IT-Hausordnung für \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Ziel:** Diese Regeln sollen den sicheren, einheitlichen und verantwortungsvollen Umgang mit IT-Systemen, Programmen und Daten im Unternehmensalltag gewährleisten.

**1. Passwörter**

* Verwenden Sie starke Passwörter mit mindestens 10 Zeichen, Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen.
* Nutzen Sie für jeden Dienst ein eigenes Passwort.
* Verwenden Sie wenn möglich einen Passwortmanager.
* Passwörter dürfen nicht auf Zetteln notiert oder weitergegeben werden.
* Regelmäßige Änderung von Passwörtern wird empfohlen.

**2. E-Mail- und Internetnutzung**

* Öffnen Sie keine Links oder Anhänge aus unbekannten oder verdächtigen E-Mails.
* Achten Sie auf ungewöhnliche Absender-Adressen und Sprachstil.
* Besuchen Sie nur seriöse Webseiten, insbesondere keine fragwürdigen Download-Portale.
* Niemals private E-Mail-Konten für geschäftliche Zwecke verwenden.

**3. Updates & Wartung**

* Schalten Sie den PC nicht aus, wenn Updates installiert werden.
* Melden Sie sich regelmäßig neu an (nicht dauerhaft im Energiesparmodus lassen).
* Installieren Sie keine Software ohne Rücksprache mit dem IT-Support.
* Lassen Sie Systempflege (z. B. Updates, Virenschutz) regelmäßig durchführen.

**4. Mobile Geräte & USB-Sticks**

* Nur autorisierte Geräte dürfen mit dem Firmennetzwerk verbunden werden.
* USB-Sticks nur verwenden, wenn sie geprüft wurden.
* Mobile Geräte wie Smartphones oder Tablets müssen mit PIN oder biometrischer Sperre geschützt sein.

**5. Datensicherung**

* Alle Arbeitsdaten sind auf Netzlaufwerken oder Cloudspeichern zu speichern, nie ausschließlich lokal.
* Wichtige Dokumente sollten regelmäßig in definierten Sicherungsordnern abgelegt werden.
* Daten auf externen Speichermedien sind verschlüsselt zu sichern.

**6. Homeoffice-Regeln (falls zutreffend)**

* Nur gesicherte WLAN-Verbindungen verwenden, keine offenen Netzwerke.
* Arbeiten Sie an einem privaten Gerät nur mit Zustimmung und nach Prüfung durch die IT.
* Bildschirm darf nicht einsehbar sein für Dritte (z.B. im Café, Zug usw.).
* Arbeitsgeräte zu Hause nicht durch Familienmitglieder nutzen lassen.

**7. Zugriffsrechte & Benutzerkonten**

* Mitarbeitende erhalten nur Zugriff auf Daten, die sie für ihre Arbeit benötigen.
* Benutzerkonten sind personenbezogen, keine Sammelkonten oder „Admin für alle“.
* Bei Ausscheiden aus dem Unternehmen ist der Zugriff umgehend zu deaktivieren.

**8. Verhalten bei IT-Störungen oder Sicherheitsvorfällen**

* Verdächtige E-Mails, Systemfehler oder ungewöhnliches Verhalten sofort dem IT-Support melden.
* Keine „Selbsthilfe“ bei Virenverdacht, Gerät sofort vom Netz nehmen und Support kontaktieren.

**9. Verantwortlichkeiten**

* Jeder Mitarbeitende trägt Verantwortung für den eigenen Umgang mit IT-Systemen.
* Die Geschäftsführung benennt einen Ansprechpartner für IT-Fragen.
* Der IT-Dienstleister unterstützt, ersetzt aber kein bewusstes Verhalten im Alltag.

**10. Empfohlene Routinen**

* Einmal wöchentlich: PC neu starten, Updates prüfen.
* Monatlich: Überprüfen, ob alle Daten korrekt gesichert sind.
* Bei jeder verdächtigen E-Mail: Nicht öffnen, sondern melden!

**Hinweis:** Diese Hausordnung ist ein Hilfsmittel zur Orientierung und ersetzt keine individuelle Sicherheitsberatung. Bitte sprechen Sie bei Fragen mit Ihrem IT-Dienstleister.