**Guidelines to protect against phishing fraud**

- According to Sidel Group's finance and control policies, Sidel operates a system of dual-authorization, including for any payment instruction changes. Any such change must be approved in advance, in writing, by two persons authorized by a Sidel legal entity. Such payment instruction changes are extremely rare. Sidel rarely asks for payment to be changed from one bank to another, especially to a third country.
- For all payment requests, a Sidel invoice is always attached. Therefore you should immediately be suspicious of any such requests that do not contain a correct invoice.
- For all reminders or follow-up queries regarding payments, a reference to the original request and invoice is systematically included. Therefore you should immediately be suspicious of any request that does not contain a reference matching the initial request and invoice.
- In case of any changes to your normal payment requests and payment instruction from Sidel legal entities or agents, (even though Sidel may appear to be the sender) we always recommend verbally confirming the instructions via a telephone call to your trusted Sidel contact using your usual Sidel contact number. **Do not** use the contact details provided by the sender that appear on payment requests and payment instruction changes. Instead, call your trusted Sidel contact using your usual Sidel contact number. This is especially important if you receive a request to transfer funds or provide business sensitive information from an email address that appears different to the firstname.surname@sidel.com format.
- Sidel only communicates from a sidel.com email address, such as firstname.surname@sidel.com. Sidel does not use any other email address ending such as sidel.net, side1.com, sidei.com etc.
- Do not open, or respond to spam e-mails from external third parties.
- Do not respond to calls or e-mail messages asking for business sensitive or personal information. Always verify the source (by recording the details of the initial request and then calling back via telephone to the person named using a verified contact number).
- When sending business sensitive information by e-mail, consider encrypting the message.
- When accessing websites using popular search engines, make sure the site you are contacting is legitimate by checking the URL address which is often displayed by the search engine.
- Always verify the identity of anyone you communicate with via electronic communication (such as email), and the purpose of their request if you are suspicious.
- Always be suspicious of external e-mail messages containing links to access websites, no matter how legitimate the e-mail message may seem.
- Never click on a hyperlink (such as a link to an internet page) in an email if you are suspicious of the message or sender. If you are directed to a Sidel website from an email, always verify the website address is a valid sidel.com address.
- The main websites that Sidel uses for external communications are www.sidel.com www.sidel.de, www.sidel.pt, www.sidel.es, www.sidel.cn, www.sidel.fr and

www.sidel.ru. If you are asked in an email to access another Sidel site please do not access the link, and instead check first via a telephone call to your relevant Sidel contact.

- Always update computers with the latest security patches. Operating systems (such as Windows) are regularly improved by their vendors offering security enhancements. Windows, for example, enable users to automatically install security patches through http://windowsupdate.microsoft.com.
- Internet browsers (such as Internet Explorer, Mozilla Firefox, Google Chrome, Safari (Apple) etc.) now offer protection against fraudulent websites and have anti-phishing functionalities in their menus. Your browser(s) should also be regularly updated with the latest version.
- All software on computers should be regularly updated. Vendors regularly push pop-up messages to propose an update of their software.
- Consider installing antivirus and anti-spyware software (which are often available in the same product) and make sure it is up-to-date. Such software should also be regularly updated.
- Most antivirus software rely on a virus database, which can be updated as often as several times a day. The antivirus software can be set to automatically install these database updates to ensure maximum protection. You can consider scanning your computer after the antivirus is installed or updated to check for any possible infection.
- Consider activating a personal firewall. This enables you to protect the computer against intrusions and control incoming and outgoing traffic.
- Secure your email. Your email software should be equipped with anti-spam filtering. Email access should be protected with login and a strong password..
- If there is any suspicion that your email address has been hacked, consider using a new email address, and communicating this appropriately to all business contacts.

Finally, please remember to always double check any requests to change funding or banking details, and to verify the identity of the authorized sender. Confirm the request by calling the sender using your normal contact details (i.e. do not use contact details provided in the email).

More information, including advice and guidelines, can be found on the international support websites http://www.stopthinkconnect.org/ and http://www.antiphishing.org/.