

BEISPIELE ALLTÄGLICHER SICHERHEITSRISIKEN

BETRIEBSAUSWEISE GEHÖREN AN DEN MANN BZW. DIE FRAU!

- Betriebsausweise sollten stets sichtbar an der Oberbekleidung getragen werden.
- Sie sollten niemals an Dritte weitergegeben werden – dies gilt auch für Besucher- oder Fremdfirmenausweise.

NUR SICHERE UND SICHER VERWAHRTE PASSWÖRTER SIND GUTE PASSWÖRTER!

- Arbeitsbezogene Passwörter sollten nicht notiert oder anderweitig zugänglich gemacht und keinesfalls Dritten mitgeteilt werden.
- Nutzen Sie stets sichere Passwörter mit Buchstaben-, Zahlen- und Sonderzeichenkombinationen.

VERTRAULICHE DOKUMENTE MÜSSEN JEDERZEIT VOR FREMDEN ZUGRIFFEN GESCHÜTZT WERDEN!

- Vertrauliche Dokumente sollten immer sicher verwahrt werden – auch bei kurzzeitiger Abwesenheit.
- Keine unbefugten Personen sollten einen Blick auf vertrauliche Dokumente werfen können.
- Geben Sie vertrauliche Dokumente niemals an unberechtigte Personen weiter.

VERTRAULICHE GESPRÄCHE SOLLTEN IMMER IN EINEM GESCHÜTZTEN UMFELD STATTFINDEN!

- Bei Gesprächen sollten andere Personen nicht ohne weiteres mithören bzw. zusehen können.
- Geben Sie am Telefon niemals vertrauliche Daten oder Informationen preis, wenn Sie von einer unbefugten Person dazu aufgefordert werden.

SICHERHEIT AUCH UNTERWEGS UND AUF GESCHÄFTSREISEN BEACHTEN!

- Gestatten Sie fremden Personen keinen Zugriff oder Blick auf Ihren Arbeitsbildschirm oder vertrauliche Dokumente, Aufzeichnungen, Notizen usw.
- Führen Sie vertrauliche Aufzeichnungen nur mit sich, wenn dies für die Ausführung Ihrer Tätigkeit zwingend erforderlich ist.

SICHERHEIT GEHT VOR HÖFLICHKEIT!

- Hinterfragen Sie ggf. die Zutrittsberechtigung von Personen und lassen Sie sich den (Mitarbeiter-)Ausweis zeigen.
- Verfolgen Sie in Ihrem Bereich konsequent eine „Clean-Desk-Policy“ und beseitigen Sie alle firmeninternen Daten und Unterlagen sowie potenzielle weitere Sicherheitslücken.

Vertrauliche Arbeitstätigkeiten und Gespräche sollten stets in einer geschützten Umgebung stattfinden.

BRIEF- UND PAKETSENDUNGEN BERGEN RISIKEN FÜR DIE INFORMATIONSSICHERHEIT!

- Sensible Daten sollten ggf. per Kurierdienst versendet und in der Zwischenzeit vor fremdem Zugriff geschützt aufbewahrt werden.

ACHTEN SIE AUF EINE SICHERE ENTSORGUNG VON DOKUMENTEN UND ELEKTRONISCHEN DATENSPEICHERMEDIEN!

- Vertrauliche Unterlagen gehören in spezielle Datenentsorgungstonnen.
- Elektronische Speichermedien sollten ausschließlich in den dafür vorgesehenen Entsorgungsbehältern entsorgt oder der IT-Abteilung übergeben werden.

 **KOSTENFREI ABONNIEREN!**