10 Goldene Regeln für die Cybersicherheit

 Vorlage

# Autorität und Überprüfung

## Dokumentenkontrolle und -prüfung

|  |  |
| --- | --- |
| **Dokumentenprüfung**  |  |
| Autor  |  |
| Eigentümer |  |
| Datum der Erstellung |  |
| Zuletzt überarbeitet von  |  |
| Datum der letzten Überarbeitung |  |

## Versionsverwaltung

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Datum der Genehmigung** | **Genehmigt durch**  | **Beschreibung der Änderung** |
| 1.0 |  |  |  |

# 10 Goldene Regeln für die Cybersicherheit

|  |  |
| --- | --- |
|  | **Schützen Sie Ihre Konten mit starker Authentifizierung!****Verwenden Sie, wann immer möglich, eine Multi-Faktor-Authentifizierung (MFA)!*** Lange Kennwörter sind effizienter. Sie sind für Cyberkriminelle schwerer zu knacken, da die Zeichenanzahl viele Möglichkeiten bietet.
* Starke Passwörter sind **mindestens 14 Zeichen lang, nicht leicht herauszufinden und enthalten: Großbuchstaben, Kleinbuchstaben, numerische Zeichen und Sonderzeichen (&, $, %, !, =, +, ...).**
 |
|  | Verwenden Sie unterschiedliche Passwörter für berufliche und private Konten |
|  | Speichern Sie alle Ihre Daten in einem System von dem regelmäßig zentrale Backups erstellt werden. |
|  | Führen Sie Sicherheitsupdates auf all Ihren Geräten durch, sobald sie verfügbar sind. |
|  | Lassen Sie niemals physische Informationen (z. B. Papiere) oder Geräte unbeaufsichtigt an Ihrem Schreibtisch liegen. |
|  | Vermeiden Sie öffentliches Wi-Fi und nutzen Sie, insofern verfügbar, das virtuelle private Netzwerk (VPN) Ihres Unternehmens. |
|  | **Vermeiden Sie Phishing, indem Sie sich folgende Fragen stellen**:* Ist der Absender jemand den ich kenne?
* Hatte ich eine Nachricht zum genannten Thema erwartet?
* Wird in der Nachricht nach Informationen wie einem Benutzernamen, einem Passwort oder einer Kontonummer gefragt?
* Ist es dringend?
* Wohin führt der Link? (nur mit dem Mauszeiger darüberfahren, nicht anklicken)
* Enthält die Nachricht einen QR-Code?
* Werde ich persönlich angesprochen?
* Gibt es Sprachfehler in der Nachricht?
* Befindet sich die Nachricht im Spam-/Junkmail-Ordner?
* Versucht jemand, mich neugierig zu machen?
* Wird eine Zahlung verlangt?

**Wie reagieren Sie auf eine Phishing-E-Mail?*** Beantworten Sie sie nicht, öffnen Sie keine Anhänge und klicken Sie nicht auf die Links.
* Geben Sie niemals per SMS oder E-Mail angeforderte Bankdaten weiter.
* Melden Sie den Phishing-Versuch an **[Ihre IT-Abteilung/Ihren Anbieter]** und löschen Sie die E-Mail/den Text.
 |
|  | Beachten Sie die folgenden Maßnahmen beim Umgang mit internen oder vertraulichen Informationen:* Sperren Sie Ihren Computer, wenn Sie ihn unbeaufsichtigt lassen.
* Lassen Sie Computer oder Papiere außerhalb der Arbeitszeit nicht unbeaufsichtigt auf den Schreibtischen liegen.
* Lassen Sie Papiere nicht unbeaufsichtigt in Druckern liegen.
* Achten Sie immer auf Ihre Umgebung wenn Sie an öffentlichen Orten vertrauliche Informationen abfragen oder besprechen. Versuchen Sie sich so weit wie möglich abzuschotten, um zu verhindern, dass jemand das Gespräch mithört.
 |
|  | Verwenden Sie zum Herunterladen von Anwendungen und Software nur offizielle Websites und Plattformen. Das Herunterladen von Software sollte weitgehend vermieden werden. Software wird nur von **der IT-Abteilung/vom Anbieter** installiert**.** |
| Marketing outline | Melden Sie alle Vorfälle im Bereich der Informationssicherheit **[Ihrer IT-Abteilung/Ihrem Provider]**. Wenden Sie sich immer an **[Ihre IT-Abteilung/Ihren Provider]**, wenn:* Sie Fragen oder Anmerkungen zu diesem Dokument haben;
* Sie etwas bemerken was diesem Dokument widerspricht;
* ein vermuteter oder bestätigter Vorfall eintritt.

Kontaktinformationen: **[Telefonnummer der IT-Abteilung/des Anbieters] / [E-Mail der IT-Abteilung/des Anbieters].** |