IT-Richtlinien

1. Einleitung

Diese IT-Richtlinie soll die vom Unternehmen getroffenen Maßnahmen zum Schutz von (personenbezogenen) Daten vor unbefugter Kenntnisnahme durch Dritte oder nichtberechtigte Mitarbeiter unterstützen und darüber hinaus eine grundlegende Information für alle Mitarbeiter im Hinblick auf den Umgang mit Daten sein.

2. Geltungsbereich

Diese IT-Richtlinie gilt für alle Beschäftigte unseres Unternehmens. Dazu gehören alle Voll- und Teilzeitangestellte, Lehrlinge, Praktikanten sowie Aushilfskräfte etc. Auch externe Personen, die regelmäßig im Unternehmen tätig sind, sind verpflichtet, sich an diese Richtlinie zu halten. Das Unternehmen wird entsprechende Vorkehrungen treffen, damit diese Richtlinie auch für die externen Personen verbindlichen Charakter hat.

3. Einhaltung von Rechtsvorschriften

Bei der Benutzung der IT-Systeme und Applikationen im Unternehmen sind von den Mitarbeitern die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie die Unternehmensregelungen einzuhalten. Sollten Mitarbeiter unsicher sein, ob und inwieweit Rechtsvorschriften oder Unternehmensregelungen einzuhalten sind, haben sie sich an ihren Vorgesetzten zur Klärung zu wenden.

4. Schulung

Das Unternehmen trägt Sorge dafür, dass die Mitarbeiter die erforderlichen Schulungen und Instruktionen/Anweisungen erhalten, die für den jeweiligen Umgang mit den IT-Systemen und/oder Applikationen erforderlich sind.

5. Allgemeine Regelungen

Die Nutzung der IT-Systeme und Applikationen im Unternehmen ist ausschließlich zu dienstlichen Zwecken und in jeweils erlaubten Umfang zur Aufgabenerledigung zulässig. Abweichungen hiervon bedürfen der ausdrücklichen Erlaubnis des Arbeitgebers, die schriftlich erfolgen muss.

Die Installation von Software zu privaten Zwecken ist untersagt. Im Übrigen darf nur die Software auf IT-Systemen des Unternehmens installiert werden, die vom Arbeitgeber oder der IT-Abteilung freigegeben worden ist.
Die Benutzung privater Hard- und Software zu dienstlichen Zwecken ohne Genehmigung des Arbeitgebers ist nicht zulässig. Davon ausgenommen ist die Einrichtung des Firmen-E-Mail Accounts am Mobiltelefon.

6. Arbeitsplatz

Der Arbeitsplatz ist von den Mitarbeitern so zu gestalten, dass Besucher bzw. Kunden (im Falle eines Außendienstmitarbeiters) oder sonstige Dritte keinen Zugang zu personenbezogenen Daten bekommen können, ohne hierfür berechtigt zu sein. So sind Büros nach dem Verlassen des Arbeitsplatzes grundsätzlich zu verschließen. Beim Verlassen des Arbeitsplatz-PCs muss der jeweilige Mitarbeiter sich „abmelden“, so dass vor der erneuten Nutzung des IT-Systems und/oder der Applikation(en) eine Authentifizierung (Benutzername/Passwort) erforderlich wird.

In Bereichen mit Publikumsverkehr sind die IT-Systeme – insbesondere die Bildschirme – so auszurichten, dass das Risiko der Kenntnisnahme durch Besucher oder Dritte nach Möglichkeit ausgeschlossen wird.

Informationen in Papierform sind so abzulegen, dass Besucher oder sonstige Dritte keine Kenntnisnahme von den Daten erhalten können. Vertrauliche Informationen sind stets unter Verschluss zu halten.

7. Verwendung von PCs, Laptops und Terminalserver

Bei längerer Nichtverwendung, zB Arbeitsende, ist das Arbeitsgerät (PC oder Laptop) herunterzufahren. Bei Laptops ist dafür Sorge zu tragen, dass diese nicht in den Standby-Modus übergehen (zB Zuklappen des Bildschirmdeckels), sondern das Betriebssystem komplett heruntergefahren wird. Dies ist wichtig, um die evtl. anstehenden Undates für Soft/Hardware zu ermöglichen.
Für alle Geräte gilt, dass diese wöchentlich durch den Benutzer zumindest zweimal neu gestartet werden.
Am Terminalserver sind die benötigten Programme und Benutzerprofile bereits vorinstalliert. Auch hier gilt, dass sich Benutzer bei längerer Nichtbenutzung, zumindest jedoch täglich, abmeldet. Das ledigliche Schließen des Terminalfensters führt nicht zur Abmeldung.
Weiters ist zu beachten, dass jeden Freitag, um 14:00 Uhr beginnend, Updates auf allen zentralen Geräten eingespielt werden. Benutzer haben daher am Freitag bis 14:00 Uhr alle Programme zu schließen und sich ggf vom Terminalserver abzumelden.

8. Passwort-Gebrauch

Soweit technisch möglich sind alle IT-Systeme und Applikationen erst nach hinreichender Authentifizierung des Nutzers nutzbar. Die Authentifizierung erfolgt in der Regel durch die Verwendung der Kombination Benutzername/Passwort. Die IT-Abteilung wird, soweit keine betrieblichen oder technischen Gründe entgegen sprechen, jedem einzelnen berechtigten Nutzer einen Benutzernamen sowie ein Passwort zuweisen.
Passwörter müssen eine Mindestlänge von 10 Zeichen haben. Das Passwort ist alphanumerisch (Buchstaben und Zahlen/Zeichen mit Sonderzeichen) zu gestalten.
Passwörter werden seitens der IT-Abteilung regelmäßig geändert.

9. Schutz vor schädlichen Inhalten ("Threats")

Zum Schutz vor schädlichen Inhalten werden im Unternehmen Schutzprogramme eingesetzt. Insbesondere eingehende E-Mail-Kommunikation wird durch die eingesetzten Schutzprogramme überprüft. Dabei kann es auch zur Löschung von E-Mails und Dateianhängen kommen. Für den Fall, dass ein Mitarbeiter eine verdächtige E-Mail mit zB einem unbekannten Dateianhang oder Link erhält, ist dieser verpflichtet, sich unverzüglich an die IT-Abteilung zu wenden. Der unbekannte Dateianhang oder Link darf erst nach Freigabe durch die IT-Abteilung geöffnet werden.

10. Schutz vor unverlangter Werbung ("Spam")

Zum Schutz vor unverlangter Werbung durch E-Mail werden im Unternehmen so genannte Spam-Filter eingesetzt. Durch den Spam-Filter kann es dazu kommen, dass im Einzelfall E-Mails unterdrückt oder gelöscht werden. Die Mitarbeiter sollen Sorge dafür tragen, dass zum Beispiel beim erwünschten Erhalt von betrieblichen E-Mail-Newsletter die entsprechenden Absender-Adressen in ihr E-Mail-Adressbuch gespeichert werden, um fehlerhafte Klassifizierungen zu vermeiden.

11. Nutzung von E-Mail/Internet

Soweit nicht ausdrücklich eine Zustimmung des Unternehmens erfolgt ist, darf die Nutzung von E-Mail und Internet nur für dienstliche Zwecke erfolgen.

E-Mail-Adressen des Unternehmens dürfen nur für dienstliche Zwecke verwendet werden. Die Registrierung von Accounts oder Zugängen mit der E-Mail-Adresse des Unternehmens, die nicht im Zusammenhang mit der betrieblichen Tätigkeit stehen, ist zu unterlassen.

12. Verhalten bei Sicherheitsvorfällen

Sollte der Mitarbeiter merken, dass der Schutz oder die Sicherheit von Daten in irgendeiner Weise gefährdet sein könnte, hat dieser sich unverzüglich an die IT-Abteilung und seinen Vorgesetzten zu wenden. Dies gilt insbesondere dann, wenn die Gefährdung sich auf personenbezogene Daten bezieht.

13. Weisungen

Die Mitarbeiter sind verpflichtet, den Weisungen der IT-Abteilung Folge zu leisten.

ENDE DES DOKUMENTS