# Impersonation and Ensuring Authenticity of Straker Representatives

At Straker, we prioritize the security and integrity of our operations. We wish to assure our vendors and partners that robust measures are in place to prevent and respond to any incidents involving individuals impersonating Straker employees.

Presented below are Straker's standard operating procedures designed to ensure a secure working relationship with our vendors and provide external vendors with the necessary information to identify and avoid potential impersonation attempts claiming to represent Straker.

## Vendor Engagement and Agreement

All vendors engaged by Straker are required to sign a vendor agreement prior to commencing work. This agreement outlines the terms and conditions of our working relationship, including confidentiality and data protection obligations.

## Platform Security

Where possible Straker vendors operate exclusively using the following means:

1. In our proprietary tools including:
    a. **Straker Workbench**
    b. **Straker Verify**
    c. **Straker Enterprise (formerly Lingotek)**
2. For certificate clients files will be directly accessed to work on via our Vendor Platform. Files are never emailed directly to the client.
3. For some institutional clients we may use platforms such as Trados.
4. If any other toolset is used we will notify the Vendor of this within their purchase orders or on becoming a preferred vendor for a specific customer that requires this.
5. Unless specified we do not permit vendors to use other platforms or tools to perform work on our behalf. This ensures that all work is conducted within a secure and controlled environment.

## Communication Channels

Straker communicates with our vendors in the following manner:

1. Localisation vendors solely through email and through our Vendor Portal
2. Interpreting vendors via email, our intepreting platform Intepreter Intelligence and via text message

We do not use private messaging services such as Telegram, WhatsApp, Messenger, or other unsecure and unauthorised channels. This ensures that all communication is transparent, auditable, and secure.

Straker communicates with vendors using only these email domains:

**@strakergroup.com**

**@straker.ai**

**@strakertranslations.com**

## Reporting Scams and Security Incidents

If you suspect a scam or security incident related to Straker or our vendors, please report it immediately using the reporting mechanisms provided by the platform where the incident occurred (e.g., Facebook's scam reporting tool). We also encourage vendors to report any suspicious activity or security concerns directly to us.

## Contact Us

If you have any questions or concerns about our security practices, please do not hesitate to contact us through your Vendor Manager or at security@strakergroup.com.

Thank you for your partnership and cooperation in maintaining a secure working relationship.