Checkliste Mitarbeiter:
Erfülle ich die wichtigsten IT-Sicherheitsrichtlinien?

	Ja
Passwörter	
• Sichere, starke Passwörter gewählt? (Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen?)	☐
• Passwörter nicht älter als 3 Monate?	☐
• Passwörter nicht weitergegeben, Stellvertreterfunktion genutzt?	☐
• Evtl. notiertes Passwort sicher aufbewahrt?	☐
Sicherer Umgang mit dem Computer	
• Schutz vor unbefugtem Zugriff auf IT-Systeme bei Abwesenheit gesperrt?	☐
• Bildschirmschoner mit Kennwortschutz auf 5 Minuten eingestellt?	☐
• Sicherheitsupdates für Betriebssystem und Anwendungen auf dem aktuellsten Stand (immer alle akzeptiert und baldmöglichst neu gestartet)?	☐
• Anti-Virenprogramm aktiviert und Virendefinitionen aktualisiert?	☐
• IT-Systeme nicht eigenmächtig verändert (Installationen)?	☐
• Wird nur von Unternehmens-IT genehmigte Software eingesetzt?	☐
Nutzung von E-Mail / Internet	
• Verantwortungsvoller Umgang mit E-Mail und Internet (geschäftliche/private Nutzung)?	☐
• Risikobewusster Umgang, z.B. bei E-Mails von unbekannten Absendern, mit unerwarteten Inhalten?	☐
• Spam gecheckt?	☐
• Etwaige Phising-Attacke an Helpdesk/Administrator gemeldet?	☐
• Standard-Sicherheitseinstellung nicht geändert (z.B. Webbrowser)	☐
• Vertrauliche E-Mail-Anhänge verschlüsselt, Passwort NICHT per E-Mail zum Empfänger übermittelt?	☐
Umgang mit mobilen Geräten (Notebooks, PDAs, Handies, USB-Sticks)	
• Schutz vor unbefugtem Zugriff gewährleistet? Laptop-Schloss ("Kensington") angebracht?	☐
• PDA, Handy, etc. bei Nicht-Benutzung verschlossen?	☐
• Bluetoothfunktion bei Handy ausgeschaltet?	☐
• USB-Speichermedien (sog. USB-Sticks) sicher aufbewahrt?	☐
• Backup (z.B. lokaler Daten) regelmäßig durchgeführt?	☐

Checkliste Mitarbeiter : Erläuterungen

Passwörter

Sichere, starke Passwörter gewählt? 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 nicht älter als 3 Monate? Häufiger Passwort-Wechsel ist eine einfache Methode, um die Sicherheit zu erhöhen.
Passwörter nicht weitergegeben, Stellvertreterfunktion genutzt?
Geben Sie Ihr persönliches Passwort NIE weiter. Ändern Sie bekannt gewordene Passwörter sofort. Verwenden Sie bei Abwesenheit z.B. für Ihr Outlook-Postfach die Stellvertreterregelung.
Wenn Passwort aufgeschrieben, dann sicher aufbewahrt? Wenn Sie Ihr Passwort aufschreiben, dann bewahren Sie es an einem sicheren Ort auf.

Sicherer Umgang mit dem Computer

Schutz vor unbefugtem Zugriff - IT-Systeme bei Abwesenheit gesperrt?
Sperren Sie Ihren PC bei jedem Verlassen des Arbeitsplatzes (Strg_Alt_Entf oder Funktionstaste-Windows+L). Schalten Sie Ihren PC nach der Arbeit aus und schließen Sie - sofern möglich - Ihr Büro ab. Verwehren Sie Nicht-Berechtigten den Zugang zu IT-Systemen (z.B. Besucher, externe Dienstleister).
Bildschirmschoner mit Kennwortschutz auf 5 Minuten eingestellt? Diese Sicherheitseinstellung schützt Ihren PC automatisch gegen unberechtigten Zugriff.
Sicherheitsupdates für Betriebssystem und Anwendungen auf dem aktuellsten Stand? Erkannte Sicherheitslücken Ihrer Software werden durch ein Einspielen von Sicherheitsupdates, so genannten Patches, behoben.
Anit-Virensoftware ist aktiv und verwendet aktuelle Virendefinitionen? Schutz durch Vorbeugung erreichen Sie, wenn Sie Ihren installierten Virenscanner 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 bösartigen 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, z.B. bei E-Mails von unbekannten Absendern? Vorsicht bei E-Mails von unbekannten 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 die Grafikanzeige bestätigen dem Absender nur die Korrektheit Ihrer E-Mail Adresse. Überprüfen Sie den Spam-Ordner auf fälschlich aussortierte E-Mails.
Phising Attacke an Helpdesk/Administrator 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 – so können Ihre Kollegen gewarnt werden.
Standard-Sicherheitseinstellung nicht geändert (z.B. Webbrowser) Die Standardeinstellungen aktueller Anwendungen, z.B. Ihres Webbrowsers sind als sicher einzustufen. Verändern Sie diese Einstellungen nicht ohne „Not“.
Vertrauliche E-Mail-Anhänge verschlüsselt, Passwort NICHT per E-Mail zum Empfänger übermittelt? Vertrauliche Informationen sollten nur verschlüsselt übertragen werden. Zu den technischen Möglichkeiten fragen Sie Ihre IT-Abteilung.

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

Schutz vor unbefugtem Zugriff gewährleistet? Laptop-Schloss ("Kensington-Lock") angebracht? Schützen Sie mobile Geräte (z.B. Notebook, Blackberry) vor Diebstahl. Wenn möglich, verschlüsseln Sie vertrauliche Informationen.
PDA, Handy etc. 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.
Bluetoothfunktion bei Handy ausgeschaltet? Bluetooth-Geräte suchen den Kontakt zu anderen Geräten mit gleicher Übertragungstechnik. Verhindern Sie den unberechtigten Zugriff auf Ihre Daten: lassen Sie Bluetooth deaktiviert und schalten Sie es nur gezielt ein.
USB-Speichermedien sicher aufbewahrt? Den kleinen USB-Stick verlegt man schnell. Bewahren Sie ihn nach der Benutzung sofort sicher auf. Um Ihre Daten bei Verlust eines USB-Sticks zu schützen, sollten Sie diese - sofern technisch möglich – verschlüsseln.
Backup (z.B. lokaler Daten) regelmäßig durchgeführt Extern (z.B. im Home Office) erstellte und lokal gespeicherte Daten sollten Sie eigenverantwortlich sichern.