Mitarbeiterinformation zur Benutzung der IT Arbeitsplätze

Dokumentinformationen

☐ Prozess ☐ Dokumentation ☐ Checkliste ☒ Mitarbeiterinformation

☐ Strategie / Konzept ☐ Sonstiges

☒ Operativ ☐ Strategisch

Hauptgeschäftsprozess: Informationstechnologie

Ablage / Verzeichnis:

C:\Dokumente und Einstellungen\j.sommer\Desktop\Mitarbeiterinformation IT-Arbeitsplätze.doc

Datum der letzten Änderung 15.05.2009

Genehmigungsstatus

☐ Genehmigt durch die Geschäftsleitung Name:

☐ Genehmigt durch den IT-Administrator Name:

Verteiler: Alle Mitarbeiter

Inhaltsverzeichnis

Sehr geehrte Mitarbeiterinnen, sehr geehrte Mitarbeiter,

ein wichtiges Anliegen jeder IT-Abteilung besteht darin, für die Sicherheit der Daten zu sorgen. Zu den hierfür notwendigen Aufgaben gehört die Absicherung von Daten im Hinblick auf

- Authentifizierung (Schutz vor unerlaubtem Zugriff)
- Datenintegrität (Schutz vor Verfälschung) und
- Verfügbarkeit

Hiermit sind verschiedene technische Verfahren verbunden, die bei der Vergabe von Passwörtern und Sicherheitsrechten beginnen, Verfahren für Datensicherung und Virenschutz einschließen und die Bereitstellung hochverfügbarer Netzwerk- und Serversysteme beinhalten.

Die Bereitstellung technischer Mittel und Verfahren alleine genügt jedoch nicht, um umfangreiche Sicherheit zu erzielen. Sicherheit muss die davon betroffenen Personen einbeziehen und fordert einen professionellen und umsichtigen Umgang mit Daten, Zugriffen und Systemen.

Aus diesem Grunde benötigen wir Ihre Mitarbeit. Diese PC-Richtlinien beinhalten Anleitungen und Anweisungen für den sicheren Umgang mit Daten und Systemen für alle Mitarbeiter. Sie helfen uns auf diese Weise, für die Sicheheit Ihrer Daten, der Ihrer Kollegen und Mitarbeiter, sowie den Schutz der Daten zu sorgen.

Geltungsbereich

Diese PC-Richtlinien beziehen sich auf alle IT-Arbeitsplätze sowie alle Geräte, die Zugang zum internen Netzwerk haben. Hierzu gehören neben den PC-Arbeitsplätzen auch mobile Arbeitsplätze (Laptops, Palmtops, Pocket-PCs, Smartphones, etc.) sowie damit verbundene Geräte (USB-Sticks, Speicherkarten, Festplatten, Drucker, etc.).

Ansprechpartner

Bereich	Name	E-Mail	Telefon
Geschäftsleitung			
IT-Administration			
Datenschutz			

Anmeldung am Arbeitsplatz, Gebrauch von Passwörtern

Ihr Arbeitsplatz ermöglicht es Ihnen, die IT-Dienste und Programme zu nutzen, die für das Unternehmen und Ihren Arbeitsplatz frei gegeben sind und auf das Netzwerk zuzugreifen.

Bei der Anmeldung am System werden Sie durch Ihren Benutzernamen und Ihr Passwort authentifiziert. Damit sind Sie gegenüber dem System eindeutig identifiziert und erhalten Zugriff auf Daten im Rahmen Ihrer persönlichen Berechtigungen.

Aus diesem Grunde sind Passwörter und Zugangskennungen ausdrücklich geheim zu halten und dürfen an andere Personen in keinem Fall weitergegeben werden. Bitte geben Sie Passwörter und Zugangskennungen auch nicht aufgrund von e-Mailaufforderungen weiter. Einige Mailversender versuchen durch Sicherheitsmeldungen z.B. Zugangsdaten für Bankkonten, e-Bay-Konten o.ä. zu erfahren. Diese Mails verweisen auf eine betrügerische Internetseite und fordern in der Regel Benutzernamen, Kontonummer und Zugangsinformationen (z.B. PIN und TAN). Ihr Passwort ist der wichtigste und erste Schutz vor Datenmissbrauch und ein wichtiger Bestandteil der Unternehmenssicherheit. Angreifer versuchen daher in der Regel zuerst an Passwörter von Benutzern zu gelangen. Dies kann durch geschickt geführte Telefonanrufe geschehen, bei denen sich der Angreifer als interner Mitarbeiter ausgibt. Weitere Methoden versuchen auf technischem Wege Passwörter auszulesen.

Geben Sie daher Ihre Passwörter in keinem Fall weiter und speichern Sie diese niemals unverschlüsselt auf Ihrem Rechner (z.B. in Form von Outlook-Notizen oder in eigens angelegten Worddokumenten). Auch ist unbedingt zu verhindern, dass Passwörter für andere zugänglich notiert werden (z.B. in persönlichen Kalendern).

Wählen Sie Ihre Passwörter so, dass diese nicht ohne weiteres erraten werden können. Benutzen Sie Kombinationen von Sonderzeichen, Buchstaben und Zahlen. Ein sorgfältig gewähltes Passwort kann durch Fremde oder spezielle Programme kaum erraten werden.

Um sicherzustellen, dass Passwörter nicht missbraucht werden können, ist es notwendig, diese spätestens nach 90 Tagen zu ändern. Eine entsprechende Systemeinstellung fordert Sie dazu auf. Sollte der Verdacht bestehen, dass andere Personen Kenntnis von Ihrem Passwort erhalten haben, so wechseln Sie dieses bitte sofort.

Um einen Missbrauch Ihres Arbeitsplatzes auszuschließen, ist es außerdem notwendig, diesen gegen unbefugte Benutzung während Ihrer Abwesenheit zu schützen. Melden Sie sich daher bei längeren Abwesenheiten ab oder schalten Sie das System aus. Bei kurzen Arbeitsunterbrechungen und Abwesenheit sperren Sie das System gegen unbefugte Benutzung.

Vertretungsregeln

Es ist nicht gestattet, die eigene Zugangskennung und Passwörter an andere Personen weiterzugeben. Diese Regelung ist auch dann zu beachten, wenn Sie für einen längeren Zeitraum (z.B. Urlaub) nicht anwesend sind. Werden Daten von anderen Personen benötigt, so sind die jeweiligen Daten vorher an diese im Rahmen einer Übergabe zu übermitteln.

Werden Daten eines abwesenden Mitarbeiters dringend benötigt und ist es nicht möglich, diese Daten zu erhalten, so ist der Administrator berechtigt, Zugriff auf die Daten zu gewähren. Wir weisen noch einmal ausdrücklich darauf hin, dass keine privaten Dateien auf den Systemen zu speichern sind und alle Dokumente grundsätzlich Eigentum des Unternehmens sind.

Datenspeicherung

Daten, die sich in Ihrem Home-Verzeichnis und E-Mail-Postfach befinden, werden dreimal wöchentlich gesichert und sind anderen Personen nicht zugänglich. Bitte speichern Sie deshalb vertrauliche Daten in Ihrem Home-Verzeichnis. Daten, die auf Netzlaufwerk gespeichert werden, werden ebenfalls täglich gesichert; diese sind jedoch ausgewählten Benutzergruppen zugänglich.

Alle geschäftlich genutzten Daten sollen grundsätzlich im Netzwerk abgespeichert werden. Bitte speichern Sie keine geschäftlich genutzten Daten auf dem lokalen IT-Arbeitsplatz (z.B. Laufwerk C:), da Sie in diesem Falle über keinen Schutz vor Datenverlust und unberechtigtem Zugriff verfügen.

Es ist nicht gestattet, ohne betrieblichen Anlass Fremddaten im Netzwerk zu speichern.

Alle Daten und Dokumente, die während der Arbeit erstellt oder bearbeitet werden, sind Eigentum des Unternehmens.

Dauerhaftes Verlassen einer Stelle

Wenn Sie Ihre Stelle dauerhaft verlassen, ist dies mit der Deaktivierung Ihres Benutzerkontos verbunden. Es ist Ihnen dann nicht mehr möglich, auf Ihre Daten zuzugreifen. Bitte entfernen Sie daher grundsätzlich alle nicht geschäftlichen Daten aus Ihrem Home-Verzeichnis und Ihrem E-Mail-Postfach. In der Regel wird Ihre E-Mail-Adresse deaktiviert. Es ist jedoch möglich, dass Ihre eingehenden E-Mails zur Bearbeitung an einen anderen Mitarbeiter weitergeleitet werden und dieser Zugriff auf die E-Mails erhält. Da das e-Mailsystem ausschließlich der geschäftlichen Nutzung dient, behält sich die Geschäftsleitung vor, auf die e-Mailnachrichten Ihres Accounts zuzugreifen. Insbesondere in Fällen, die der Bearbeitung von Kundenanfragen dienen, kann dies der Fall sein.

Datenträger

Sofern Daten auf externen Datenträgern (USB-Sticks, Disketten, CD-ROM, etc.) gespeichert werden, ist vorher zu prüfen, ob hierfür ein betrieblicher Grund vorliegt. Sofern dies nicht der Fall ist, ist die Speicherung zu unterlassen. Die Speicherung vertraulicher Daten auf mobilen Datenträgern ist besonders sicherheitsrelevant, da die Gefahr des Missbrauchs und Abhandenkommens sehr hoch ist.

Werden Datenträger nicht mehr benötigt, so sind diese an den IT-Administrator zu übergeben, welcher die datenschutzgerechte Entsorgung sicher stellt. Im Falle des Verlassens Ihrer Arbeitsstelle sind alle in Ihrem Besitz befindlichen Datenträger an den IT-Administrator zu übergeben. Die Speicherung und Weiterverarbeitung von betrieblichen Daten auf privaten Systemen ist ausdrücklich untersagt.

Software

Software ist urheberrechtlich geschützt. Aus diesem Grunde darf Software nur mit ausdrücklicher Zustimmung des Herstellers installiert und genutzt werden. Die Grundlage für die Nutzung von Software ist der mit dem Hersteller abgeschlossene Lizenzvertrag, der die Anzahl der Installationen und die Nutzungsbedingungen regelt. Auf einem IT-Arbeitsplatz dürfen grundsätzlich nur lizenzierte und durch das Unternehmen freigegebene Programme installiert und genutzt werden. Zusätzliche Software muss daher per e-Mail an den IT-Administrator beantragt werden. Die Installation erfolgt ausschließlich durch von der Geschäftsleitung berechtigte Mitarbeiter oder mittels automatischer Installationsverfahren.

Es ist grundsätzlich nicht gestattet, Software selbständig und ohne Genehmigung auf einem Arbeitsplatz zu installieren. Dies gilt auch und besonders für Software, die möglicherweise keine Lizenz benötigt (sog. Freeware) oder deren Lizenz in Ihrem Privatbesitz ist. Außerdem ist es nicht gestattet, Software zu kopieren und diese für die private Nutzung auf anderen Systemen zu verwenden.

Um die Sicherheit und Funktionalität Ihres PCs zu gewährleisten, darf die Grundkonfiguration des IT-Arbeitsplatzes ebenfalls nur durch den IT-Administrator verändert werden.

Fernwartung des IT-Arbeitsplatzes

Der Zugriff von IT-Mitarbeitern auf den IT-Arbeitsplatz des Benutzers kann direkt vor Ort oder indirekt mittels Übernahme im Netzwerk erfolgen. Der IT-Administrator darf den IT-Arbeitsplatz nur nach Abstimmung mit dem Benutzer zur Fehlerbehebung, Wartung, Softwareeinspielung und Demonstration befristet übernehmen. Ein Zugriff auf vertrauliche Daten ist hiermit nicht verbunden. Der Fernzugriff auf eine Arbeitsstation erfolgt also nur im Beisein des Benutzers und nach dessen ausdrücklicher Zustimmung.

Hardware

Die Beschaffung, Installation und Wartung der Hardware wird ausschließlich durch den IT-Administrator übernommen. Private IT-Geräte und Datenträger dürfen grundsätzlich nicht eingesetzt werden.

Die Verbringung von IT-Equipment aus dem Firmengebäude sowie die Standortveränderung von nicht-mobilem IT-Equipment auch innerhalb des Firmengebäudes (z.B. Umbau von Tastaturen oder Druckern) ist ohne Zustimmung des IT-Administrators nicht gestattet.

Es ist den Nutzern nicht gestattet, unberechtigt den stationären IT-Arbeitsplatzrechner logisch oder physisch aus der Netzwerkumgebung zu entfernen oder auf andere Art dem Zugriff der Systemverantwortlichen zu unterbinden.

Service, Wartung und Reparatur

Service-, Wartungs- und Reparaturarbeiten sowie die Entsorgung defekter Geräte werden nur durch den IT-Administrator durchgeführt.

Um eine einwandfreie Kontrolle über die Systemumgebung und den einwandfreien Zustand der IT-Arbeitsplätze zu ermöglichen, ist es den Nutzern nicht gestattet, selbst Eingriffe in den normalen Systemablauf eines Rechners vorzunehmen, wie z.B. andere als die eigenen Geräte ohne Berechtigung ein- oder auszuschalten, Stecker, Tastaturen oder Mäuse abzuziehen.

Notwendige Reparaturen sind dem IT-Administrator (e-Mail) oder der Geschäftsleitung zu melden, der die weiteren Schritte veranlassen wird. Es ist Ihnen nicht gestattet, eigenständig Reparaturaufträge an externe Unternehmen zu vergeben.

Rückgabe des IT-Arbeitsplatzes

Sofern Ihr IT-Arbeitsplatz ausgetauscht wird, haben Sie eigenständig dafür Sorge zu tragen, dass sich auf dem Gerät keine persönlichen und produktiven Daten (Softwareprogramme sind hiervon ausgenommen) mehr befinden. Sollten sich dennoch Daten auf den Speichermedien befinden, übernimmt das Unternehmen für die Wiederherstellung der Dateien keinerlei Verantwortung.

Netzwerk

Jeglicher Zugang von und zu anderen Netzen wird ausschließlich durch das Unternehmen oder den IT-Administrator bereitgestellt. Es ist strengstens verboten, selbständig eigene Übergänge von und in andere Netze zu realisieren und zu betreiben, da hiermit eine massive Beeinträchtigung der Netzwerksicherheit verbunden ist.

Virenschutz

Viren stellen die größte Gefährdung von Daten und dar. Im Wesentlichen wird dies durch die Nutzung von e-Mail und Internet hervorgerufen. Daher ist auf allen IT-Arbeitsplätzen eine Antivirensoftware installiert, die über die aktuellsten Virensignaturen und Schutzmechanismen verfügt. Diese Software darf in keinem Fall deinstalliert oder deaktiviert werden. Selbst wenn hiermit persönliche Einschränkungen verbunden sind, dürfen die Einstellungen der Antivirensoftware keinesfalls geändert werden,

Gelegentlich werden durch den IT-Administrator Virenwarnungen herausgegeben. Beachten Sie diese unbedingt. Dagegen sind Virenwarnungen aus nicht zuverlässig informierten Quellen wie z.B. von Freunden oder Kollegen (die sich nicht professionell mit der Gefahr durch Viren beschäftigen) oftmals Falschmeldungen. Solche Falschmeldungen nennen sich HOAX. Ein HOAX ist eine bewusst in Umlauf gebrachte Falschmeldung, die das Ziel hat Verwirrung und Schaden zu verursachen. Die Meldung enthält oft neben der Gefahrenmeldung außerdem eine Beschreibung, wie Sie den Virus angeblich entfernen können (z.B. durch das Löschen einer speziellen Datei). **Löschen Sie niemals einfach aufgrund einer solchen E-Mail eine Datei von Ihrem Arbeitsplatzrechner.** Gerade das Löschen von Dateien durch den Benutzer ist das Ziel der Meldung und führt unter Umständen dazu, dass Ihr PC nicht mehr korrekt funktioniert oder schlimmstenfalls neu installiert werden muss. Sollten Sie eine Virenmeldung von jemand anderen als den im Unternehmen zuständigen Stellen erhalten, senden Sie die Warnung bitte nicht an Kollegen weiter.

E-Mail und Internet

Die Nutzung von E-Mail- und Internet-Diensten dient geschäftlichen Zwecken, sowie der Kommunikation der Beschäftigten untereinander. Jede Internetbenutzung, bei der die Gefahr besteht, den Interessen des Unternehmens oder dessen Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Gesetze oder Verordnungen verstößt, ist unzulässig. Die private Nutzung der IT-Arbeitsplätze ist ausdrücklich untersagt. Es wird ausdrücklich auf die Beachtung der gesetzlichen, dienstlichen und ethischen Grundsätze bei der Nutzung der E-Mail- und Internetdienste hingewiesen. Nichtbeachtung und insbesondere vorsätzlicher Missbrauch können zu dienstlichen und rechtlichen Konsequenzen führen.

Aus technischen Gründen und zur Sicherstellung des ordnungsgemäßen Betriebs der E-Mail- und der Internet-Dienste werden personenbezogene Daten (Protokoll- oder Verbindungsdaten) gespeichert. Diese müssen der besonderen Zweckbindung gemäß Datenschutzgesetz *"personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden"* unterliegen. Treten beim Betrieb von E-Mail- und Internet-Diensten - insbesondere durch zweckwidrige Nutzungen - Störungen und Beeinträchtigungen auf, behält sich die Geschäftsleitung unter Beachtung des Datenschutzgesetzes eine Sichtung und Kontrolle der Protokoll- und Verbindungsdaten vor.

Personenbezogene Daten (Protokoll- oder Verbindungsdaten), die bei der Nutzung der E-Mail- und Internetdienste gespeichert werden, dürfen nicht zu einer Leistungs- und Verhaltenskontrolle verwendet werden.

E-Mail

Das Abrufen von E-Mails von externen E-Mail-Providern (z.B. web.de, gmx.de. oder hotmail.com) ist aus Gründen der Sicherheit (z.B. Virenschutz) verboten. Eine automatische Weiterleitung von E-Mails an externe E-Mail-Accounts ist nicht gestattet.

Bitte beachten Sie, dass das eingesetzte E-Mailsystem kein Authentifizierungsverfahren einsetzt, welches die Identität eines Absenders immer eindeutig sicherstellt. Dieses ist auch aus technischen und organisatorischen Gründen nicht möglich, da dies immer der Zustimmung und Mitarbeit des Absenders bedarf. Aus diesem Grunde prüfen Sie bitte bei wichtigen Meldungen und bei berechtigten Zweifeln die Identität des Absenders, indem Sie dort nachfragen. Es ist technisch ohne weiteres möglich, den Absender einer E-Mail zu fälschen und in dessen Namen gefälschte Meldungen zu verschicken. Einige Viren machen hiervon Gebrauch, indem Sie Viren-befallene Dateien unter falschem Namen an bekannte E-Mailadressen versenden.

Beim Versenden vertraulicher Informationen ist darauf zu achten, dass diese nur in geeigneter Weise verschlüsselt übertragen werden. Fragen Sie gegebenenfalls den IT-Administrator nach geeigneten Maßnahmen, um die Integrität und den Schutz der Daten beim Versand über E-Mail zu gewährleisten.

Beim Versenden personenbezogener Daten sind die jeweiligen Bestimmungen zum Datenschutz zu beachten.

Internet

Alle Mitarbeiter sind zu einem vorsichtigen Umgang mit WWW-Inhalten verpflichtet. Der Zugang zum Internet von einem IT-Arbeitsplatz muss immer geschützt durch eine Firewall erfolgen. Dies ist im Unternehmensnetzwerk der Fall.

Der Aufruf von Seiten mit strafrechtlich relevanten oder sittenwidrigen Inhalten (z.B. rassistische, frauenfeindliche, pornographische oder rechtsgerichtete Inhalte) ist nicht gestattet. Grundsätzlich ist jegliche Privatnutzung untersagt.

Mobile Geräte (z.B. Notebooks, PDAs, Smartphones, Handys)

Mobile Geräte müssen besonders gegen Diebstahl geschützt werden. Der Zugriff zu den Geräten muss durch ein Kennwort/PIN oder ein geeignetes Authentifizierungsverfahren abgesichert werden. Sollte dies nicht möglich sein, dürfen keine sensiblen Informationen darauf gespeichert und verarbeitet werden.

Zur Sicherung der lokalen Daten von mobilen Geräten muss eine regelmäßige Synchronisation mit den zentralen Servern durchgeführt werden. Hierfür ist der Besitzer des Gerätes selbst verantwortlich. Bitte achten Sie insbesondere bei Synchronisation mit zentralen Datenlaufwerken darauf, dass hierbei keine Serverdaten überschrieben werden, die von anderen Personen benötigt werden.

Bitte kontaktieren Sie bei Fragen zu diesem Leitfaden die unter „Ansprechpartner“ genannten Personen. Durch die Beachtung der obigen Sicherheitsmaßnahmen unterstützen Sie unser Unternehmen bei der Aufrechterhaltung der Datensicherheit und der Verfügbarkeit der IT-Systeme.

Impressum

Erstellungsdatum: 15.08.2009

Autor: Dr. Jochen Sommer, Herausgeber: Sommer-Solutions GmbH