IT-Sicherheitsrichtlinie

Geltungsbereich der Richtlinie

Diese Richtlinie gilt verbindlich für alle Mitarbeiter ohne Ausnahme für die Nutzung dienstlicher IT. Verstöße gegen die Inhalte der Richtlinie können zu arbeitsrechtlichen Konsequenzen führen. Bei der Beschäftigung externer Mitarbeiter hat der betreuende interne Mitarbeiter darauf zu achten, dass die Vorgaben dieser Richtlinie beachtet werden.

Umgang mit Informationen

Die im Unternehmen verarbeiteten Informationen sind eine Grundlage für den Geschäftsbetrieb. Jeder Mitarbeiter ist für die sorgsame Behandlung der von ihm bearbeiteten Informationen verantwortlich. Das gilt insbesondere für vertrauliche Daten und dem Datenschutzgesetz unterliegenden Personendaten.

Vertretungsregelung

Für den Fall der Abwesenheit (Geschäftsreise, Urlaub, Krankheit) ist vorzusorgen. Es sind Vertreter zu benennen, die vom Stelleninhaber einzuweisen und zu informieren sind.

Einsatz von Soft- und Hardware

Der Einsatz neuer Soft- und Hardware wird vorher von dem für die IT verantwortlichen Mitarbeiter getestet und muss freigegeben werden. Nicht freigegebene Hard- und Software – insbesondere privat mitgebrachte – darf nicht verwendet werden.

Entsorgung von Informationen

Belege und Druckausgaben, die vertrauliche Informationen beinhalten, müssen getrennt vom übrigen Abfall im Aktenvernichter entsorgt werden. Das gilt auch für elektronische Datenträger mit vertraulichen Informationen, die nicht weiter benötigt werden.

Weitergaberegelungen

Bei der Weitergabe von Informationen ist ihr Schutzbedarf zu beachten und eine geeignete Versandart zu wählen. Vertrauliche Informationen oder Datenträger (USB-Stick, CD-ROM etc.) mit vertraulichen Informationen dürfen erst dann versendet werden, wenn die Vertraulichkeit auch beim Versand gewährleistet ist. Im Zweifelsfall erkundigen Sie sich im Sekretariat.

Zutritts- und Zugangsregelungen

Der Zutritt zu den Räumlichkeiten und zu den IT-Systemen ist gegen Unbefugte zu schützen und zu kontrollieren. Lassen Sie betriebsfremde Personen nicht unbeaufsichtigt in die Firmenräume. Der Zugriff auf die IT-Systeme ist durch Passwörter sichergestellt, die Passwortregelungen sind zu beachten. PC-Arbeitsplätze sind bei Verlassen zu sperren. Dazu wird der Bildschirmschoner mit Passwortschutz eingesetzt, der sich spätestens nach 10 Minuten Inaktivität automatisch einschaltet.

Verschlüsselung

Vertrauliche und andere sicherheitsrelevante Daten sind verschlüsselt zu speichern. Zur Verschlüsselung steht Ihnen das Programm (XYZ) zur Verfügung.

Schadsoftware

Auf allen PC-Arbeitsplätzen und den Servern sind Viren-Schutzprogramme installiert, die regelmäßig aktualisiert werden. Das Abschalten oder Umgehen dieser Programme ist untersagt.

Datensicherung/ Archivierung

Ihre täglich verarbeiteten und auf den Netzlaufwerken gespeicherten Daten werden regelmäßig gesichert. Bei Datenverlusten wenden Sie sich zur Wiederherstellung der Daten an den IT-Administrator. Lokal auf dem PC gespeicherte Daten werden nicht gesichert und gehen bei einem Defekt der Festplatte verloren.

Fernzugriff auf das interne Netz

Generell ist der „Zugriff vor Ort“ dem „Fernzugriff“ vorzuziehen. Wenn Sie von einem mobilen Arbeitsplatz auf das Netz zugreifen, darf das nur über den VPN-Zugang erfolgen. Andere Zugänge auf das Firmennetz sind untersagt.

Zur Kenntnis genommen:

……

Ort, Datum, Unterschrift Mitarbeiter/in