checks where necessary to resolve a discrepancy, protect an account, investigate suspected misuse or satisfy an applicable legal obligation.

Users must not knowingly obstruct lawful verification or investigation processes, submit deliberately misleading responses or attempt to circumvent relevant controls.

Where suspicious activity is identified, Vyler may take proportionate protective measures, including restricting account access, declining a transaction, requesting further information or referring a matter to the appropriate service provider or competent authority where legally justified.

These measures do not, by themselves, establish that a user has committed an offence.

13. AUDITS AND AUTHORISED REVIEWS

Users acknowledge that relevant account, verification and transaction information may be reviewed where reasonably necessary for legitimate purposes, including:

- **Account-security reviews.**
- **Fraud-prevention investigations.**
- **Transaction-dispute resolution.**
- **Verification of compliance with Platform terms.**
- **Financial-crime prevention and relevant screening.**
- **Authorised internal or external audits.**
- **Compliance with applicable legal or regulatory requirements.**
- **The establishment, exercise or defence of legal claims.**

Access must be limited to relevant information and authorised persons or service providers with a legitimate need to review it.

Such reviews do not grant unrestricted access to all user information and remain subject to applicable privacy and confidentiality requirements.

14. PRIVACY AND INFORMATION HANDLING

Users must respect the privacy and confidentiality of other users.

Users must not:

- **Attempt to access another person's private account or verification information without authorisation.**
- **Use another person's personal information for an unrelated or unlawful purpose.**
- **Publish another user's confidential information without an appropriate lawful basis.**
- **Attempt to obtain identity documents, verification records or payment information they are not authorised to access.**
- **Use information obtained through a transaction to harass, impersonate, defraud or unlawfully target another person.**

Vyler's collection, use, retention and sharing of personal information are governed by its Privacy Policy and applicable law.

15. HARASSMENT, THREATS AND MISUSE OF COMMUNICATIONS

Users must communicate honestly and respectfully when using the Platform.

Users must not use Vyler's communication channels to threaten, harass, intimidate, extort or unlawfully discriminate against another user.

Users must not send malicious links, harmful files, unsolicited fraudulent communications or content intended to compromise another person's account or device.

Vyler may restrict communication features or take other proportionate action where necessary to protect users, maintain security or enforce applicable rules.

16. TECHNICAL MISUSE AND PLATFORM INTEGRITY

Users must not attempt to compromise the security, availability or integrity of Vyler.

Prohibited conduct includes:

- **Unauthorised access to systems, accounts or restricted data.**
- **Attempting to bypass authentication, verification or access controls.**
- **Introducing malicious code or harmful software.**
- **Interfering with the normal operation of the Platform.**
- **Exploiting vulnerabilities without authorisation.**
- **Scraping, extracting or harvesting information in violation of applicable law or Platform restrictions.**
- **Reverse engineering or interfering with protected components except to the extent expressly permitted by applicable law.**

- **Submitting automated requests that materially disrupt the Platform or evade its safeguards.**
- **Manipulating transaction records or attempting to alter system logs without authorisation.**

Users who identify a security vulnerability should report it responsibly through an appropriate contact channel rather than exploit it or access information belonging to others.

17. BUSINESS REPRESENTATIVES AND AUTHORITY

A person using Vyler on behalf of a company or other legal entity represents that they have the necessary authority to act in the relevant capacity.

Business representatives must ensure that information submitted about the entity is accurate and that they do not falsely claim ownership, directorship, beneficial ownership or authority to transact.

Where a user's authority is withdrawn, materially changed or disputed, the user must not continue to represent that they hold authority they no longer possess.

Vyler may request further information or restrict relevant activity where necessary to establish account authority or protect the parties involved.

18. ACCOUNT RESTRICTIONS AND ENFORCEMENT

Where Vyler reasonably believes that a user has breached this Policy, misused the Platform or created a material security, fraud or compliance risk, it may take proportionate action.

Depending on the circumstances, action may include:

- **Requesting clarification or additional verification.**
- **Restricting access to specific features.**
- **Declining or suspending a transaction.**
- **Temporarily restricting an account while a legitimate concern is assessed.**
- **Suspending or terminating access where justified.**
- **Preserving relevant records for dispute resolution, security or lawful compliance purposes.**
- **Referring relevant information to a service provider or competent authority where legally justified.**

Where appropriate and lawful, Vyler may notify the user of the reason for a restriction and provide a channel through which the user can respond or request a review.

Any restriction affecting protected funds remains subject to the applicable third-party arrangements, the relevant transaction terms and applicable law. Vyler does not claim authority over funds held by another provider beyond the authority established by the applicable arrangements.

Enforcement action must not be used to unlawfully deprive a user of their rights or avoid legitimate obligations.

19. CONSEQUENCES OF BREACH

A breach of this Policy may result in contractual remedies, account restrictions, transaction-related measures or other lawful action appropriate to the circumstances.

Where a user's conduct causes loss, damage, third-party claims or reasonable investigation costs, responsibility will be determined under the applicable contractual terms and law.

Nothing in this Policy creates an automatic right for Vyler to impose arbitrary penalties, retain funds without authority or exclude liability that cannot lawfully be excluded.

20. REPORTING SUSPECTED MISUSE

Users who suspect fraud, account compromise, impersonation or other misuse should contact Vyler promptly.

Reports should include relevant transaction references and a clear description of the concern. Users should provide supporting evidence where reasonably available and lawful to share.

Users must not knowingly make false reports or use the reporting process to harass another user or obtain an improper financial advantage.

Reports will be handled according to the nature of the concern, the information available, the applicable procedures and any relevant legal obligations.

21. CHANGES TO THIS POLICY

Vyler may update this Policy to reflect changes in the Platform, transaction workflows, security measures, service providers or applicable legal requirements.

The latest version will be made available through the Platform or relevant website.

Where notice or consent is required by law or contract, Vyler will take the appropriate steps.

22. GOVERNING LAW

This Policy is governed by the laws of the Republic of South Africa, subject to applicable legal requirements and the rights of users under relevant legislation.

Nothing in this Policy is intended to exclude consumer protections, privacy rights or other statutory rights that cannot lawfully be excluded or limited.

23. CONTACT INFORMATION

For questions about this Policy, account obligations or suspected misuse of Vyler, contact:

CLEARHOLD (Pty) Ltd
Website: https://vyler.co.za
Email: support@vyler.co.za
Company registration number: 2026/035423/07

By using Vyler, users agree to comply with the obligations applicable to their use of the Platform, subject to the terms of the applicable agreement and South African law.

End of User Obligations and Acceptable Use Policy