**Richtlinien zum Schutz gegen Phishing-Angriffe**

- Entsprechend den Finanz- und Kontrollregeln der Sidel Group arbeitet Sidel mit einem zweistufigen Autorisierungssystem, das auch für Änderungen an Zahlungsanweisungen gilt. Solche Änderungen müssen vorab schriftlich von zwei Personen genehmigt werden, die von einem Rechtssubjekt der Sidel Group dazu ermächtigt wurden. An Zahlungsanweisungen werden nur in sehr seltenen Fällen Änderungen vorgenommen. Es kommt kaum vor, dass Sidel die Bank für eine Zahlung ändert, schon gar nicht an eine Bank in einem Drittland.
- Einer Zahlungsaufforderung liegt immer eine von Sidel ausgestellte Rechnung bei. Eine Zahlungsaufforderung ohne korrekt beigefügte Rechnung sollte sofort Ihr Misstrauen wecken.
- Zahlungserinnerungen oder Rückfragen zu Zahlungen nehmen systematisch auf die erste Aufforderung und die Rechnung Bezug. Eine Aufforderung ohne korrekte Bezugnahme auf die erste Aufforderung und die Rechnung sollte sofort Ihr Misstrauen wecken.
- Im Fall von Änderungen an den normalen Zahlungsaufforderungen und -anweisungen von Rechtssubjekten oder Vertretern von Sidel empfehlen wir, die Anweisung immer (auch wenn Sidel der Absender zu sein scheint) telefonisch von Ihrem gewohnten Sidel-Ansprechpartner unter der Ihnen bekannten Rufnummer bestätigen lassen. **Verwenden Sie nicht** die vom Absender auf den geänderten Zahlungsaufforderungen und -anweisungen angegebenen Kontaktdaten. Wenden Sie sich stattdessen an Ihren gewohnten Sidel-Ansprechpartner unter der Ihnen bekannten Rufnummer. Dies ist besonders wichtig, wenn Sie eine Aufforderung zur Überweisung von Geldern oder zur Übermittlung von vertraulichen betriebsinternen Informationen von einer E-Mail-Adresse erhalten, die vom E-Mail-Format vorname.zuname@sidel.com abweicht.
- Sidel verwendet nur E-Mail-Adressen mit dem Domänennamen sidel.com im Format vorname.zuname@sidel.com. Sidel verwendet keine E-Mail-Adressen, die auf sidel.net, side1.com, sidei.com usw. enden.
- Öffnen und beantworten Sie keine Spam-Mails von externen Dritten.
- Beantworten Sie keine Anrufe oder E-Mails, die nach vertraulichen oder persönlichen Informationen fragen. Überprüfen Sie immer die Herkunft (indem Sie die Angaben der ersten Aufforderung notieren und die genannte Person unter einer überprüften Rufnummer anrufen).
- Verschlüsseln Sie E-Mails, die vertrauliche betriebsinterne Informationen enthalten.
- Stellen Sie beim Zugriff auf Websites mit allgemeinen Suchmaschinen sicher, dass die besuchte Website unbedenklich ist, indem Sie die URL-Adresse überprüfen, die in der Regel von der Suchmaschine angezeigt wird.
- Überprüfen Sie die Identität und die Absichten von Personen, mit denen Sie elektronisch (z. B. per E-Mail) kommunizieren, wenn Sie Zweifel haben.
- Lassen Sie bei externen E-Mail-Nachrichten, die Links zu Websites enthalten, immer Vorsicht walten, auch wenn sie einen unbedenklichen Eindruck machen.
- Klicken Sie nie auf einen Hyperlink (z. B. einen Link zu einer Internet-Seite) in einer E-Mail, wenn Sie der E-Mail oder dem Absender misstrauen. Wenn Sie in einer E-

Mail zu einer Sidel-Website weitergeleitet werden, überprüfen Sie immer, ob die Adresse der Website eine gültige sidel.com-Adresse ist.

- Für die externe Kommunikation verwendet Sidel vor allem folgende Websites: www.sidel.com, www.sidel.de, www.sidel.pt, www.sidel.es, www.sidel.cn, www.sidel.fr und www.sidel.ru. Wenn Sie in einer E-Mail aufgefordert werden, eine andere Sidel-Site aufzurufen, verwenden Sie den Link nicht, sondern überzeugen Sie sich erst telefonisch bei Ihrem zuständigen Sidel-Ansprechpartner.
- Aktualisieren Sie Ihre Rechner immer mit den neuesten Sicherheits-Patches. Betriebssysteme (wie z. B. Windows) werden von ihren Herstellern regelmäßig verbessert, um die Sicherheit zu erhöhen. So ermöglicht beispielsweise Windows den Benutzern, über http://windowsupdate.microsoft.com automatisch Sicherheitsupdates zu installieren.
- Internet-Browser (z. B. Internet Explorer, Mozilla Firefox, Google Chrome, Safari (Apple) usw.) bieten auch Schutz gegen betrügerische Websites und Menüs mit Anti-Phishing-Funktionen. Verwenden Sie immer die neueste Version Ihres/Ihrer Browser(s).
- Aktualisieren Sie regelmäßig alle Programme auf Ihren Computern. Zur Erinnerung werden regelmäßig Popup-Meldungen der Hersteller mit der Aufforderung angezeigt, die Software zu aktualisieren.
- Installieren Sie eine Antivirus-Software und eine Software zum Schutz gegen Spyware (meist in einem Produkt angeboten) und stellen Sie sicher, dass sie immer auf dem neuesten Stand sind. Diese Programme müssen regelmäßig aktualisiert werden.
- Die Antivirus-Software basiert auf einer Viren-Datenbank, die mehrmals täglich aktualisiert wird. Die Antivirus-Software kann so eingestellt werden, dass sie diese Datenbank-Updates automatisch installiert, um maximale Sicherheit zu gewährleisten. Sie können nach der Installation oder Aktualisierung der Antivirus-Software Ihren Computer scannen, um eine eventuelle Infizierung aufzufinden.
- Eine weitere Möglichkeit ist die Aktivierung einer persönlichen Firewall. Eine Firewall schützt Ihren Computer gegen Angriffe und kontrolliert den ein- und ausgehenden Datenverkehr.
- Sichern Sie Ihre E-Mail. Ihre E-Mail-Software sollte über einen Spam-Filter verfügen. Der E-Mail-Zugriff sollte mit einem Benutzernamen und einem gut gewählten Passwort geschützt werden.
- Wenn Sie vermuten, dass Ihre E-Mail-Adresse gekapert wurde, sollten Sie eine neue E-Mail-Adresse verwenden und Ihren Geschäftspartnern mitteilen.

Vergessen Sie nicht, jede Aufforderung zur Änderung von Überweisungen oder Kontodaten zu überprüfen und die Identität des Absenders festzustellen. Überprüfen Sie die Richtigkeit der Aufforderung, indem Sie den Absender unter Verwendung Ihrer gewohnten Kontaktdaten anrufen (verwenden Sie nicht die Kontaktdaten in der E-Mail mit der Aufforderung).

Weitere Informationen sowie Ratschläge und Richtlinien finden Sie auf den internationalen Support-Websites http://www.stopthinkconnect.org/ und http://www.antiphishing.org/.