

Checkliste Mitarbeiter: Erfülle ich die wichtigsten IT-Sicherheitsrichtlinien?

Ja Nein

I Passwörter

- Sichere, starke Passwörter gewählt? (Groß-, Kleinbuchst., Ziffern, Sonderzeichen) Ja Nein
- Passwörter nicht älter als 3 Monate? Ja Nein
- Passwörter nicht weitergegeben, Stellvertreterfunktion genutzt? Ja Nein
- Evtl. notiertes Passwort sicher aufbewahrt? Ja Nein

II Sicherer Umgang mit dem Computer

- Schutz vor unbefugtem Zugriff auf IT-Systeme bei Abwesenheit gesperrt? Ja Nein
- Bildschirmschoner mit Kennwortschutz auf 5 Minuten eingestellt? Ja Nein
- Sicherheitsupdates für Betriebssystem und Anwendungen auf dem aktuellsten Stand(immer alle akzeptiert und baldmöglichst neu gestartet)? Ja Nein
- Anti-Virenprogramm aktiviert und Virendefinitionen aktualisiert? Ja Nein
- IT-Systeme nicht eigenmächtig verändert (Installationen)? Ja Nein
- Wird nur von Unternehmens-IT genehmigte Software eingesetzt? Ja Nein

III Nutzung von E-Mail / Internet

- Verantwortungsvoller Umgang mit E-Mail und Internet (geschäftl./private Nutzung)? Ja Nein
- Risikobewusster Umgang, z.B. bei E-Mails von unbekanntem Absendern mit unerwarteten Inhalten? Ja Nein
- Spam gecheckt? Ja Nein
- Etwaige Phishing-Angriffe an Helpdesk/Administrator gemeldet? Ja Nein
- Standard-Sicherheitseinstellung nicht geändert (z.B. Webbrowser) Ja Nein
- Vertrauliche E-Mail-Anhänge verschlüsselt, Passwort NICHT per E-Mail zum Empfänger übermittelt? Ja Nein

IV Umgang mit mobilen Geräten (Notebooks, PDAs, Handies, USB-Sticks)

- Schutz vor unbefugtem Zugriff gewährleistet, z.B. mit Laptop-Schloss? Ja Nein
- PDA, Handy, etc. bei Nicht-Benutzung verschlossen? Ja Nein
- Bluetooth-Funktion bei Handy ausgeschaltet? Ja Nein
- USB-Speichermedien (USB-Sticks) sicher aufbewahrt? Ja Nein
- Backup (z.B. lokaler Daten) regelmäßig durchgeführt? Ja Nein

Checkliste Mitarbeiter : Erläuterungen

Passwörter

Sichere, starke Passwörter?

Wählen Sie ein starkes, persönliches Passwort aus mind. 8 klug kombinierten Zeichen. Verwenden Sie Eselsbrücken, z.B.: „Es war einmal ein Passwort“ -> „Es war 1 mal 1 Pa\$wort“ -> „Ew1*1P\$w“

Passwörter erneuert?

Häufiger Passwortwechsel (min. alle 3 Monate) erhöht die Sicherheit sehr leicht.

Passwörter nicht weitergegeben?

Geben Sie Ihr persönliches Passwort NIE weiter. Bekannt gewordene Passwörter sofort ändern. Bei Abwesenheit Stellvertreterregelung für E-Mail-Postfach nutzen.

Passwörter aufgeschrieben?

Falls Sie Ihr Passwort aufschreiben, bewahren Sie es an einem sicheren Ort auf.

Sicherer Umgang mit dem Computer

Schutz vor unbefugtem Zugriff auf IT-Systeme bei Abwesenheit?

Sperren Sie Ihren PC bei jedem Verlassen des Arbeitsplatzes (Strg_Alt_Entf oder Windowstaste+L). Schalten Sie den PC nach der Arbeit aus und verschließen Sie Ihr Büro. Verwehren Sie Nicht-Berechtigten (Besucher, Dienstleister) den Zugang. Diese Sicherheitseinstellung schützt Ihren PC automatisch gegen unberechtigten Zugriff.

Bildschirmschoner mit Kennwortschutz auf 5 Minuten eingestellt?

Sicherheitsupdates für Betriebssystem und Anwendungen?

Durch das Einspielen der aktuellsten Sicherheitsupdates, sogenannten Patches, werden erkannte Sicherheitslücken Ihrer Software behoben.

Anti-Virensoftware ist aktiv mit aktuellen Virendefinitionen?

Guten Schutz erreichen Sie, wenn Sie Ihren Virens scanner immer aktiviert und durch neue Virendefinitionen aktuell halten - am besten durch automatische Aktualisierung.

IT-Systeme nicht eigenmächtig verändert (Installationen)?

Ändern Sie die Konfiguration Ihres Arbeits-PC nicht ohne Genehmigung der IT-Abteilung und schließen Sie ohne Genehmigung keine private Hardware oder mobile Endgeräte an das Firmen-Netzwerk an.

Wird nur von Unternehmens-IT genehmigte Software eingesetzt?

Installieren Sie Software auf Ihrem Arbeits-PC nur mit Erlaubnis der IT-Abteilung. Beachten Sie das Urheberrecht.

Nutzung von E-Mail / Internet

Verantwortungsvoller Umgang mit E-Mail und dem Internet (geschäftliche/private Nutzung)?

Verwenden Sie das Internet und E-Mail nur dienstlich und surfen Sie nicht auf zweifelhaften Internet-Seiten. (Infektionsgefahr durch Viren und böswärtigen Code). Berücksichtigen Sie das Urheberrecht. Denken Sie daran, dass Ihre E-Mails von anderen gelesen werden können, und richten Sie nie eine automatische E-Mail-Weiterleitung an externe Adressen ein.

Risikobewusster Umgang mit E-Mails?

Vorsicht bei E-Mails von unbekanntem Absendern bzw. mit unerwarteten Inhalten. Öffnen Sie NIE Anhänge solcher E-Mails.

Spam gecheckt?

Antworten Sie nie auf dubiose E-Mails (z.B. Spam) und leiten Sie diese auch nicht weiter. Eine Antwort auf Spam-E-Mails, das Anklicken von Links oder Grafik-anzeigen bestätigen dem Absender nur die Korrektheit Ihrer E-Mail Adresse. Überprüfen Sie den Spam-Ordner auf fälschlich aussortierte E-Mails.

Phishing Attacke gemeldet?

Geben Sie nie vertrauliche Informationen per E-Mail weiter, (z.B. PIN und TAN Ihres Kontos). Betrüger benutzen Phishing-Mails um Sie zu täuschen. Informieren Sie Ihren HelpDesk bzw. die IT-Abteilung – damit Ihre Kollegen gewarnt werden.

Standard-Sicherheitseinstellung?

Die Standardeinstellungen aktueller Anwendungen, z.B. Ihres Webbrowsers sind als sicher einzustufen. Verändern Sie diese Einstellungen nicht ohne „Not“.

Vertrauliche E-Mail-Anhänge verschlüsselt?

Vertrauliche Informationen sollten nur verschlüsselt und das Passwort NICHT per E-Mail übermittelt werden. Ihre IT-Abteilung berät zu technischen Möglichkeiten.

Umgang mit mobilen Geräten (Notebooks, PDAs, Handys, USB-Sticks)

Schutz vor unbefugtem Zugriff gewährleistet?

Schützen Sie mobile Geräte (z.B. Notebook, Blackberry) vor Diebstahl, verschlüsseln Sie vertrauliche Informationen. Nutzen Sie ein Laptop-Schloss.

PDA / Handy bei Nicht-Benutzung gesichert oder ausgeschaltet?

Aufgrund Ihrer Größe werden diese Geräte häufiger gestohlen bzw. verloren. Sicherung durch PIN oder durch Datenverschlüsselung ist hier besonders wichtig.

Bluetooth-Funktion ausgeschaltet?

Bluetooth-Geräte suchen Kontakt zu anderen Geräten mit gleicher Übertragungstechnik. Verhindern Sie den Zugriff auf Ihre Daten: aktivieren Sie es nur gezielt.

USB-Speicher sicher aufbewahrt?

Den kleinen USB-Stick verlegt man schnell. Bewahren Sie ihn immer sicher auf. Um Ihre Daten zu schützen, sollten Sie diese technisch verschlüsseln.

Regelmäßiger Backup lokaler Daten?

Extern (z.B. im Home Office) erstellte und lokal gespeicherte Daten sollten Sie eigenverantwortlich sichern.