# **Vorlage: Merkblatt Cybersecurity für Mitarbeitende**

**Cybersecurity in der**

Willkommen im Unternehmen! Die folgenden Regeln zur Cybersecurity gelten für alle Mitarbeitenden von ab Tag 1.

**Sicherheitsvorkehrungen der Firma**

* Auf allen Geräten, die Sie für berufliche Zwecke nutzen, ist ein Virenschutz installiert. Dieser Virenschutz wird ständig aktualisiert. Er darf nicht deaktiviert werden.
* Auf allen Geräten, die Sie für berufliche Zwecke nutzen, ist eine Firewall aktiv. Sie darf nicht deaktiviert werden.
* Bei Virenschutz, Firewall und Betriebssystem werden regelmässig Updates vorgenommen. Diese dürfen weder verzögert noch verhindert werden.
* Auf allen Geräten wird eine regelmässige Datensicherung durchgeführt. Der Erfolg dieser Sicherung wird jeweils geprüft.
* Alle Geräte, die Sie für berufliche Zwecke nutzen, sind der IT bekannt. Im Notfall ist ein Remote-Zugriff auf die Geräte möglich.

**Das sind Ihre Pflichten**

* Sie verwenden für alle Zugriffe auf Arbeits- und Teamplattformen nur die Geräte, die Ihnen von der zur Verfügung gestellt wurden. [Ergänzung, falls Nutzung privater Geräte erlaubt: Für die Verwendung privater Geräte müssen Sie vorgängig die Erlaubnis der/des IT-Verantwortlichen einholen.]
* Sie verwenden für alle Zugriffe auf Arbeits- und Teamplattformen ein Passwort, das den Standards der entspricht:
* Ihr Passwort soll mindestens 12, besser 20 Zeichen lang sein. Es muss Gross- und Kleinbuchstaben enthalten sowie mindestens eine Zahl und ein Sonderzeichen (!, %, &).
* Verwenden Sie keine leicht zu erratenden Passwörter wie 1234, Passwort, Ihr Geburtsdatum, die Vornamen Ihrer Kinder, …
* Sie prüfen bei eingehenden E-Mails stets die Richtigkeit des Absenders und dessen Vertrauenswürdigkeit, bevor Sie diese und allfällige Anhänge öffnen. Im Zweifelsfall nehmen Sie zuerst mit dem Absender Kontakt auf – idealerweise nicht per E-Mail, sondern telefonisch.
* Sie nutzen keine portablen Speichermedien, die nicht von der IT-Abteilung ausgegeben und registriert wurden. Sie verbinden keine nicht zugelassenen Speichermedien mit Ihren Arbeitsgeräten – auch nicht für kurze Zeit.
* Auf Geschäftsreisen gelten strengere Regeln für Cybersicherheit:
* Stellen Sie sicher, dass auf Ihren Geräten der aktuellste Virenschutz installiert ist.
* Aktivieren Sie die Sperrung Ihrer Geräte und wechseln Sie Ihre PIN.
* Ändern Sie für die Dauer der Reise Ihr Passwort.
* Meiden Sie unterwegs ungesicherte Wi-Fi-Netzwerke und prüfen Sie das Sicherheitsprotokoll im Hotel.
* Schalten Sie die Angabe von Standortdaten aus.
* Deaktivieren Sie nach Möglichkeit Bluetooth.
  + Auffälligkeiten, Geräte- oder Datenverlust melden Sie unverzüglich an . Versehentliche, nicht absichtliche Fehlbedienungen haben keine negativen Konsequenzen für Sie.
* Die Installation zusätzlicher Software auf Arbeitsgeräten muss von der IT-Abteilung bewilligt werden.
* Regelmässige Fortbildung zur Cybersicherheit ist Pflicht.

Sind Sie unsicher, ob und wie Sie einzelne dieser Punkte umsetzen sollen, wenden Sie sich bitte an .