Nutzungsrichtlinie IT-Sicherheit

DIHK Deutscher Industrie- und Handelskammertag

#GemeinsamSicherHandeln

Inhaltsverzeichnis

1. Einleitung ---- 3
2. Verantwortung der Mitarbeiter ---- 3
3. Regelungen ---- 3
   3.1 Umgang mit Informationstechnologie ---- 3
   3.2 Zugangsdaten und Passwörter ---- 4
   3.3 Umgang mit Internet und E-Mail ---- 4
   3.4 Regeln für die Datenablage ---- 5
4. Folgen bei Verstoß ---- 5

1. Einleitung

Der Stellenwert der Informationstechnologie in unserer Firma nimmt weiter zu. Intern oder extern verursachte Einflüsse auf die IT können den Betriebsablauf erheblich beeinträchtigen oder Schaden verursachen. Die Folge kann der Verlust der Integrität, Vertraulichkeit und Verfügbarkeit von Daten, sensiblen Informationen und IT-Systemen sein. Die Ursache für schädlichen Einfluss auf die IT-Infrastruktur ist oftmals menschliches Fehlverhalten (bewusst oder unbewusst) und die unsachgemäße Nutzung der bereitgestellten IT-Ressourcen.

2. Verantwortung der Mitarbeiter

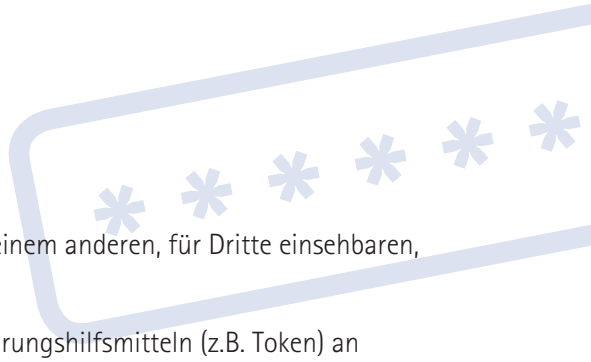
Alle Mitarbeiter sind verpflichtet, die Vorgaben dieser Nutzungsrichtlinie zu beachten. Diese Richtlinie wird allen Mitarbeitern bekannt gegeben und, wenn möglich, im Intranet veröffentlicht. Alle Mitarbeiter sind verpflichtet, an angebotenen Schulungen zur IT-Nutzung und zu IT-Sicherheitsthemen teilzunehmen. Bei Fragen zur IT-Nutzung und zur IT-Sicherheit wenden sich die Mitarbeiter an den oder die von der Geschäftsführung benannten Ansprechpartner.

3. Regelungen

3.1 Umgang mit Informationstechnologie

- ☐ Die Nutzung der bereitgestellten IT-Dienste ist nur zur Erledigung dienstlicher Aufgaben gestattet.
- ☐ Die Nutzung fremder und privater Geräte und Speichermedien (Notebook, Smartphone, USB Sticks, etc.) zu dienstlichen Zwecken ist ohne ausdrückliche Genehmigung nicht erlaubt.
- ☐ Es darf nur Software verwendet werden, die ausdrücklich zur Nutzung freigegeben wurde.
- ☐ Es ist nicht zulässig, eigenmächtig Änderungen an den Systemen vorzunehmen (Installation, Deinstallation, Konfigurationsänderungen etc.). Dies ist nur dem Administrator oder IT-Dienstleister gestattet.
- ☐ Das Betriebssystem sowie die Anwendungen sind stets auf aktuellem Stand zu halten.
- ☐ Beim Verlassen des Arbeitsplatzes ist darauf zu achten, Unbefugten den Zugriff auf Informationen und IT-Anwendungen nicht zu ermöglichen.
- ☐ Alle IT-Geräte sind mit einem Code bzw. Passwort vor unberechtigtem Zugriff zu sichern.
- ☐ Der Verlust eines Gerätes muss umgehend dem IT-Ansprechpartner gemeldet werden.
- ☐ Nicht genutzte Kommunikationsschnittstellen (WLAN, Bluetooth etc.) sind zu deaktivieren.
- ☐ Bei Außerbetriebnahme des Gerätes sind die gespeicherten Daten zu löschen, SD-Karten zu entnehmen und das Gerät auf den Werkszustand zurückzusetzen.

3.2 Zugangsdaten und Passwörter



- ☐ Zugangsdaten dürfen in schriftlicher Form nicht am Arbeitsplatz oder einem anderen, für Dritte einsehbaren, Ort aufbewahrt werden.
- ☐ Die Weitergabe von eigenen Zugangsdaten und sonstigen Authentifizierungshilfsmitteln (z.B. Token) an unautorisierte Dritte ist nicht zulässig.
- ☐ Das Passwort darf nicht leicht zu erraten sein. Namen, Kfz-Kennzeichen, Geburtsdatum usw. dürfen deshalb nicht als Passwörter gewählt werden.
- ☐ Ein Passwort sollte aus Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen bestehen. Es müssen mindestens zwei dieser Anforderungen umgesetzt sein.
- ☐ Das Passwort muss mindestens 12 Zeichen lang sein.
- ☐ Vorgegebene Passwörter müssen durch individuelle Passwörter ersetzt werden.
- ☐ Wichtige Passwörter müssen für die Hinterlegung schriftlich fixiert und sicher aufbewahrt werden (z.B. in einem Safe).
- ☐ Jedes Passwort muss geändert werden, wenn das Passwort einer unautorisierten Person bekannt geworden ist oder der Verdacht dazu besteht.
- ☐ Abgelaufene Passwörter dürfen nicht wieder verwendet werden.

3.3 Umgang mit Internet und E-Mail

- ☐ Internet und E-Mail dürfen nur benutzt werden, wenn das Betriebssystem aktuell ist, ein Virenschutzprogramm installiert und aktiv ist sowie die Virensignaturen aktuell sind.
- ☐ Die Konfiguration der Interneteinstellungen im Browser dürfen nicht eigenmächtig geändert werden.
- ☐ Es dürfen keine Angebote abgerufen oder Inhalte zugänglich gemacht werden, die pornografisch, rassistisch, gewalt- oder kriegsverherrlichend, ehrverletzend oder sonst wie rechts- oder sittenwidrig sind.
- ☐ Das Herunterladen und das Ausführen von Programmen oder von ausführbaren Programm-Codes aus dem oder über das Internet sind aus Sicherheitsgründen ohne vorherige Prüfung und Freigabe durch den IT-Verantwortlichen nicht erlaubt.
- ☐ Bei nicht identifizierbaren, fremdartigen bzw. bizarren E-Mails informieren und fragen Sie Ihren IT-Ansprechpartner, bevor Sie diese E-Mails öffnen oder bearbeiten.
- ☐ Beim Versand von nach außen gehenden E-Mails ist darauf zu achten, dass jede E-Mail mit einem passenden Betreff und geeigneter Absenderinformationen versehen ist.
- ☐ Vertrauliche Informationen, die per E-Mail nach extern versendet werden, müssen verschlüsselt werden. Sind die technischen Voraussetzungen nicht gegeben, sind alternative, sichere Versandwege zu nutzen.
- ☐ Die Weitergabe vertraulicher Informationen bedarf der Zustimmung des Eigentümers der Information.

3.4 Regeln für die Datenablage

- ☐ Firmendaten müssen primär auf Servern und dürfen nicht dauerhaft auf lokalen Laufwerken gespeichert werden.
- ☐ Werden sensible Daten auf mobilen Geräten oder Speichermedien gehalten, müssen die Daten verschlüsselt werden.
- ☐ Nicht mehr benötigte Daten und E-Mails sind zu löschen oder bei Bedarf zu archivieren.
- ☐ Nicht mehr benötigte Datenträger, die vertrauliche Informationen enthalten, sind unbrauchbar zu machen, sicher zu löschen und danach ggfs. fachgerecht zu entsorgen.
- ☐ Werden Datenträger vor der Entsorgung gesammelt (Container etc.), so sind diese vor unberechtigten Zugriff zu schützen.

4. Folgen bei Verstoß

Zuwiderhandlungen und Verstöße gegen diese Nutzungsrichtlinie können arbeitsrechtliche Konsequenzen nach sich ziehen. Die Geschäftsführung behält sich für jeden Verstoß gegen diese Nutzungsrichtlinie ausdrücklich arbeitsrechtliche Maßnahmen vor.