zürisee IT
Betriebsinformatik

MICRODYN AG ▪ züriseeIT
Schwerzistrasse 6
CH-8807 Freienbach (SZ)

Tel. **+41 55 510 0 510**
Mail: support@zueriseeIT.ch
Web: www.zueriseeIT.ch

Freienbach, 6. Juni 2022

Merkblatt zu Datenschutz und Sicherheit für private Anwender V1.0

Wir empfehlen unseren Kunden folgende Datenschutz- und Sicherheitsmaßnahmen im Zusammenhang mit Computern und Smart Mobile Geräten:

SICHERUNG:

- Sichern Sie Ihr komplettes System (Betriebssystem, Programme und Daten) regelmäßig auf ein oder sogar zwei örtlich getrennte und an einem sicheren Ort aufbewahrte Geräte. Beispiel: USB Festplattenlaufwerk.

AKTUALITÄT von SOFTWARE:

- Verwenden Sie ein aktuelles Betriebssystem und aktuelle Programme (nicht älter als 2 Generationen).
- Aktualisieren Sie das Gerät, das Betriebssystem und die Programme regelmäßig mit Herstellerupdates.

FIREWALL:

- Benutzen Sie einen Firewall, um unberechtigten Zugang auf Ihre Geräte zu vermeiden.

KENNWÖRTER:

- Teilen Sie Ihre Kennwörter auf keinen Fall.
- Nutzen Sie unterschiedliche Kennwörter für die unterschiedlichen Zugänge.
- Nutzen Sie sichere Kennwörter. (Min. 14 Zeichen lang – mit Buchstaben (Groß/Klein), Zahlen und Sonderzeichen.
- Notieren Sie Ihre Kennwörter und bewahren Sie Sie an einem sicheren Ort auf. Dazu kann z.B. das Programm „Keypass“ verwendet werden.
- Wenn Sie einen Swisscom, Salt, Sunrise, Mobilezone Shop oder ähnliche besuchen, weil Sie dort ein neues Gerät einrichten lassen möchten oder weil Sie Anpassungen an Ihrem Gerät vornehmen lassen möchten – merken Sie sich die Kennwörter, die im Rahmen dieser Arbeiten neu gesetzt wurden oder verlangen Sie dass der Mitarbeiter Sie auf dem neuen Gerät selbst das bekannte Kennwort eintippen lässt. Vermeiden Sie spontane Kennwortrücksetzungen durch Personal dieser Unternehmen - da diese oft dazu führen, dass auf weiteren Geräten – z.B. auf dem PC zu Hause Programme wie Outlook oder Thunderbird bezüglich Zugangsdaten wieder angepasst werden müssen. (Kettenreaktion). Verlangen Sie eine Dokumentation der durchgeführten Arbeiten.
- Wenn Ihre Zugangsdaten kompromittiert wurden, melden Sie sich sofort bei der entsprechenden Hersteller Hotline. Sie erhalten dann i.d.R. einen Brief mit Anweisungen zum wieder Freischalten mittels neuen Kennworts.
- Ändern Sie Ihre Kennwörter von Zeit zu Zeit.
- Wenn Sie ein Kennwort auf einer Webseite eingeben, achten Sie darauf, dass die Kommunikation zu dieser Webseite verschlüsselt sein muss. Achten Sie darauf, dass der Betreiber der Webseite einen entsprechenden Nachweis über seine Identität erbringt.

WLAN:

- Achten Sie darauf, dass Ihr WLAN mit einem Passwort geschützt und verschlüsselt ist.

zürisee IT
Betriebsinformatik

MICRODYN AG ▪ züriseeIT
Schwerzistrasse 6
CH-8807 Freienbach (SZ)

Tel. **+41 55 510 0 510**
Mail: support@zueriseeIT.ch
Web: www.zueriseeIT.ch

Freienbach, 6. Juni 2022

SUPPORT:

- Seriöse Hotlines rufen Sie nicht ungefragt an und verlangen keinen Zugang zu Ihrem PC per Fernsteuerung. Sollten Sie z.B. Anrufe von MICROSOFT erhalten handelt es sich mit hoher Wahrscheinlichkeit um einen Betrugsversuch eines indischen Call Centers (SCAM) genannt. Informieren Sie sich beim Nationalen Zentrum für Cybersicherheit NCSC über die möglichen Vorgehensweisen: https://www.ncsc.admin.ch
  Lassen Sie sich von Ihrem Supporter mehrere überprüfbare Referenzkunden angeben.

DOWNLOADS:

- Laden Sie keine Software herunter welche nicht von der Herstellerseite selbst stammt.

E-MAIL Anhänge:

- Öffnen Sie keine E-Mail-Anhänge oder E-Mails von Personen welche Ihnen nicht als vertrauenswürdig bekannt sind.

VIRENSCHUTZ:

- Nutzen Sie einen guten und aktuellen Virenschutz.

PRIVILEGIEN DER KONTEN so klein wie möglich halten:

- Achten Sie darauf, dass die eingerichteten Konten auf den PCs keine Administrativen Rechte haben. Richten Sie ein nicht privilegiertes Konto für den alltraggebrauch für jedes Familienmitglied ein. Für Administrative Aufgaben richten Sie je ein Konto für die Familienmitglieder ein – wo dies nötig ist. Dieses wird dann nur wenn nötig genutzt. z.B. bei einer Softwareinstallation.

KINDERSCHUTZ:

- Sprechen Sie mit Ihren minderjährigen Kindern über Gefahren im Internet und bei Nutzung von Smart-Geräten.
- Schützen Sie Ihre minderjährigen Kinder, indem Sie Sie nicht unbeaufsichtigt Smart-Geräte oder das Internet nutzen lassen.
- Bauen Sie ein Vertrauensverhältnis auf, sodass die Kinder selbständig bei allem was neu ist auf Sie zukommen und fragen – bevor Vorfälle eintreten. Hypes in der Schule oder bei Kollegen führen rasch dazu, dass Kinder ungewollt oder unbedarft in die Illegalität abdriften.

ERWACHSENENSCHUTZ:

- Menschen, welche sich in besonderen Umständen befinden wie: Depression, Krankheit, Alterskrankheiten, Entmündigte, vor kurzem geschiedene, zurückgezogen lebende usw. müssen besonders vorsichtig im Umgang mit Smart-Geräten und dem Internet sein. Allenfalls bedürfen Sie einer Begleitung durch die Familie, Vormund, durch Freunde oder eine darauf spezialisierte Behörde.
  Betrüger weltweit haben sich auf diese Zielgruppen spezialisiert.

Für Fragen oder Ergänzungswünsche zu diesem Merkblatt senden Sie bitte eine E-Mail an support@zueriseeIT.ch
Alle Angaben in diesem Merkblatt verstehen sich ohne Gewähr.

Falls Sie beim Umsetzen dieser Punkte Hilfe benötigen, stehen wir gerne mit Rat und Tat zur Seite.