Updated March 2022

IETA TASK GROUP ON INTEGRITY IN DIGITAL CLIMATE MARKETS
INITIAL GUIDING PRINCIPLES

Initial set of recommendations for guiding principles for the application for digital innovation to the carbon market that ensure overall market integrity.

Credible Standards: Where carbon credits are being used to issue digital tokens, these credits should come from projects that are validated, verified and registered under endorsed and conditionally endorsed standards by ICROA or government-approved carbon crediting schemes (the "Standards").

Registry Control: The authority to decide whether or not to allow market participants to tokenise carbon credits and retire them should reside solely with the Standards. The Standards should have the infrastructure to record and track carbon credits that are being tokenised before allowing market participants to tokenise them.

Tokens: Tokens should be minted only for issued, ex-post verified carbon credits, not cancelled or retired credits. The Standards should not allow token issuers to use expected forward streams of un-verified or un-issued emissions reductions and removals from projects.

Consumer Protection / Transparency / Know Your Customer (KYC) / Anti-Money Laundering (AML): Token issuers should be subject to KYC and AML checks by the Standards. Customers should look for full transparency around KYC/AML in digital carbon trading markets. The infrastructure to manage the KYC/AML of the users should be explored.

Investor Safeguards: Where tokenisation involves no direct nexus to the underlying carbon asset the risk of confusion among end users is high, and so token issuers and DAOs in particular should ensure that digital climate assets are suitable for customer's goals, needs and risk tolerance and appropriate for their knowledge and experience, particularly when assets are marketed to retail investors.

ieta.org
@ieta

secretariat@ieta.org
+41 22 737 05 00

Grand-Rue 11
CH-1204 Genève, Switzerland

Sustainability: Any digital technology deployed must be truly sustainable. This means it must be inclusive, open, resilient and secure as well as have a low carbon footprint.

IT Security: Digital technology should be deployed safely using proven methods of protection against cyber-attacks.

Public Record of Tokens: Tokenised carbon credits should be issued (not retired or cancelled) and recorded or held in escrow in a publicly accessible registry linked to the Standard, and shall be reflected in the relevant data repositories to avoid double selling, duplicate claims and non-authorised tokens.

Claims: Where tokens are digital twins of issued carbon credits, claims relating to carbon neutrality, offsetting, and/or compensation of emissions shall only be made after the token is permanently removed from circulation (by "burning" it on the blockchain) and the underlying carbon credits are been retired.

No valid compensation claims should be made in relation to only holding, but not retiring, credits. Further, the above claims should not be made for tokens trading in markets that are not directly and immutably linked to the underlying carbon assets.

Digital MRV Integrity: The deployment of digital MRV tools needs to draw upon best practices to ensure integrity and that proper standards are followed. The increased use of digital MRV should be coupled with a rigorous and transparent process to control data and claims integrity, eliminate bad actors, and ensure auditability and data accuracy to appropriate levels of confidence for intended use.