Einfache IT-Richtlinie

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 Festangestellte, Teilzeitangestellte, Auszubildende, Werkstudenten sowie Aushilfskräfte etc. Auch externe Personen, die regelmäßig in unserem 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.

Die IT-Richtlinie tritt am ……………… in Kraft.

3. Einhaltung von Rechtsvorschriften

Bei der Benutzung der IT-Systeme und Applikationen in unserem 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.

6. Arbeitsplatz

Der Arbeitsplatz ist von den Mitarbeitern so zu gestalten, dass Besucher 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“ bzw. den Arbeitsplatz-PC sperren, 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. 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 wird, soweit keine betrieblichen oder technischen Gründe entgegen sprechen, jedem einzelnen berechtigten Nutzer einen Benutzernamen sowie ein Passwort zuweisen.

Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist alphanumerisch (Buchstaben und Zahlen/Zeichen mit Sonderzeichen) zu gestalten.

Soweit technisch möglich ist jeder Mitarbeiter verpflichtet, sein Initial-Passwort unverzüglich zu ändern.

Die Passwörter sind so zu wählen, dass sie nicht durch Dritte leicht zu erraten sind. Vor-und Familiennamen oder Geburtstage sowie Namen von Angehörigen sind nicht zur Passwortwahl geeignet. Gleiches gilt für trivial angeordnete Zahlenkombinationen (z.B. 12345).

Passwörter sollten regelmäßig gewechselt werden. Bereits genutzte Passwörter dürfen nicht noch einmal wieder verwendet werden.

8. Schutz vor Schadinhalten

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

9. Schutz vor unverlangter Werbung („Spam“)

Zum Schutz vor unverlangter Werbung durch E-Mail werden im Unternehmen so genannte Spam-Filter eingesetzt. Der Einsatz des Spam-Filters erfolgt aus betrieblichen Gründen. 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 E-Mail-Newsletter die entsprechenden Absender-Adressen in ihr E-Mail-Adressbuch gespeichert werden, um fehlerhafte Klassifizierungen zu vermeiden.

10. 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.

Den Mitarbeitern kann gestattet werden, private E-Mails über ihren eigenen, privaten Webmail-Account zu empfangen und zu senden. Der Umfang dieser Nutzung kann aus betrieblichen Gründen vom Unternehmen eingeschränkt werden.

11. 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 den die IT-Abteilung (falls vorhanden) und seinen Vorgesetzten zu wenden. Dies gilt insbesondere dann, wenn die Gefährdung sich auf personenbezogene Daten bezieht.

12. Weisungen

Die Mitarbeiter sind verpflichtet, den Weisungen der Geschäftsführung / IT-Abteilung Folge zu leisten. Sofern Zweifel an der Richtigkeit oder der Sinnhaftigkeit von Weisungen der IT-Abteilung bestehen, kann der Leiter der IT-Abteilung oder die Geschäftsführung eingebunden werden.