

# DecenTGigs: Anti-Fraud and Security Policy

**Effective Date:** 21 November 2025

This policy outlines the measures and prohibitions against fraudulent activity on the DecenTGigs decentralized platform.

## 1. Decentralized Identity (DID) as Fraud Prevention

- **1.1 Atala PRISM Requirement:** The mandatory use of a registered **Atala PRISM DID** for all users participating in paid contracts serves as the primary layer of identity-based fraud prevention.
- **1.2 DID Blacklisting:** In the event of confirmed fraud, the Platform and the Dispute Arbitration Body reserve the right to publicly flag or blacklist the associated **DID and Public Wallet Address** within the Platform's indexing layer, which will prevent that DID from accessing services (bidding, posting jobs, arbitration access) in the future.
- **1.3 Verifiable Credentials:** Users providing **forged or revoked Verifiable Credentials** (VCs) to misrepresent their identity or qualifications will be immediately banned from the Platform.

## 2. Prohibited Fraudulent Activities

The following activities constitute fraud and are strictly prohibited:

- **Off-Platform Payment:** Negotiating or executing payments for jobs initiated on the Platform outside of the Aiken Escrow Smart Contract. This activity undermines the integrity of the on-chain reputation system.
- **Fake Credentials/Experience:** Claiming false professional experience, submitting fraudulent portfolio samples, or using **forged VCs** to mislead other Users.
- **Deceptive Evidence:** Submitting fabricated or misleading evidence (files, communications) to manipulate the on-chain Proof-of-Work Verification or the Dispute Arbitration Body.
- **Sybil Attacks:** Creating multiple DIDs or utilizing multiple Public Wallet Addresses for the purpose of manipulating ratings, reputation scores, or the arbitration process.

## 3. Enforcement and Penalties

- **3.1 Non-Custodial Enforcement:** As the Platform is non-custodial, the developers cannot seize funds. Enforcement relies on **on-chain reputation penalties** and **platform-level service denial**.
- **3.2 Penalties:** Confirmed fraudulent activity may result in:
  - Permanent blacklisting of the User's **DID and Public Wallet Address**.
  - Irreversible damage to the User's **Permanent Reputation Score** (through the `reputation.aiken` contract).
  - Permanent loss of Platform access.

# DecenTGigs: Kebijakan Anti-Penipuan dan Keamanan

Tanggal Berlaku: 21 November 2025

Kebijakan ini menguraikan langkah-langkah dan larangan terhadap aktivitas penipuan di platform terdesentralisasi DecenTGigs.

## 1. Identitas Terdesentralisasi (DID) sebagai Pencegahan Penipuan

- **1.1 Persyaratan Atala PRISM:** Penggunaan wajib **DID Atala PRISM** yang terdaftar untuk semua pengguna yang berpartisipasi dalam kontrak berbayar berfungsi sebagai lapisan utama pencegahan penipuan berbasis identitas.
- **1.2 Daftar Hitam DID:** Jika terjadi penipuan yang dikonfirmasi, Platform dan Badan Arbitrase Sengketa berhak untuk menandai atau memasukkan **DID dan Alamat Dompot Publik** terkait ke dalam daftar hitam secara publik di dalam lapisan pengindeksan Platform, yang akan mencegah DID tersebut mengakses layanan (menawar, memposting pekerjaan, akses arbitrase) di masa mendatang.
- **1.3 Kredensial yang Dapat Diverifikasi:** Pengguna yang memberikan **Kredensial yang Dapat Diverifikasi (VC) palsu atau dicabut** untuk salah merepresentasikan identitas atau kualifikasi mereka akan segera dilarang dari Platform.

## 2. Aktivitas Penipuan yang Dilarang

Aktivitas berikut merupakan penipuan dan dilarang keras:

- **Pembayaran di Luar Platform (Off-Platform Payment):** Negosiasi atau pelaksanaan pembayaran untuk pekerjaan yang dimulai di Platform di luar Kontrak Cerdas Escrow Aiken. Aktivitas ini merusak integritas sistem reputasi on-chain.
- **Kredensial/Pengalaman Palsu:** Mengklaim pengalaman profesional palsu, mengajukan sampel portofolio palsu, atau menggunakan **VC palsu** untuk menyesatkan Pengguna lain.
- **Bukti Menipu:** Mengajukan bukti yang dibuat-buat atau menyesatkan (file, komunikasi) untuk memanipulasi Verifikasi Bukti-Kerja on-chain atau Badan Arbitrase Sengketa.
- **Serangan Sybil:** Membuat banyak DID atau menggunakan banyak Alamat Dompot Publik dengan tujuan memanipulasi peringkat, skor reputasi, atau proses arbitrase.

## 3. Penegakan dan Sanksi

- **3.1 Penegakan Non-Kustodial:** Karena Platform bersifat non-kustodial, pengembang tidak dapat menyita dana. Penegakan mengandalkan **sanksi reputasi on-chain** dan **penolakan layanan tingkat platform**.
- **3.2 Sanksi:** Aktivitas penipuan yang dikonfirmasi dapat mengakibatkan:
  - Pemasukan ke daftar hitam permanen **DID dan Alamat Dompot Publik** Pengguna.
  - Kerusakan permanen yang tidak dapat diubah pada **Skor Reputasi Permanen** Pengguna (melalui kontrak `reputation.aiken`).
  - Kehilangan akses Platform secara permanen.

