Merkblatt – IT-Richtlinien für Beschäftigte

Vorwort

Dieses Merkblatt soll Sie als MitarbeiterIn anhand von systematisch aufgebauten Richtlinien auf konkrete Risiken und Gefahren im Zusammenhang mit der IT-Nutzung aufmerksam machen, einen kompakten und allgemein verständlichen Überblick über das Thema Informationssicherheit geben und zu Eigenverantwortung motivieren.

Beachten Sie: Keine Richtlinie kann alleine alle denkbaren Gefahrensituationen berücksichtigen. Deshalb gilt vor allem: Seien Sie wachsam, denken Sie mit und machen Sie sich stets die vielfältigen Informationssicherheitsrisiken bewusst, mit denen Sie im Arbeitsleben immer wieder konfrontiert sein werden.

Helfen Sie bitte aktiv mit, die sensiblen, oft gesundheitsbezogenen Daten unseres Unternehmens zu schützen. Befolgen Sie in Ihrem täglichen Umgang mit personenbezogenen Daten jederzeit die in diesem Merkblatt benannten Verhaltensregeln.

1. Allgemeine Sicherheitsbestimmungen

Das Verändern von Einstellungen, die bei Installation der PCs, Laptops oder in der (Terminal-) Serverumgebung durch die IT-Abteilung vorgenommen wurden, sowie das Einbringen zusätzlicher Programme (Software) sind nicht gestattet. Dazu gehört auch das Herunterladen von Programmen aus dem Internet. Die Lizenzbedingungen von Softwareherstellern sind einzuhalten.

Es ist unter keinen Umständen gestattet, die Windows-Firewall oder Virenschutzprogramme zu deaktivieren.

Störungen oder Schäden an den IT-Geräten sind unverzüglich zu melden.

Alle sicherheitsrelevanten Ereignisse (z.B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verfügbarkeit nicht explizit freigegebener Dienste, Verdacht auf Missbrauch der eigenen Benutzerkennung usw.) sind sofort an den IT-Verantwortlichen oder den/die Vorgesetzte/n zu melden.

Beim Umgang mit den IT-Ressourcen ist jeder Mitarbeiter angehalten, die IT-Geräte pfleglich zu behandeln und mit den Ressourcen sparsam umzugehen. Das betrifft auch den wirtschaftlichen Verbrauch von Speicherplatz auf den Servern und von Verbrauchsmaterialien wie Druckerpapier, Druckfolien, Druckerpatronen usw.

Die betriebliche IT-Infrastruktur dient ausschließlich der betrieblichen Nutzung.

Die Nutzung der IT für private Zwecke ist untersagt. Dies betrifft sowohl die Nutzung der Geräte an sich (PC, Laptop, Smartphone…) als auch Ihr Firmenpostfach (E-Mail) und den Firmeninternetanschluss. Sollte die private Nutzung von Ihrer Seite notwendig sein (z. B. privater E-Mail Abruf über den privaten E-Mail Account), holen Sie sich bitte eine schriftliche Ausnahmebestätigung von Ihrem Vorgesetzten ein.

2. Clear Desk Policy

Unter der Clear-Desk-Policy versteht man, dass Mitarbeiterinnen und Mitarbeiter alle vertraulichen Dokumente, die sich auf ihrem Arbeitsplatz befinden, verschließen. Unberechtigte Personen (Reinigungspersonal, unbefugte Kolleginnen und Kollegen oder Besucher) dürfen keinen Zugriff darauf erhalten.

Bei Verlassen des Arbeitsplatzes müssen alle Ausdrucke, Kopien oder dergleichen - mit vertraulichem Inhalt - so verstaut werden, dass diese Dokumente nicht für Dritte zugänglich sind.

Lassen Sie keine Ausdrucke im Drucker/Kopierer liegen.

Bewahren Sie unter keinen Umständen Passwortnotizen an Ihrem Arbeitsplatz auf.

Sperren Sie Ihren Computer, wenn Sie Ihren Arbeitsplatz verlassen (z. B. unter Windows mit „Windows-Taste + L“)! Unbeaufsichtigte, nicht gesperrte Computer sind ein hohes Sicherheitsrisiko. Unbefugte könnten so Zugang zu vertraulichen Daten erhalten.

3. Umgang mit Passwörtern

Stellen sie sich ein Passwort wie einen Schlüssel zu ihrer Wohnung oder zu ihrem Haus vor. Zuhause möchte sie auch ein gutes Schloss besitzen, welches vor einem unbefugten Zutritt schützt. Genauso verhalten sich auch Passwörter. Passwörter schützen vor unbefugten Zutritt.

Geben Sie ihr Passwort an niemanden weiter, auch nicht an Ihre ArbeitskollegInnen.
Auch die IT-Administratoren benötigen ihr Kennwort nicht.

Verwenden Sie nie das gleiche Passwort für unterschiedliche Zugänge.

Verwenden sie Kennwörter, die mindestens 8 Zeichen haben. Ein Passwort muss aus Großbuchstaben, Kleinbuchstaben, Ziffer und einem Sonderzeichen bestehen um halbwegs sicher zu sein.

Niemals *Namen, Vornamen, Geburtsdaten, Tel.-Durchwahlen etc.* verwenden. Diese werden bei Angriffen zuerst ausprobiert.

Verwenden sie keine Begriffe aus einem Wörterbuch (auch nicht in einer anderen Sprache). Es gibt Programme, die Wortlisten mit mehreren tausend Begriffen sofort abrufen und so mögliche Passwörter finden. Auch Eigennamen, geografische Begriffe etc. dürfen nicht verwendet werden. Trivial-Passwörter (hallohallo, abcdefgh, 08/15, 1234 etc.) sind ebenfalls ungeeignet. Sie können von Anderen leicht beim Beobachten der Passworteingabe erkannt werden.

Überlegen Sie sich einen Satz und verwenden sie nur die Anfangsbuchstaben für Ihr Passwort.

- *Die Arbeit beginnt jeden Tag um 7 Uhr - DAbjTu7U*
- *Am Samstag arbeite ich von 9 bis 13 Uhr - ASaiv9-13U*

Sie sind für Ihr Kennwort verantwortlich! Sollten Sie den Verdacht haben, dass ein unbefugter Dritter Ihr Kennwort kennt, ändern Sie dieses sofort, bzw. setzen Sie sich mit Ihrer IT-Administration in Verbindung.

4. Dokumente und Datenträger richtig entsorgen

Sorglos weggeworfene Dokumente stellen ein ernstes Sicherheitsproblem dar, wenn diese Daten in falsche Hände geraten. Aus diesem Grund müssen Dokumente, Datenträger (USB Stick, Festplatte, SD-Karte, CD/DVD…) sicher entsorg werden.

Werfen Sie Datenträger oder wichtige Dokumente auf keinen Fall in den Papierkorb! Sofern es sich um Inhalte handelt, die Außenstehenden nicht zugänglich gemacht werden dürfen, müssen die Datenträger und Dokumente sicher entsorgt werden. Beachten Sie, dass diese Vorgehensweise auch bei Archivmaterial einzuhalten ist.

Auf zurückgegebenen, nicht mehr verwendeten Endbenutzergeräten (PCs, Laptops, …) und Datenträgern gespeicherte Daten werden ausschließlich von der IT-Abteilung physisch gelöscht.

5. Datenspeicherung

Bitte versichern sie sich, dass Daten nur an den dafür definierten Bereichen gespeichert werden. Die Daten müssen an Standorten mit einer Serverinfrastruktur immer auf einem Netzlaufwerk gespeichert werden. **Die Datenspeicherung auf dem Desktop ist nicht zulässig.**

Die Nutzung der Cloud-Sharing-Dienste iCloud, Dropbox (Datenablage auf dem Online-Speicher im Internet) ist für personenbezogene und betriebliche Daten (Texte, Bilder) nicht zulässig. Sonderregelungen gelten für die betrieblich genutzten Online IT-Anwendungen (s. auch Punkt 11)

Die Speicherung von Betriebsdaten sollte grundsätzlich so vorgenommen werden, dass bei Ausfall eines Mitarbeiters dessen Vertretung oder der/die Vorgesetzte auf diese Daten zugreifen kann (Gruppenverzeichnisse / Netzlaufwerke). Namen für Ordner oder Dokumente sollen eindeutig gewählt werden, damit Dokumente auch von KollegInnen schnell geortet werden können.

Bei der Datenspeicherung, insbesondere von Bildern und Videos, sollte das erzeugte Datenvolumen kritisch geprüft werden. Alte, nicht mehr erforderliche Dateien, Bilder sowie E-Mails sollen regelmäßig gelöscht werden, um die Speicherkapazitäten im System frei zu halten.

6. E-Mail-Nutzung

E-Mail gehört schon fast zur Standardausrüstung eines Arbeitsplatzes. Dadurch lohnt es sich auch für Kriminelle, diese Form der Kommunikation zu nutzen. Somit landen aber auch Spam-, Hoax- oder Phishing-Mails sowie mit Schadprogrammen verseuchte Nachrichten in Ihrem Posteingang.

Öffnen Sie keine E-Mails, wenn Ihnen Absender oder Betreffzeile verdächtig erscheinen.

Öffnen Sie niemals Dateianhänge, die Ihnen verdächtig vorkommen. Auch bei vermeintlich bekannten und vertrauenswürdigen Absendern ist zu prüfen: Passt der Text der E-Mail zum Absender (englischer Text von deutschsprachigem Absender, unsinniger Text, fehlender Bezug zu aktuellen Vorgängen etc.)? Erwarten Sie die beigelegten Dateien und passen die Dateien zum Absender, oder kommen diese völlig unerwartet?

Öffnen Sie keine E-Mails mit Spaßprogrammen, da diese Schadsoftware enthalten können.

Sogenannte Phishing-Mails, die zur Übermittlung von persönlichen Online-Banking-Daten oder Passwörtern (z.B. PIN oder TAN) auffordern, müssen gelöscht werden. Die angeforderten, vertraulichen Informationen dürfen Sie auf keinen Fall weitergeben.

Oftmals kann in einer E-Mail ein Link angeklickt werden, um eine Webseite aufzurufen. Seien Sie dabei vorsichtig: In betrügerischen E-Mails wird in diesen Links oft eine völlig andere Internet-Adresse hinterlegt, als in Mails zu sehen ist. Beim Anklicken wird dann eine gefälschte Phishing-Webseite aufgerufen oder sogar Schadsoftware installiert. Sicherer ist es, den Link mittels „Hyperlink kopieren“ in den Browser zu übertragen und ihn vor dem Aufrufen noch einmal zu überprüfen.

Beantworten Sie keine Spam-Mails! Die Rückmeldung bestätigt dem Spam-Versender nur die Gültigkeit Ihrer Mail-Adresse und erhöht dadurch Ihr Risiko, weitere Zusendungen zu erhalten. Das Abbestellen von E-Mails ist nur bei seriösen Zustellern sinnvoll.

Benachrichtigen Sie auch Ihre KollegInnen über verdächtige Zusendungen. Besprechen Sie die aktuellen E-Mails, die sie als Phishing-Versuche oder Virus-Mails erkannt haben, um gemeinsam die typischen Kennzeichen kennenzulernen. Sie können auf diese Weise sehr rasch Ihre Erkennungsfähigkeit trainieren und verbessern.

Das Versenden von E-Mails mit Anhängen von mehr als 8 MB ist zu unterlassen.

7. Internet Nutzung

Auch beim normalen Surfen im Internet liegen Gefahren und Risiken, die nicht gleich als solche erkannt werden. Es liegt in ihrer eigenen Verantwortung, solche Bedrohungen zu erkennen und entsprechend darauf zu reagieren.

Übermitteln Sie keine persönlichen Daten, vor allem nicht, wenn die Verbindung nicht als Sicher (http**s**://) markiert wird.

Das Herunterladen von Dateien (auch Musik, Videos) kann - abgesehen von der Gefahr des Einschleppens von Schadsoftware - auch zu lizenz- und urheberrechtlichen Problemen führen. Das gilt auch für Software, die nicht installiert oder ausgeführt wurde, und nur auf dem PC gespeichert ist.

Meiden Sie Hackerseiten und solche, auf denen kommerzielle Software, möglicherweise in gecrackter Form, zum Download angeboten wird.

Rufen Sie keine Websites mit pornografischen, gewaltverherrlichenden oder strafrechtlich bedenklichen Inhalten auf. Das kann gravierende rechtliche Probleme – für Sie aber auch für das Unternehmen – nach sich ziehen.

Ferner dürfen Inhalte, die dem Ansehen oder dem Erscheinungsbild der Reha-Südwest und deren Töchter schaden, nicht verbreitet werden.

Im Rahmen der Nutzung von Internetinhalten dürfen weder im Namen der Unternehmen der Reha-Südwest für Behinderte gGmbH und deren Tochterunternehmen noch im Namen anderer Personen Vertragsverhältnisse eingegangen werden.

8. Datenschutz

Das „Mit-Sich-Führen“ von sicherheitskritischen Daten (auch auf USB-Sticks, CD/DVD, externen Festplatten, ...) ist nur in abgeschlossenen Taschen/Koffern und nur bei beruflicher Notwendigkeit gestattet. Innerhalb der Geschäftsräume sind derartige Speichermedien bei (auch nur zeitweiser) Abwesenheit unter Verschluss zu halten.

Der Verlust oder Diebstahl von PCs, Laptops, mobilen Endgeräten oder anderen IT-Geräten ist unverzüglich der IT-Administration zu melden.

Bei Versenden von externen Massenmails verwenden Sie die BCC: Funktion

Bilder oder sonstige urheberrechtlich geschützte fremde Inhalte (z. B. Audio- und Videodateien, ggf. auch Texte) dürfen nur mit Zustimmung des Urhebers veröffentlicht sowie dauerhaft auf Datenträgern gespeichert werden. Es gilt das Recht am eigenen Bild bzw. Werk.

9. Nutzung von Social-Media (Soziale Medien) und öffentlicher Messenger-Dienste

Soziale Medien wie Whats-App, Facebook, Instagram, Twitter, Snapchat und Co erfreuen sich großer Beliebtheit. Speziell für Firmen werden soziale Medien mehr und mehr zum Problem in Punkto Sicherheit. Dieses Sicherheitsproblem wird meist ungewollt von Mitarbeitern verursacht, die nur schnell mal eine Information austauschen wollen, oder nur kurz ein Bild weiterleiten möchten.

Informationen über unser Unternehmen und Öffentlichkeitsarbeit im Zusammenhang mit der Arbeit in unserem Unternehmen werden in sozialen Medien nur von den zuständigen betrieblichen Stellen geteilt.

Ohne ausdrückliche Genehmigung ist die Weitergabe von personenbezogenen Daten, Fotos und Videos über soziale Medien nicht gestattet.

Posten Sie keine Fotos von ihrem Arbeitsplatz. Posten Sie keine Statusinformationen, die das Unternehmen betreffen. Geben Sie in keinen Foren oder sozialen Medien irgendwelche Informationen über das Unternehmen, in dem Sie arbeiten, preis.

Messenger-Dienste erfüllen aufgrund ihrer Allgemeinen Geschäftsbedingungen nicht die Voraussetzungen für eine rechtssichere digitale Kommunikation. Eine rechtssichere Kommunikation ist für uns jedoch unter Beachtung der Persönlichkeitsrechte, des Datenschutzes sowie unseres Anspruchs an eine professionelle Kommunikation zwingend geboten.

Eine Kommunikation über öffentliche Messenger-Dienste ist kein offizieller Dienstweg für den Kontakt zum Arbeitgeber, zu Kollegen und Kolleginnen oder Familien. Für diese Zwecke steht die betriebliche Online IT Anwendung schul.cloud zur Verfügung (s. Punkt 11).

10. Spezielle Regelung für die Nutzung mobiler Endgeräte (Smartphone, Laptop, Tablet)

Ein Smartphone, Laptop, oder Tablet ist ein mobiles Arbeitsgerät, das sehr leicht an unterschiedlichen Standorten für die tägliche Arbeit genutzt werden kann. Naturgemäß werden diese Geräte häufiger gestohlen oder verloren als stationäre PCs.

Für die Nutzung dieser Geräte gilt eine gesonderte Verfahrensanweisung (VA IT/13/001). Von den NutzerInnen wird eine Übergabebestätigung angefordert und die Übergabe wird formell dokumentiert (Formular IT/13/503).

11. Spezielle Regelung für die Nutzung von betrieblichen Online IT-Anwendungen

Im Rahmen der kollaborativen[1] Büro- und Teamarbeit werden unternehmensweit auch Online IT-Anwendungen eingesetzt. Diese sind Teil der digitalen Infrastruktur und digitalen Datenverarbeitung.

Für die Nutzung der Online IT-Anwendungen gelten spezifische Nutzungsbestimmungen welche in einer gesonderten Verfahrensanweisung (VA IT/13/002) erfasst sind. Dort werden die Anwendungen auch beschrieben und relevante Informationen zum Datenschutz und zur Datensicherheit benannt. Die Nutzung ist an die Einwilligung in die Nutzungsbestimmungen und eine Datenschutzerklärung gebunden. (Formular IT/13/504).

[1] Digitale, Vernetzte Form der Zusammenarbeit

12. Regelung für den externen Datenzugriff per VPN im Home-Office

Diese Regelungen gelten für den Fall, dass Sie als MitarbeiterIn Zugriff über VPN (Virtuelles Privates Netzwerk) bekommen.

Die Zugangsberechtigung darf nur zur persönlichen Nutzung verwendet werden und darf Dritten nicht zugänglich gemacht werden. Bei dem Verdacht auf eine Nutzung der Zugangsberechtigung durch Dritte ist der Bereich IT unverzüglich zu informieren.

Der VPN-Zugang darf nur über Endgeräte und VPN-Software erfolgen, die von Reha-Südwest für Behinderte gGmbH bereitgestellt wurden.

Insbesondere müssen Schutzvorkehrungen ergriffen werden, um die Verbreitung von unternehmerischen Daten durch den externen Zugriff an unbefugte Dritte oder über Schadprogrammen zu verhindern.

Die Übertragung von betrieblichen Daten während des externen Zugriff auf private Datenspeicher oder Geräte ist nicht gestattet.

Benutzernamen und Kennwörter dürfen bei der Herstellung der Datenverbindung nicht automatisch gespeichert werden. Entsprechende Meldungen des Fremdsystems sind stets mit einer Verneinung zu beantworten.

Es ist darauf zu achten, dass nach Beendigung der Nutzung die Datenverbindung zu den betrieblichen Systemen ordnungsgemäß beendet wird.

13. Austritt aus dem Unternehmen

Bei Austritt aus dem Unternehmen behält sich der Arbeitgeber das Recht vor, E-Mail-Adressen des ausscheidenden Mitarbeiters weiter zu verwenden, um den Unternehmensablauf nicht zu beeinträchtigen. Darüber hinaus verpflichtet sich der Mitarbeiter, sämtliche Dokumente, IT-Equipment und Unterlagen bei Austritt unaufgefordert dem Unternehmen bereitzustellen.

In einem Beschäftigungsverhältnis ist in der Regel der Arbeitgeber der Inhaber des generierten Geistigen Eigentums. Speziell im Hinblick auf Dokumente, Berechnungen oder dergleichen ist dies ein wesentlicher Punkt.

Eine willkürliche Löschung von Dokumenten, E-Mails oder sonstigen firmenrelevanten Daten ist strengstens untersagt.

14. Nutzung privater Datenverarbeitungsgeräte (IT-Geräte) für dienstliche Zwecke durch pädagogische Fachkräfte

Die Nutzung von privaten IT-Geräten für betriebliche Zwecke jeder Art ist auch für Lehrkräfte und andere pädagogische Fachkräfte nicht mehr gestattet. Die zur Verfügung gestellten betrieblichen Endgeräte (IPads) sind zu verwenden.

Die gilt auch für die Aufnahme von Videos oder Bildaufnahmen, also den Einsatz von Video(Kameras).

Die schülerbezogene Datenverarbeitung und Verwaltung (Zeugnisse, Berichte, Korrespondenz, Gutachten, …) ist ausschließlich über die eingesetzte pädagogische Softwareanwendung (Virtueller Lernbegleiter) vorzunehmen.

15. IT-Nutzung durch Klienten (Bereich: Schule, Internat)

Die schulische IT-Infrastruktur darf nur für schulische Zwecke genutzt werden. Als Nutzung zu schulischen Zwecken ist neben Arbeiten im Rahmen des Unterrichts auch die Nutzung zum Zwecke der Ausbildungs- und Berufsorientierung anzusehen.

Die schulische IT-Infrastruktur in Internaten darf neben der Nutzung für Ausbildungszwecke auch im allgemeinen Freizeitbereich verwendet werden.

Schülerinnen und Schüler einer Einrichtung sind über die IT-Nutzungsstandards in geeigneter Art und Weise zu informieren, aufzuklären und aktuell zu halten.

Aufsichtführende Personen sind zur Erfüllung ihrer Aufsichtspflicht verpflichtet! Dies beinhaltet, die Inhalte von aufgerufenen Webseiten zu kontrollieren.