

Firmenlogo, Briefkopf, ...

IT- Richtlinien

Diese Richtlinien regeln den Zugang, die Nutzung und die Sicherung von Software und Daten.

Zugang

Jeder Mitarbeiter hat im Rahmen seiner Möglichkeiten dafür zu sorgen, daß sein Rechner nicht durch Unberechtigte genutzt werden kann.

Der Benutzer einer Software hat dafür Sorge zu tragen, daß ihm bekannte Paßwörter nicht anderen Benutzern bekannt werden können.

Paßwörter sind in regelmäßigen Abständen zu ändern, es ist verboten Namen, Kalenderdaten, „leere“ Eingaben oder Einzelzeichen als Paßwörter zu verwenden.

Paßwörter dürfen keinesfalls in schriftlicher Form oder als lesbare Daten verwahrt werden.

Bei Verlassen des Arbeitsplatzes (auch zwischendurch) ist dafür zu sorgen, daß niemand Zugang zum System erhält.

Außer bei explizit für Gruppen definierten Benutzerkonten ist es grundsätzlich nicht zulässig, anderen Benutzern das eigene Paßwort zur Arbeit zur Verfügung zu stellen oder selbst unter Verwendung von Paßwörtern Anderer das System zu benutzen.

Nutzung

Die Nutzung der betrieblichen Rechenanlagen ist nur autorisierten Mitarbeitern und nur im Rahmen der für sie freigegebenen Anwendungen erlaubt.

Es ist verboten, Programme zu laden und zu benutzen, die nicht von einem Softwarebeauftragten für diesen Arbeitsplatz freigegeben wurden, die Nutzung ist weiters nur für dienstliche Zwecke gestattet.

Es darf nur die vom Arbeitgeber dem Mitarbeiter zur Verfügung gestellte Hard- und Software genutzt werden, Hard- und Software darf nicht von außen mitgebracht werden.

Es ist verboten Programme und Daten zu kopieren um sie außerhalb der Betriebsstätte zu nutzen oder an Dritte weiterzugeben.

Hard- und Software darf nur auf ausdrückliche Anweisung und für betriebliche Nutzung außer Haus mitgenommen werden.

Die Nutzung von Software unterliegt dem Urheberschutzgesetz.

Die Mitarbeiter können davon ausgehen, daß für sie installierte bzw. zur Verfügung gestellte Software lizenziert ist.

Die Installation von Programmen auf den Rechnern ist ausschließlich durch IT zulässig. In besonderen Einzelfällen können Programme nach Genehmigung durch IT selbst installiert werden. Diese Regelung gilt für alle Arten von Programmen – auch für sog. Freeware od. Shareware.

Datensicherung, Weitergabe von Daten

Kopien von zugekauften Programmen und Daten dürfen nur von Softwarebeauftragten und nur im für die Datensicherung notwendigen Umfang erstellt werden.

Kopien von firmeninternen Daten sind nur zum Zweck der Datensicherung bzw. für betrieblich erforderliche Zwecke zulässig.

Die Datenträger der Sicherung dürfen nicht am Arbeitsplatz gelagert werden, sie sind an den vorgeschriebenen Plätzen aufzubewahren.

Die veränderten Datenbestände müssen regelmäßig, jedoch mindestens wöchentlich und nach grundlegenden Änderungen gesichert werden.

Ist für die Arbeit an einem Projekt ein Verzeichnis auf einem Server vorgesehen, so sind die Daten des Projektes nur in diesem Verzeichnis abzulegen, die Sicherung auf lokale Datenträger entfällt dann; lokale Kopien der Daten sind nur für Testzwecke zulässig, nach Testende sind die Daten am Server zu aktualisieren und die lokalen Daten zu löschen.

Besondere Vorsicht ist bei der Weitergabe von Daten an Firmenfremde geboten. In unklaren Fällen ist vorab mit dem Vorgesetzten oder beim Leiter IT zu klären, ob die Weitergabe im Einklang mit den Firmeninteressen ist.

Nicht mehr benötigte Datenträger sind zu löschen oder an IT zur Löschung oder Zerstörung zu übergeben.

Für Ausdrucke auf Papier gelten sinngemäß dieselben Bestimmungen.

Datenfernübertragung

Die lokale Installation und Inbetriebnahme von Datenübertragungseinrichtungen (Modems u.a.) ist nur auf ausdrückliche Anweisung zulässig, die Genehmigung gilt nur im Rahmen eines Projektes für die Datenübertragung mit vorher vereinbarten Gegenstellen.

Wenn nicht anders vereinbart, sind Zeitpunkt und Dauer von aktiven und / oder passiven Verbindungsaufnahmen zu protokollieren.

Die Benützung der installierten Einrichtung durch Andere ist im Rahmen der gegebenen Möglichkeiten zu unterbinden (s. „Zugang“).

Viren

Unter Viren versteht man Programme, die sich selbst an andere Programme anhängen und damit verbreiten können. Außer ihrer Verbreitung haben sie meist den Zweck, Programme und Daten zu zerstören oder auszuspionieren (automatischer Versand sensibler Daten mittels e-mail u.a.).

Viren werden fast ausschließlich durch Programme oder Dokumente eingebracht die an e-mails angehängt sind, aus dem Internet geladen werden oder aus anderen, nicht autorisierten Quellen bezogen werden („Raubkopien“).

Die meisten Viren können durch sog. Antivirenprogramme entdeckt werden, die Entfernung ohne Datenverlust ist allerdings nicht immer möglich.

Zur besonderen Beachtung:

Die Schadwirkung von Viren wird unmittelbar bei der ersten Verwendung der befallenen Programme*) bzw. Daten in Gang gesetzt. Selbst ein Programm, das „nur“ ausprobiert wurde kann Schaden anrichten – ebenso wie Programme, die „nicht funktioniert“ haben weil „gleich eine Fehlermeldung gekommen“ ist, in diesem Fall kann das Programm bereits seine Schadwirkung gestartet und dann absichtlich einen Systemfehler herbeigeführt haben.

*) Unter „Programme“ sind alle ausführbaren Dateien – inkl. Bildschirmschoner u. dgl. Zu verstehen (Dateiendungen .EXE, .COM, .SCR).

E-mail

Besteht Zugang zum e-mail- System, können Daten mit anderen Rechnern bzw. deren Benutzern ausgetauscht werden.

Werden Daten oder Programme mittels e-mail übertragen, gelten sinngemäß die Bestimmungen des Absatzes „Datensicherung, Weitergabe von Daten“. Das Versenden oder empfangen von Dateien ist nur im Rahmen der Arbeit zulässig. Werden unverlangte Dateien empfangen sind diese zu löschen.

Die Geschäftsleitung behält sich das Recht vor, e-mails mit angehängten Dateien auf deren Inhalt zu prüfen.

Zugänge zu Rechnern und Netzwerken außerhalb der Abteilung

(Rechner anderer Abteilungen, Internet, ...)

Der Zugriff ist nur nach Erteilung einer entsprechenden Berechtigung gestattet bzw. möglich. Vor dem Herunterladen von Programmen und anderen ausführbaren Dateien ist mit einem Vorgesetzten Rücksprache zu halten.

Besteht Zugang zum Internet, dient das zur Erfüllung der Aufgaben im Unternehmen. Die Geschäftsleitung behält sich vor, die abgerufenen Seiten und Dateien in Stichproben zu kontrollieren und bei offensichtlichem Mißbrauch Einschränkungen zu definieren bzw. den Zugang zu sperren.

Der Zugriff auf abteilungsfremde Rechner ist ohne Berechtigung auch dann nicht gestattet, wenn die technischen Voraussetzungen dazu gegeben sind.

Entfernter Zugriff auf das Firmennetzwerk

(Einwahl, über Internet)

Nur berechtigte Mitarbeiter dürfen unter Verwendung geeigneter Schutzmaßnahmen (Paßwort, ggf. Rückruf) auf das Firmennetzwerk zugreifen.



Ich nehme zur Kenntnis daß Software nach dem Urheberrechtsgesetz sowohl unter zivil- als auch strafrechtlichem Schutz gestellt ist, für Verstöße dieses Gesetzes sieht der Gesetzgeber Strafen mit bis zu fünf Jahren Freiheitsentzug vor.

Ich erkläre hiermit die genannten Richtlinien in der vorliegenden Fassung zur Kenntnis genommen zu haben und verpflichte mich diese einzuhalten. Die Nichtbeachtung der Richtlinien zieht entsprechende arbeitsrechtliche Folgen nach sich.

Vorherige Fassungen dieser Richtlinien verlieren ihre Gültigkeit. Weiters bestätige ich die Übernahme einer Kopie dieser Richtlinien.

Name

Geburtsdatum

....., am

.....
Unterschrift