CUSTOMER POLICY

Acceptable Use Policy

For Duewarden, operated by TECBINO (Pty) Ltd

Entity	TECBINO (Pty) Ltd
Document date	27 September 2026
Status	Effective

Effective date: 27 September 2026

1. Purpose and scope

This Acceptable Use Policy (AUP) forms part of the Duewarden Terms of Service and applies to customers, workspace administrators, users, API or integration clients, and anyone using access provided through a Duewarden account.

2. Lawful and authorised use

Duewarden may be used only for lawful business purposes and within the permissions granted by the customer, the selected plan and applicable law. Customers remain responsible for ensuring that they are authorised to collect, upload and use the data they place in Duewarden.

3. Prohibited activity

- Accessing or attempting to access another customer's workspace, account, credentials, API keys, tokens or data without authorisation.
- Probing, scanning, exploiting, reverse engineering or testing TECBINO production systems without prior written authorisation and an agreed scope.
- Uploading malware, ransomware, credential theft tooling, destructive code or other harmful content.
- Interfering with service availability, deliberately exhausting resources, bypassing rate / plan limits or using automated activity that materially degrades the Service.
- Using Duewarden for fraud, unlawful surveillance, harassment, impersonation, intellectual-property infringement, unlawful direct marketing, or other illegal conduct.
- Uploading personal information or confidential information that the customer is not lawfully authorised to process.
- Using the Service to store secrets or high-risk regulated data where the Service is not designed or contractually approved for that purpose.
- Reselling, sublicensing or making the Service available as a competing hosted service unless TECBINO has agreed in writing.

4. Data quality and compliance records

Users must not represent Duewarden records, reminders, certificates or status indicators as proof of calibration, safety, statutory compliance or technical fitness unless the underlying evidence supports that conclusion. Duewarden assists with record management; it does not replace competent technical verification.

5. Security research and vulnerability reporting

A customer may test its own devices, data and integrations where it has authority and the testing cannot affect TECBINO or another customer. Testing TECBINO production infrastructure or shared services requires prior written permission. Report suspected vulnerabilities to support_duewarden@tecbino.co.za and avoid accessing more data than is necessary to demonstrate the issue.

6. Enforcement

TECBINO may investigate suspected breaches and may restrict or suspend access where reasonably necessary to protect the Service, users or legal compliance. Where practicable and safe, TECBINO will notify the customer and allow a reasonable opportunity to remedy the issue. Serious, malicious or unlawful activity may result in immediate suspension or termination and may be reported where law requires.

7. Contact

Report abuse or security concerns to support_duewarden@tecbino.co.za. Do not send passwords, full payment-card details or unnecessary personal information in a report.