Firmenvereinbarung 2024

© Software4You Planungssysteme GmbH

Inhalt

[1 Urlaubsregelung 4](#_Toc163722261)

[2 Sonderurlaub 4](#_Toc163722262)

[3 Krankmeldung 4](#_Toc163722263)

[4 Arbeitszeit 5](#_Toc163722264)

[5 Zahlungstermine 5](#_Toc163722265)

[6 Abwesenheit 5](#_Toc163722266)

[7 Privateigentum 5](#_Toc163722267)

[8 Firmeneigentum 5](#_Toc163722268)

[9 Kündigung 6](#_Toc163722269)

[10 Geheimhaltung 6](#_Toc163722270)

[11 Datenschutz und Vertraulichkeit der Informationen 6](#_Toc163722271)

[12 Reisekostenabrechnung 7](#_Toc163722272)

[13 Zugangskontrolle 7](#_Toc163722273)

[14 Schlussbestimmung 8](#_Toc163722274)

[Anlage A: Maximen (Corporate Behaviour) 9](#_Toc163722275)

[Anlage B: Regeln zur Kommunikation via E-Mail und Teams 12](#_Toc163722276)

[Anlage C: Firmenvereinbarung zur Nutzung der Internet und E-Mail Dienste der Software4You Planungssysteme GmbH 15](#_Toc163722277)

[Anlage D: Firmenvereinbarung zur Wiederverwendung, Löschung, Entsorgung oder Rückgabe von Datenträgern bei der Software4You Planungssysteme GmbH 17](#_Toc163722278)

[Anlage E: Firmenvereinbarung zur mobilen Datenverarbeitung – außerhalb üblicher Büroumgebungen der Software4You Planungssysteme GmbH 19](#_Toc163722279)

[Organisatorische Rahmenbedingungen 20](#_Toc163722280)

[Technische Maßnahmen 20](#_Toc163722281)

[Anlage F: Informationsklassifizierung S4U (Short) 22](#_Toc163722282)

[14.1 Klassifizierung von Information 22](#_Toc163722283)

[14.1.1 Schutzklassen 22](#_Toc163722284)

[Schutzklasse 1 22](#_Toc163722285)

[Schutzklasse 2 22](#_Toc163722286)

[Schutzklasse 3 22](#_Toc163722287)

[Schutzklasse 4 23](#_Toc163722288)

[Schutzklasse 5: streng vertraulich 23](#_Toc163722289)

[14.2 Informationsinventar mit Vertraulichkeitsklasse: 23](#_Toc163722290)

[14.3 Kennzeichnung von Information 24](#_Toc163722291)

[Anlage G (Firmenvereinbarung): Reisen im Namen von Software4You 25](#_Toc163722292)

Die nachfolgende Vereinbarung gilt für alle Mitarbeiter der Software4You Planungssysteme GmbH und ersetzt alle vorherigen Firmenvereinbarungen. Sie gilt als Anlage zum Arbeitsvertrag.

# Urlaubsregelung

Der Mitarbeiter erhält pro Kalenderjahr 30 Arbeitstage Erholungsurlaub. Tritt ein Mitarbeiter während des Kalenderjahres bei Software4You Planungssysteme GmbH ein oder verlässt die Firma, so hat er Anspruch auf 1/12 des Jahresurlaubs pro Monat für die Zeit, in der er im aktuellen Kalenderjahr für das Unternehmen tätig ist bzw. war.

Der Jahresurlaub muss bis zum 31.12. des Jahres genommen werden.  Er kann nur aus zwingenden betrieblichen oder persönlichen Gründen in Abstimmung mit der Geschäftsführung in das Folgejahr übertragen werden. Liegen keine zwingenden Gründe vor, verfällt der Urlaub am 31.12. des Jahres. Liegen zwingende Gründe vor, wird der Urlaub mit der Geschäftsführung abgestimmt. In diesem Fall verfallen Urlaubstage aus dem Vorjahr spätestens am 31.3. des Folgejahres.

Urlaubswünsche von > 10 Arbeitstagen müssen 3 Monate im Voraus dem Vorgesetzten mitgeteilt werden. Jeder Urlaub muss vor dem Antritt durch den Vorgesetzten genehmigt werden.

Der 24.12. und der 31.12. gelten als ½ Arbeitstage, d. h. es ist jeweils nur ein halber Urlaubstag notwendig, sofern die Tage auf einen Wochentag fallen. Der Faschingsdienstag gilt als normaler Arbeitstag.

# Sonderurlaub

Die Firma gewährt in folgenden Fällen Sonderurlaub:

* 2 Arbeitstage einmalig für die eigene Hochzeit
* 1 Arbeitstag für einen Umzug, jedoch maximal alle 2 Jahre
* 1 Arbeitstag für die Geburt des eigenen Kindes
* 2 Arbeitstage im Todesfall eines Angehörigen 1. Grades (Ehepartner, Eltern, Kind)
* 1 Arbeitstag im Todesfall eines Angehörigen 2. Grades (Geschwister)

# Krankmeldung

Bei Krankheit muss die Abwesenheit am 1. Krankheitstag bis 10:00 Uhr dem Unternehmen gemeldet werden. Ab dem 3. Krankheitstag muss dem Arbeitgeber eine ärztliche Bescheinigung unaufgefordert vorgelegt werden.

Während der ersten 28 Tage der Beschäftigung erfolgt keine Gehaltsfortzahlung bei Krankheit durch den Arbeitgeber. Der Ausgleich muss vom Mitarbeiter selbst bei der jeweiligen Krankenkasse beantragt werden.

# Arbeitszeit

Die Wochenarbeitszeit beträgt 40 Stunden. Überstunden werden nicht gesondert vergütet, sondern sind mit dem Gehalt abgegolten, soweit sie einen Umfang von 16 Stunden pro Ka-lendermonat nicht überschreiten und dadurch der gesetzliche Mindestlohn nicht unterschritten wird. Überstunden, die über die 16 Stunden pro Kalendermonat hinausgehen, müssen von einem Mitglied der Geschäftsführung explizit freigegeben werden und müssen innerhalb der folgenden drei Monate als Freizeitausgleich abgebaut werden.

Es gilt folgende Kernzeiten einzuhalten, sofern die Arbeitszeiten nicht anders vereinbart wurden:

Montag – Freitag 09:00 Uhr – 16:00 Uhr

# Zahlungstermine

Das Gehalt wird nachträglich und monatlich ausbezahlt. Für variable Vergütungen können Sonderregeln gelten.

# Abwesenheit

Abwesenheiten müssen, soweit diese vorher bekannt sind, mit den dafür vorgesehenen Mitteln (z. B. Outlook-Ordner, E-Mail, Teams...) kommuniziert werden.

Mitarbeiter, denen ein Telefon zugeordnet ist, müssen die Rufumleitung aktivieren (z. B. zur Zentrale), wenn Sie über einen längeren Zeitraum (>30 Minuten) im Büro nicht erreichbar sind.

# Privateigentum

Privateigentum ist durch die Firma nicht versichert und nur auf eigenes Risiko in den Geschäftsräumen von Software4You Planungssysteme GmbH geduldet.

Es ist untersagt, private Software auf Anlagen von Software4You Planungssysteme GmbH einzuspielen. Private Radio/Fernsehgeräte müssen vom Mitarbeiter selbst bei der GEZ angemeldet werden.

Es ist untersagt Unternehmenssoftware auf Privateigentum zu installieren, oder von Privateigentum auf Unternehmensnetzwerke zuzugreifen. Genauere Regelung: siehe **11 Datenschutz**

# Firmeneigentum

Das Firmeneigentum ist generell pfleglich und umsichtig zu behandeln. Generell darf Firmeneigentum nur in Abstimmung mit einem Vorgesetzten aus den Geschäftsräumen von Software4You Planungssysteme GmbH entnommen werden, dies gilt insbesondere für das Inventar, Software und Literatur. Firmeneigene Software darf nicht für private Zwecke kopiert oder in Umlauf gebracht werden, sofern dieses nicht zu den ausdrücklichen Aufgaben des Mitarbeiters gehört.

# Kündigung

Mit Beendigung des Arbeitsverhältnisses hat der Mitarbeiter alle ihm überlassenen Arbeitsmittel, Dokumente, Quellcodes, Schlüssel und Software der Firma in ordentlichem Zustand zurückzugeben. Ein Rückbehaltungsrecht besteht in keinem Fall, dies gilt auch für Kopien.

# Geheimhaltung

Alle Mitarbeiter müssen sich darüber bewusst sein, dass alle firmeninternen Angelegenheiten, von Software4You Planungssysteme GmbH und deren Vertragspartnern der absoluten Geheimhaltung unterliegen. Dies gilt auch und insbesondere für personenbezogene oder andere Daten von Kunden, Lieferanten, der Software4You Planungssysteme GmbH und weiteren Dritten, sowie organisatorische Abläufe und Dokumente, zu denen die Mitarbeiter Zugang bekommen. Auch das Gehalt eines Mitarbeiters unterliegt der Geheimhaltung.

Es ist untersagt Informationen der Vertraulichkeitsklassen 3-5 auf Privateigentum zu übertragen.

# Datenschutz und Vertraulichkeit der Informationen

Bei Verwendung von Passwörtern sind alle Mitarbeiter verpflichtet, maschinengenerierte Passwörter zu nutzen, außer bei Anmeldung wo das Kopieren des Passwortes nicht möglich ist, Dashlane stellt dafür einen Passwortgenerator bereit.

Authentifizierungsdaten (insbesondere Passwörter und kryptographische Schlüssel) sind streng geheim zu halten und gegenüber unbefugten Dritten nicht bekannt zu geben. Mitarbeiter sind insbesondere verpflichtet, diese Authentifizierungsdaten nicht im Klartext aufzubewahren. Software4You stellt ein sicheres Kennwortverwaltungsprogramm (Dashlane) für diesen Zweck zur Verfügung.

Soweit das Betriebssystem oder eingesetzte Software die Möglichkeit bieten, Formulareingaben und/oder Passwörter zu speichern, sind alle Mitarbeiter verpflichtet, diese Funktionalität zu deaktivieren.

Für den Zugriff auf Firmendatendürfen sie ausschließlich die dienstlich zur Verfügung gestellten Computer und Mobiltelefone benutzen . Virenscanner und Update Funktionen der Scanner müssen eingeschaltet sein.

Personenbezogene Daten oder Informationen der Vertraulichkeitsklassen 4 und 5 sind bei jeder Übertragung und/oder Speicherung auf mobile Datenträger oder Systeme (insbesondere auf Notebooks und Laptops, Microsoft Teams) zu verschlüsseln. Eine Speicherung auf externen Festplatten, CD, DVD, USB-Sticks, Bänder und Speicherkarten ist nicht gestattet. Eine Sonderregelung kann mit Erlaubnis des Kunden und des entsprechenden Teamleiters getroffen werden. Die Sonderregelung muss ein Verfahren für die Speicherung, Verschlüsselung, Übergabe und Entsorgung enthalten und vom Kunden, sowie von einem Mitglied der S4U Geschäftsführung unterschrieben werden. Für die Übertragung von personenbezogenen Daten eines Kunden in eine Testumgebung ist eine schriftliche Freigabe des Kunden erforderlich (siehe Verfahren zur Übertragung von Kundendatenbanken). Diese Freigabe ist abzulegen.

Personenbezogene Daten von ADP dürfen nicht auf lokale Speichermedien übertragen werden.

Auf Ihrem Rechner muss einen Bildschirmschoner mit Passwort eingeschaltet sein, der sich nach längstens 5 Minuten einschaltet. Zudem ist der Mitarbeiterverpflichtet bei Verlassen des Arbeitsplatzes seinen Bildschirm zu sperren.

Aus allen Daten, die auf einer unserer Maschinen gespeichert werden, um Zugriff z.B. von Entwicklern zu ermöglichen, muss der Personenbezug entfernt werden (z.B. Name und Vorname verändern).

Originaldokumente, Datenträger und jegliche personenbezogenen Daten in Papierform sind auch während der Bearbeitung vor unberechtigtem Zugriff zu schützen. Alle Mitarbeiter sind verpflichtet sicherzustellen, dass diese bei jedem - auch nur kurzzeitigem - Verlassen des Arbeitsplatzes vor unberechtigtem Zugriff geschützt sind (“Clean Desk Policy“).

# Reisekostenabrechnung

Reisekostenabrechnungen müssen nach Beleg und besten Wissen abgezeichnet werden. Vorsätzlich falsche Angaben in der Reisekostenabrechnung sind ein Grund für eine fristlose Kündigung.

# Zugangskontrolle

Jeder Mitarbeiter erhält einen Schlüssel zu den Geschäftsräumen von Software4You Planungssysteme GmbH. Der Mitarbeiter darf den Schlüssel Dritten nicht zugänglich machen und muss dessen Verlust unverzüglich der Firma mitteilen.

# Schlussbestimmung

Änderungen der Firmenregelung werden dem Mitarbeiter mitgeteilt. Eine Zustimmung des Mitarbeiters für inhaltliche Änderungen bzw. für deren Umsetzung und Verwirklichung ist nicht nötig, sofern diese nicht im Widerspruch mit dem Arbeitsvertrag stehen bzw. dort nicht geregelt sind.

Diese Firmenvereinbarung tritt mit Stichtag 01.03.2024in Kraft und ist Bestandteil des Arbeitsvertrags.

Ich habe die Firmenvereinbarung zur Kenntnis genommen, verstanden und akzeptiert:

Ort/Datum: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Unterschrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Anlage A:** S4U Maximen (Corporate Behaviour)

**Anlage B:** Regeln zur Kommunikation via E-Mail und Teams

**Anlage C:** Firmenvereinbarung zur Nutzung der Internet und E-Mail Dienste

**Anlage D:** Firmenvereinbarung zur Wiederverwendung, Löschung, Entsorgung oder Rückgabe von Datenträgern

**Anlage E:** Firmenvereinbarung zur Mobilen Datenverarbeitung

**Anlage F:** Klassifizierung von Informationen

**Anlage G::** Reisen im Namen von Software4You

Anlage H: Informationssicherheitsleitlinie

# Anlage A: Maximen (Corporate Behaviour)

1 Einleitung

Wir verstehen uns als kompetentes Dienstleistungsunternehmen, das mit Engagement Problemlösungen für seine Kunden erarbeitet. Dabei folgen wir steht dem Anspruch, unseren Kunden „World Class HR Controlling“ zu ermöglichen. Unsere Kompetenz geht über technischen Lösungen hinaus und erstreckt sich sowohl auf die speziellen Herausforderungen des HR Controllings, die Allgemeine Betriebswirtschaftslehre und Sozialkompetenz. Wir möchten, dass sich Kunden und Mitarbeiter im täglichen Umgang gleichermaßen wohl fühlen und wir somit ein angenehmes Arbeitsumfeld schaffen. Hierzu gibt es einige Anhaltspunkte, die im Folgenden aufgelistet werden.

2 Umgang mit Kollegen

Nachdem wir den Großteil unserer Zeit an unserem Arbeitsplatz und mit Arbeitskollegen verbringen, ist ein sorgfältiger Umgang miteinander eine wichtige Voraussetzung für eine harmonische Atmosphäre. Gegenseitige Rücksicht und Toleranz, Hilfsbereitschaft und Höflichkeit, der Respekt gegenüber anderen und Freundlichkeit erleichtern allen Beteiligten - vor allem in angespannten Situationen - die Bewältigung des Arbeitsalltags. Grundsätzlich sollte man Kollegen so behandeln, wie man selbst gerne behandelt werden möchte.

3 Umgang mit Kunden

Unser Erfolg hängt unmittelbar mit der Zufriedenheit unserer Kunden zusammen. Letztlich gilt: unser Gehalt wird von unseren Kunden bezahlt. Daher widmen wir unseren Kunden besondere Aufmerksamkeit und begegnen ihnen mit Höflichkeit und Respekt. Wir vermitteln ihnen das Gefühl, uns wirklich wichtig zu sein. Wir vermitteln, der richtige und kompetente Ansprechpartner zu sein und behandeln sie mit verbindlicher Freundlichkeit. Mit Toleranz und Einfühlungsvermögen gehen wir auf ihre Wünsche ein und nehmen auf eventuelle Eigenheiten Rücksicht, auch wenn es manchmal aus persönlichen Gründen schwerfallen sollte.

4 Besprechungskultur

Wir finden uns zu Besprechungen ein, um effektiv und gemeinsam zu einem Ziel zu gelangen. Die Grundvoraussetzung hierfür sind ordentliche Rahmenbedingungen wie Pünktlichkeit der Teilnehmenden. Wichtig ist der Ausschluss von Störfaktoren wie Lärm, parallele Arbeit an anderen Dingen oder das Lesen von Nachrichten. Die ungeteilte Aufmerksamkeit der Zuhörenden gehört dem jeweiligen Redner. Eine Besprechung sollte möglichst knapp gehalten sein und mit einem Ergebnis enden.

5 Telefonkultur

Nachdem wir einen Großteil unserer Kommunikation per Telefon abwickeln, gelten hier nicht nur die oben genannten Umgangsformen, sondern es sind noch einige zusätzliche Feinheiten zu beachten. Die freundliche und deutliche Nennung der Firma und des Namens am Telefon ist natürlich Grundvoraussetzung (man kann ein Lächeln durchaus hören!). Auch und gerade am Telefon sollte der Anrufer eine angenehme Erinnerung an Software4You behalten, d.h. wir kümmern uns aktiv um den Anrufer und seine Belange. Und natürlich verabschieden wir uns auch freundlich.

6 Äußeres Erscheinungsbild

Das äußere Erscheinungsbild der einzelnen Mitarbeiter vermittelt dem außenstehenden Betrachter ebenfalls einen bleibenden Eindruck des Unternehmens, daher sind Kleidung und Erscheinung nicht nur der jeweiligen Situation angepasst, sondern grundsätzlich ordentlich.

7 Büroräume

Wir bewegen uns den gesamten Arbeitstag in unseren Büroräumen und teilen diese mit anderen Kollegen, zeitweise auch mit unseren Kunden. Daher wollen wir auch in unseren Büroräumen ein für alle angenehmes Umfeld schaffen und dieses gemeinsam halten. In der Umsetzung bedeutet das z.B. den eigenen Schreibtisch ordentlich zu verlassen oder die Waschräume und Küchen sauber zu halten (Spülmaschine ein- und ausräumen!).

Grundsätzlich gilt innerhalb unserer Geschäftsräume striktes Rauchverbot. Die Plätze, die von Rauchern aufgesucht werden, werden auch von diesen in Ordnung gehalten.

8 Umgang mit Geschenken und Zuwendungen von Dritten

Geschenke und Zuwendungen bis 10€ sind zulässig. Im Zweifel oder bei größeren Zuwendungen ist die Geschäftsleitung zu informieren, die das Thema mit dem zuwendenden Geschäftspartner klärt.

9 Allgemein

Nachdem im Allgemeinen bei S4U ein lockerer Umgangston gepflegt wird, sollte dennoch darauf hingewiesen werden, dass wir uns trotzdem daran erinnern, Diskretion und Zurückhaltung zu üben.

Wir arbeiten alle gemeinsam an einem intakten und harmonischen Betriebsklima, in dem sich jeder wohl fühlen kann und darf. Für den Fall, dass sich jemand nicht mehr wohl fühlt, steht ihm unser Geschäftsführer gerne und jederzeit als Ansprechpartner zur Verfügung.

im Überblick

... im Umgang mit Kollegen:

„Was Du nicht willst, das man Dir tu, das füg‘ auch keinem anderen zu.“

... im Umgang mit Kunden:

„Der Kunde zahlt unser Gehalt.“

... für unsere Besprechungskultur:

„Stell Dir vor, es ist eine Besprechung vereinbart, und keiner geht hin.“

... für unsere Telefonkultur:

„D‘rum lächle, auch wenn es keiner sieht.“

... für unser äußeres Erscheinungsbild:

„Kleider machen eben doch (Geschäfts-) Leute.“

... für unsere Büroräume:

„Our office is our castle. “

... allgemein:

„Konfuzius sagt: Arbeite fröhlich, ohne Knurren, ohne Murren

# Anlage B: Regeln zur Kommunikation via E-Mail und Teams

Ziel

Erklärtes der Regeln zur Kommunikation via E-Mail und Teams ist es, die tägliche Mail- und Teams-Chat-Flut, die unser papierloses Büro mit sich bringt, für alle Beteiligten so angenehm, sinnvoll und effektiv wie möglich zu gestalten.

Interne vs. externe Kommunikation

Für die interne Kommunikation nutzen wir Microsoft Teams. E-Mail nutzen wir für die Kommunikation mit unseren Kunden und anderen externen Geschäftspartnern. In E-Mails können Kollegen per CC einbezogen werden, auch die Weiterleitung von E-Mails an Kollegen ist möglich (es müssen keine E-Mails in Teams übertragen werden, wenn sie intern weitergeleitet werden sollen). Bei der Kommunikation via E-Mail mit externen Parteien sind Informationsklassifizierung und die Vorgaben aus §11 der Firmenvereinbarung einzuhalten.

Teams, Channels und Chats

Für die themenspezifische Kommunikation bietet Teams Channels innerhalb von Teams. Beiträge in Channels können von allen Mitgliedern des Teams gelesen werden und sollten nur für Beiträge verwendet werden, die auch für alle Mitglieder relevant sind. Ein Betrag kann „untergehen“ wenn im Text nicht auf das Team oder den Channel verwiesen wird (z.B. via @Channelname).

Für nicht-themenspezifische Kommunikation wird die Chat-Funktion genutzt.

Handling AN/CC/BCC in E-Mails

AN:

Dieser Empfängerkreis ist von der Nachricht direkt betroffen. Eventuell verlangt der Sender vom Empfänger Aktionen. Bitte setzen Sie nur denjenigen in die „An“-Zeile, der für den jeweiligen Sachverhalt als verantwortlich angesehen wird.

Alle anderen sollten die Mail lediglich CC bekommen. Diese Vorgehensweise gibt den Empfängern auch die Möglichkeit, die Wichtigkeit des Mails richtig einzuordnen und es evtl. erst zu einem späteren Zeitpunkt zu lesen.

CC:

Diese Empfänger bekommen das Mail nur zur Information. Aktion kann vom Sender nicht erwartet werden. Einem CC-Empfänger steht es aber dennoch frei, zu reagieren.

BCC:

Empfänger und CC erhalten keine Nachricht darüber, dass das Mail auch an den BCC Empfänger gesendet wird. Dies widerspricht jedoch dem in unserem Unternehmen offenen Umgang miteinander und sollte unterbleiben.

1 Betreff in E-Mails

Mit dem Betreff soll dem Empfänger unter anderem die Möglichkeit gegeben werden, rasch einzuschätzen, um was es in der Mail geht und wie wichtig sie für ihn ist.

Der Betreff sollte deshalb prägnant, konkret und ohne Füllwörter formuliert sein.

2 E-Mail Autosignatur

Im Rahmen unserer Corporate Identity ist es wichtig, einen einheitlichen Auftritt nach außen zu gewährleisten, der sich nicht nur auf Papier oder Screen beschränkt, sondern auch Mails betrifft. Daher sollten alle Mails wie folgt signiert werden:

Mit freundlichen Grüßen / Kind regards

i.A. Max Mustermann  
Referent zur Darstellung eines Musters

**Software4You Planungssysteme GmbH**

Zielstattstraße 44  
81379 München  
  
e-mail: [mmustermann@software4you.com](mailto:mmustermann@software4you.com)

office: +49 89 / 710 504-18  
fax:      +49 89 / 710 504-25

home: [http://www.software4you.com](http://www.software4you.com/)

geschäftsführer: Hanns-Dirk Brinkmann, Stefan Ebbinghaus  
HRB: 123 354 München

UID: DE 812644562

*Geplante Abwesenheit vom 23.12.2021 bis 3.1.2022*

Die hier verwendete Schriftart ist unsere definierte Schrift Segoe UI. Der Fließtext der Mail sollte ebenfalls in Segoe UI gehalten sein.

3 Disclaimer

Unter der Autosignatur sollte folgender Disclaimer stehen:

Disclaimer:   
This email may contain confidential and proprietary material for the sole use of the intended recipient.   
Any review or distribution by others is prohibited.   
If you are not the intended recipient please contact the sender and delete all copies.

Der Disclaimer sollte die gleiche Formatierung, wie die Autosignatur haben.

4 Umlaute und Sonderzeichen

Bei manchen Mail-Empfängern, insbesondere in UK und USA, können die Umlaute ÄÖÜäöü und ß nicht gelesen werden. Daher kann man diese ggf. durch “ae” und “ss” ersetzen.

5 Priorität und Lesebestätigung

Die Möglichkeit, eine Mail mit einer hohen Priorität zu versenden sollte nach Möglichkeit sparsam und sinnvoll verwendet werden. Gleiches gilt für die Lesebestätigungsfunktion, diese darf nur in Ausnahmefällen verwendet werden.

6 Rückmeldungen

Wer eine Reaktion erwartet, muss dies dem Empfänger auch deutlich machen.

Bsp.:

“Herr XY, bitte xxx bis zum 1. Januar erledigen”

“Frau AB, ich bitte um Stellungnahme”

“Um Antwort wird gebeten” oder “u.A.w.g.”

Wird um Antwort gebeten, dann sollte diese auch gegeben werden, auch wenn es sich nur um ein kurzes OK handelt. Ein ebenso kurzes Dankeschön an den Sender, z.B. für eine wertvolle Information, ist eine nette Geste.

7 Bugs

Fehlerberichte, die das operative Geschäft beeinträchtigen und/oder beim Kunden auftreten, sollten sofort mit hoher Priorität an die Technik weitergeleitet werden. Hierzu wird unser Bug-Tracking System verwendet, welches unter http://tfs2015/4plan/Dashboards/Fehler4Plan.aspx erreichbar ist. Bugmeldungen sollen nicht über Teams bzw. E-Mail erfolgen.

8 Der richtige Ton

Mails sind geschriebene Informationen, d.h. die Interpretation des Inhalts obliegt dem Empfänger. Vieles klingt im Vergleich zum gesprochenen Wort aggressiver, wenn man es schwarz auf weiß liest. Der Angesprochene hat keine Möglichkeit, sich direkt zu verteidigen und „Feindbilder“ bauen sich schneller auf.

Es ist daher ratsam, ein wenig auf den Ton des Emails zu achten und den Inhalt vor dem Senden noch einmal auf Sachlichkeit zu prüfen. Außerdem muss ausgeschlossen werden, dass der Text oder Kommentar für den Empfänger missverständlich sein könnte.

Rhetorische Mittel wie Ironie oder “Schreien” (Groß-Buchstaben) sind in diesem Medium mit großer Vorsicht zu verwenden.

# Anlage C: Firmenvereinbarung zur Nutzung der Internet und E-Mail Dienste der Software4You Planungssysteme GmbH

1 Gegenstand, Geltungsbereich

Diese Firmenvereinbarung regelt die Grundsätze für die Nutzung der Internet- und E-Mail Dienste der Software4You Planungssysteme GmbH und gilt für alle Mitarbeiter, deren Arbeitsplätze über einen geschäftlichen Internet- bzw. E-Mail Zugang verfügen.

2 Zielsetzung

Ziel dieser Vereinbarung ist es, die Nutzungsbedingungen sowie die Maßnahmen zur Protokollierung und Kontrolle transparent zu machen, die Persönlichkeitsrechte der Beschäftigten zu sichern und den Schutz ihrer personenbezogenen Daten zu gewährleisten.

3 Nutzungsbedingungen

(1) Der Internet-Zugang steht den Beschäftigten als Arbeitsmittel im Rahmen der betrieblichen Aufgabenerfüllung zur Verfügung und dient insbesondere der Verbesserung der internen und externen Kommunikation, einer höheren Effizienz und der Beschleunigung von Arbeitsprozessen.

(2) Die Nutzung von Internet, des E-Mail-Dienstes, sowie der geschäftlichen E-Mail Adresse für private Zwecke ist untersagt.

4 Verhaltensgrundsätze

(1) Unzulässig ist jede absichtliche oder wissentliche Nutzung des Internet, die geeignet ist, den Interessen des Unternehmens oder dessen Ansehen in der Öffentlichkeit zu schaden, die Sicherheit des Firmennetzes zu beeinträchtigen oder die gegen geltende Rechtsvorschriften verstoßen. Dies gilt vor allem für:

* das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
* das Abrufen oder Verbreiten von beleidigenden, verleumderischen, rassistischen, sexistischen, pornographischen, Gewalt verherrlichenden Äußerungen oder Abbildungen,
* das Abrufen oder Verbreiten unbekannter Inhalte aus unsicheren Quellen, insbesondere mit Anhängen und ausführbaren Dateien.
* Informationen der Vertraulichkeitsklassen 4 und 5 sollten nicht per E-Mail versendet werden. Sollte ein Versand per E-Mail nötig werden, ist die Verschlüsselungsfunktion von Outlook zu nutzen.

5 Protokollieren und Kontrolle

(1) Zur Kontrolle dieser Unternehmensrichtlinie werden die folgenden auch personenbezogenen Daten aufgezeichnet.

E-Mail

* Datum/Uhrzeit (senden/empfangen)
* Adressen von Absender und Empfänger
* Dateiformate und übertragene Datenmenge

Darüber hinaus können Protokollierungen vorgenommen, soweit sie in den jeweiligen Server- und Netzwerkbetriebssystemen und in den Anwendungssystemen standardmäßig vorgesehen sind.

(2) Die Protokolle nach Absatz 1 können ausschließlich zum Erkennen und zur Beseitigung von Fehlern und Störungen, zur Gewährleistung der Systemsicherheit und für Stichprobenkontrollen entsprechend Ziffer 6 dieser Vereinbarung verwendet werden.

(3) Der Zugriff auf die Protokolldateien für Stichproben und entsprechende Auswertungen ist auf die IT-Abteilung begrenzt. Dieser hat eine Verpflichtungserklärung zum Datenschutz unterschrieben.

6 Maßnahmen bei Verstößen, Missbrauchsregelung

Bei Verdacht auf unerlaubte Nutzung des Internet- oder E-Mail Account durch einen Mitarbeiter wird der Vorgesetzte informiert und ggf. zusätzliche Kontrollen durchgeführt. Nach Rücksprache mit dem Betroffenen können arbeitsrechtliche ggf. auch strafrechtliche Maßnahmen erfolgen. Bestätigt sich der Verdacht nicht, sind die Ergebnisse der zusätzlichen Kontrolle unverzüglich zu löschen.

Im Übrigen gelten die einschlägigen Regelungen des Arbeitsrechts.

7 Zugriff auf betriebliche E-Mails während einer Abwesenheit des Mitarbeiters

Bei Abwesenheit eines Mitarbeiters zur Sicherstellung des betrieblichen Ablaufs steht dem Arbeitgeber auf das E-Mail-Postfach des Betroffenen der Zugriff eingeschränkt zu.

# Anlage D: Firmenvereinbarung zur Wiederverwendung, Löschung, Entsorgung oder Rückgabe von Datenträgern bei der Software4You Planungssysteme GmbH

1 Gegenstand

Diese Firmenvereinbarung ist Bestandteil der allgemeinen Firmenvereinbarung und regelt den Umgang mit Datenträgern bei der Software4You Planungssysteme GmbH.

Es werden die Voraussetzungen und die Vorgehensweise bei der Verarbeitung, Wiederverwendung, Entsorgung oder Rückgabe von Datenträgern festgelegt. Dies ist ein wichtiger Baustein zum Schutz der personenbezogenen und Firmen-Daten der Software4You Planungssysteme GmbH.

2 Zweck

Die wesentlichen Gründe für diese Firmenvereinbarung sind:

* Schutz des geistigen Eigentums der Firma Software4You Planungssysteme GmbH vor Diebstahl / Missbrauch
* Datenschutz für sensitive Daten unserer Kunden, Lieferanten und Mitarbeiter
* Vermeidung von Imageschäden, die bei Datenpannen unvermeidlich wären

3 Verantwortliche

Verantwortlich für die Einhaltung der Firmenvereinbarung sind alle Angestellten und Arbeiter von der Software4You Planungssysteme GmbH, sowie alle Fremdfirmen und deren Mitarbeiter, die für die Software4You Planungssysteme GmbH arbeiten.

4 Umfang

Bei der Verarbeitung von Datenträgern ist zu beachten, dass die Anforderungen an technische und organisatorische Maßnahmen umso höher sein müssen, je höher die Sensibilität der Daten ist.

Die Sensibilität der Daten ist durch den Datenschutzbeauftragten zu bestimmen. Diese Vereinbarung deckt alle Arten von Datenträgern wie interne Festplatten, externe Laufwerke, CDs, DVDs, USB-Sticks, aber auch (Papier)Dokumente ab.

5 Verhaltensgrundsätze

* Mobile, externe Datenträger, die z.B. Testdaten von Kunden enthalten, müssen immer getrennt von anderen Datenträgern aufbewahrt und als solche deutlich gekennzeichnet werden. Sie müssen sicher vor unerlaubten Zugriff gelagert werden.
* Datenträger jeglicher Art dürfen nicht offen im Büro liegengelassen werden. Sobald der Arbeitsplatz verlassen wird oder externe Besucher das Büro betreten, müssen diese in abschließbaren Schränken verwahrt werden.
* Bei der Wiederverwendung von Datenträgern muss der Datenträger zunächst vollständig gelöscht werden.
* Werden Datenträger entsorgt müssen sie ebenfalls vorher ordnungsgemäß gelöscht sein.
* Das Löschen von Datenträgern, sowohl zur Wiederverwendung als auch zur Entsorgung, erfolgt ausschließlich durch die IT-Abteilung.
* Die IT-Abteilung sammelt die zu löschenden Datenträger, löscht die Daten und übergibt sie entweder zur Wiederverwendung den Mitarbeitern oder zur Entsorgung an ein beauftragtes Unternehmen.
* Datenträger zur Vernichtung dürfen nicht beim Mitarbeiter gesammelt werden sondern müssen sofort zur IT-Abteilung gebracht werden.
* Dokumente mit personenbezogenen oder Firmen-Daten, die vernichtet werden sollen, müssen sofort in einem verschließbaren Sammelbehälter entsorgt werden. Die Sicherheitsstufe für die Vernichtung nach DIN32757-1 wird vom Datenschutzbeauftragten anhand des Schutzbedarfs der Daten definiert.
* Datenträger (externe Platten, Laptops, Smartphones, USB Sticks, etc.) die außer Haus gebracht werden und die personenbezogene oder Firmen-Daten enthalten, müssen vor unbefugtem Zugriff durch Passwörter oder Verschlüsselungen geschützt werden.

6 Durchsetzung

Jeder Angestellte/Arbeiter der diese Richtlinie verletzt, muss mit disziplinarischen Maßnahmen bis hin zu Abmahnung und Kündigung rechnen.

# Anlage E: Firmenvereinbarung zur mobilen Datenverarbeitung – außerhalb üblicher Büroumgebungen der Software4You Planungssysteme GmbH

Alternierende oder auch mobile Telearbeit, bei der der Mitarbeiter abwechselnd sowohl im Unternehmen als auch zu Hause oder an anderen Orten, wie im Hotel, im Flughafen oder im Zug tätig ist, stellt aus datenschutzrechtlicher Sicht hohe Anforderungen da ein größeres Gefährdungspotential, als bei der Datenverarbeitung im Unternehmen vorhanden ist. Die Rechtmäßigkeit, Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung muss ständig gewährleistet und regelmäßig kontrolliert werden.

Die Unterschiede zum Büroarbeitsplatz ergeben sich da das Unternehmen bei mobilen, wechselnden Arbeitsstätten nicht die uneingeschränkte Organisationsgewalt über Hard- und Software, Datenbestände und der handelnden Personen hat.

Dies führt bei Telearbeitsplätzen oder der mobilen Datenverarbeitung zu einem ungleich größeren Risiko für den Datenschutz. Können gesetzliche Vorgaben des Datenschutzes mit wirtschaftlich vertretbarem Aufwand nicht umgesetzt werden, muss die Verarbeitung personenbezogener Daten auf Telearbeitsplätzen unterbleiben. Dabei ist besonders die Verarbeitung sensitiver Daten (Art. 9 DS-GVO, wie Patientendaten, Sozialdaten, Personaldaten) zu betrachten.

Beispiele der Risiken bei Heim- oder mobilen Arbeitsplätzen:

* Kenntnisnahme vertraulicher Daten durch Familienangehörige, Freunde
* Ausspähen vertraulicher Daten durch Unbefugte in Zügen, Flugzeugen, Restaurants, etc.
* Unachtsames Verhalten der Mitarbeiter an öffentlichen Orten (z.B. bei Veranstaltungen, Technologie-Events) erleichtert mobilen Hackern ihre Tätigkeiten
* Diebstahl, Verlust mobiler Geräte

Die Sicherheit der Datenverarbeitung sollte gezielt durch einen Maßnahmen-Katalog garantiert werden.

Kontrollmöglichkeiten durch das Unternehmen bei Heimatarbeitsplätzen

Je nach der Nutzungsdauer ist vor der Aufnahme der Telearbeit den Beauftragten für Sicherheit und Datenschutz nach vorheriger Terminabsprache Zugang zum geplanten Telearbeitsplatz einzuräumen, um die Erfordernisse an Arbeits- und Gesundheitsschutz, Datenschutz und Datensicherheit zu überprüfen. Werden bei der Besichtigung Mängel festgestellt, sind diese vor der Aufnahme der Tele-/Heimarbeit zu beseitigen.

Der Mitarbeiter und die in seinem Haushalt lebenden Personen müssen einer Kontrolle zustimmen. Die Einwilligung muss auf freiwilliger Basis erfolgen. Die Kontrollen müssen protokolliert werden.

Technisch-, organisatorische Maßnahmen, die in der Richtlinie geregelt werden sollen

# Organisatorische Rahmenbedingungen

* **Arbeitszeit:** nicht definiert
* **Arbeitsmittel:** 
  + Telefon- und Datenübertragungskosten werden von Software4You übernommen
  + Die technische Ausstattung wird ausschließlich von Software4You gestellt
  + Ausschließliche Verwendung von HW und SW, die von Software4You gestellt bzw.   
     konfiguriert wurde
* **Haftung:** Software4You kommt für Schaden bei Beschädigungen der technische Einrichtung durch Mitarbeiter, bei Diebstahl oder Verlust von Equipment auf
* **Datenschutz:**
  + Verpflichtung auf Vertraulichkeit der Daten nach Art. 28 Abs 3 b) DS-GVO
  + Vorgaben zur sicheren Verwahrung von Datenträgern
  + Der Arbeitsplatz (Homeoffice) muss sich in einem Raum befinden, der ein ungestörtes Arbeiten ermöglicht
  + Änderungen der Hard- und Software sind nicht zulässig, ebenso unzulässig ist die Zugangsberechtigung für Dritte
  + Nicht dienstliche Downloads aus dem Internet sind untersagt
  + Am häuslichen Arbeitsplatz nicht mehr benötigte dienstliche Akten, Unterlagen und Datenträger sind unverzüglich in der Arbeitsstätte unterzubringen
  + Zu vernichtende Schriftstücke sind ausschließlich in der Arbeitsstätte zu vernichten
  + Zur Verfügung gestelltes Equipment, dienstliche Akten, Unterlagen und Datenträger sind von der/dem Angestellten so zu schützen, dass Unbefugte weder Einsicht noch Zugriff nehmen können, dies gilt besonders für Arbeiten im öffentlichen Raum.
  + Es ist darauf zu achten, dass keine ungesicherten Wege zur Datenübertragung verwendet werden

# Technische Maßnahmen

* **Kontrolle bei der Datenübertragung:** Vertraulichkeit und Integrität muss gewährleistet werden
  + Vermeiden von öffentlichen WLAN Netzen
  + Ausschließlich sichere VPN und UMTS Tunnel nutzen
  + Bei Messe-Besuchen Bluetooth Verbindung an mobilen Geräten ausschalten (Tablets, Laptops, Smartphones)
  + Datenübermittlung nur verschlüsselt durchführen, sowohl mit Netzwerken als auch bei mobilen, externen Speichermedien
* Die Benutzung des Telearbeitsplatzes darf nur für berechtigte Personen möglich sein
* **Zugriffskontrolle**
  + Daten und Informationen sowie Passwörter sind von den Beschäftigten so zu schützen, dass Dritte keine Einsicht nehmen können.
  + Das Risiko, bei der Passworteingabe beobachtet zu werden, sollte minimiert werden.
* Sensible Daten auf mobilen Geräten nur verschlüsselt abspeichern
* Reduzierung der Zugriffsrechte bei externen Zugriffen
* Automatische Sperrung des Accounts bei Nichtbenutzung

# Anlage F: Informationsklassifizierung S4U (Short)

**Klassifizierung von Information**

Die Klassifizierung von Informationen dient der Etablierung einer angemessenen Sicherheit, die dem Wert und der Bedeutung der Informationen entspricht. Die Klassifizierung von Informationen ist die Grundlage dafür Informationen in Bezug auf Wert, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung der Sicherheit definieren zu können.

Die Klassifizierung von Informationen darf nicht die gesetzlichen Rahmenbedingungen verletzen. Anforderungen für die gemeinsame oder die eingeschränkte Nutzung von Informationen sind zu berücksichtigen.

**Schutzklassen**

**Definition Schutzklasse:** Eine Schutzklasse setzt sich aus den Abwägungen bezüglich der benötigten Vertraulichkeit, Integrität und Verfügbarkeit einer Information zusammen. Die angewendete Schutzklasse spiegelt immer den höchsten Wert dar, welcher der Vertraulichkeit, Verfügbarkeit oder Integrität zugewiesen wurde. Die Schutzklassen sind von der Geschäftsführung freigegeben.

**Schutzklasse 1**

Informationen zur uneingeschränkten Veröffentlichung. Zu diesen Informationen zählen freigegebene Presse- oder Marketinginformationen und Informationen, die auf der Software4You Homepage im Internet veröffentlicht werden.

**Microsoft Teams:** Beim Umgang und der Ablage von Informationen der Schutzklasse 1 gibt es bezüglich Microsoft Teams nichts zu beachten.

### Schutzklasse 2

Informationen, die nur für Kunden und Mitarbeiter der Software4You Planungssysteme GmbH bestimmt sind und für den täglichen Dienstbetrieb notwendig sind. Können bei Herausgabe an Außenstehende mit Wasserzeichen geschützt werden (siehe Kundeninformationen zu HRCC-Template)

**Microsoft Teams:** Beim Umgang und der Ablage von Informationen der Schutzklasse 2 gibt es bezüglich Microsoft Teams nichts zu beachten.

### Schutzklasse 3

Informationen, die nur für Mitarbeiter der Software4You Planungssysteme GmbH bestimmt sind und für den täglichen Dienstbetrieb notwendig sind. Eine Herausgabe an Dritte erfordert die Freigabe durch einen Vorgesetzten oder der Geschäftsführung.

**Microsoft Teams:** Beim Umgang und der Ablage von Informationen der Schutzklasse 3 gibt es bezüglich Microsoft Teams nichts zu beachten.

### Schutzklasse 4

Informationen, die bei Veröffentlichung oder Verlust zu einem Schaden oder Imageverlust der Software4You führen können, sowie personenbezogene Daten im Sinne der geltenden datenschutzrechtlichen Bestimmungen.

**Microsoft Teams:** Informationen der Schutzklasse 4 dürfen nur verschlüsselt in Microsoft Teams abgelegt werden (Passwortgeschützt).

### Schutzklasse 5: streng vertraulich

Informationen, bei denen die unberechtigte Einsichtnahme unter allen Umständen verhindert werden muss. Dazu zählen insbesondere aufgrund vertraglicher Verpflichtungen geheim zuhaltende Informationen. Zudem Informationen die eine nicht unerhebliche Geschäftsschädigung der S4U Planungssysteme verursachen können.

**Microsoft Teams:** Informationen der Schutzklasse 5 dürfen nur nach Freigabe und in streng zugangsbeschränkten Microsoft Teams Kanälen, abgelegt werden. Passwörter dürfen nicht in TEAMS abgelegt werden.

**Informationsinventar mit Vertraulichkeitsklasse:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information | Beispiele | SK | DSGVO | Verantwortlich |
| Werbemittel | Flyer, Homepage, Merchandise | SK 1 | nein | Sarah Jäger |
| Öffentlich zugängliche Informationen | Alles was man auch im Internet über S4U und Kunden finden kann | SK 1 | nein |  |
| Abrechnungsdaten S4U analog | Eingangsrechnungen | SK 2 | nein | Bernd Jansen |
| Kundenverträge analog | / | SK 2 | nein | Brian Scheunchen |
| Kundenverträge digital | / | SK 2 | nein | Brian Scheunchen |
| Dienstleisterverträge analog | / | SK 2 | nein | Ilona Kalmusz |
| Dienstleisterverträge digital | / | SK 2 | nein | Ilona Kalmusz |
| Partnerverträge analog | / | SK 2 | nein | Ilona Kalmusz |
| Partnerverträge digital | / | SK 2 | nein | Ilona Kalmusz |
| Vertragsvorlagen Kunden | Nutzungsvertrag, AV, TOM | SK 2 | nein | Matthias Stocker, HDB |
| Angebote Kunden | / | SK 2 | nein | Stefan Hörmann |
| Angebote Interessenten | / | SK 2 | nein | Stefan Hörmann |
| Bestellungen | / | SK 2 | nein | Bernd Jansen, Matthias Stocker, Brian Scheunchen |
| 4PLAN Dokumentation | 4PLAN Doku, Systemanforderungen, Release Notes | SK 2 | nein | Manfred Abele |
| Interessentendaten | / | SK 3 | ja | Stefan Hörmann |
| Projektabrechnung | / | SK 3 | ja | Bernd Jansen |
| Abrechnungsdaten S4U digital | Eingangsrechnungen, Kontoauszüge usw. | SK 3 | nein | ext. Schaller |
| Kundenansprechpartner | / | SK 3 | ja | Brian Scheunchen |
| Preisliste 4PLAN | / | SK 3 | nein | Stefan Hörmann, Hanns Dirk Brinkmann |
| Testdaten niedrige VK | Testdaten Funktionalität | SK 3 | nein | Manfred Abele |
| Mitarbeiterdaten analog | Personalakte Papier, Krankmeldung Papier usw. | SK 4 | ja | Ilona Kalmusz |
| Mitarbeiterdaten digital | Personalakte Digital, Krankmeldung digital usw. | SK 4 | ja | Ilona Kalmusz |
| Mitarbeiterdaten Abrechnung | Gehaltsabrechnung, sonstige Abrechnung | SK 4 | ja | ext. Schaller |
| Projektbezogene Kundendaten | Kostenstellenhierarchie, Konten usw. | SK 4 | ja | Projektleiter |
| Logs | z.B: Eventlogs der Server | SK 4 | ja | Jakob Hetkämper, Christoph Walter |
| Quellcode 4PLAN | / | SK 5 | nein | Sören Kühnholz |
| Kundendatenbanken 4PLAN Produktion | / | SK 5 | ja | Christoph Walter |
| Zugangsdaten | Schlüssel, Passwörter, Tokens | SK 5 | ja | Jakob Hetkämper |
| Konfigurationsdateien | Konfiguration 4PLAN Server, ADFS, WAP usw. | SK 5 | nein | Christoph Walter, Jakob Hetkämper |
| Testdaten hohe VK | Security Tests (z.B. verschiedene Pentests) | SK 5 | nein | Matthias Stocker |

**Kennzeichnung von Information**

Informationen werden bei Software4You nicht separat gekennzeichnet, da eine Kennzeichnung auch potenziellen Angreifern die Identifikation von geschützten Informationen erleichtert. Alle Mitarbeiter von Software4You wurden über die Informationsklassifizierung unterrichtet und kennen die, für den Fachbereich relevanten Beispiele. Ist sich ein Mitarbeiter unsicher, wie mit einer entsprechenden Information zu verfahren ist, kann der Mitarbeiter das ISMS-Team um eine Entscheidung bitten.

Die Langversion kann im ISMS der S4U Planungssysteme GmbH eingesehen werden.

# Anlage G (Firmenvereinbarung): Reisen im Namen von Software4You

1 Gegenstand

Diese Firmenvereinbarung ist Bestandteil der allgemeinen Firmenvereinbarung und regelt den Umgang mit Geschäftsreisen im Namen von Software4You.

Es werden klare Regelungen für an anmieten von Fahrzeugen und Hotelzimmern, sowie für das Buchen von Bahnfahrten oder Flügen getroffen.

2 Zweck

Die wesentlichen Gründe für diese Firmenvereinbarung sind:

* Klar definierte Regelungen, um Missverständnissen vorzubeugen und dem Mitarbeiter einen eindeutigen Handlungsrahmen zur Verfügung zu stellen
* Festlegung der Verantwortlichkeiten und Entscheidungsbefugnisse

3 Rahmenbedingungen

Mit diesem Dokument wird Software4You Rahmenbedingungen schaffen, die immer dann greifen, wenn der Mitarbeiter eine Reise im Namen von Software4You antritt. Reist der Mitarbeiter im Namen von Software4You zu einem Kunden, so sind zusätzlich zu den Anforderungen von Software4You auch die vom Kunden vertraglich fixierten Reisebedingungen zu beachten (z.B. nur Bahnfahrten zweiter Klasse/ Hotelkosten bis maximal 100€/Nacht werden übernommen usw.).

4 Anreise/Abreise

Bei einer Reisezeit von mehr als 2,5 Stunden kann der Mitarbeiter die Reise bereits am Vortag antreten und eine Hotelübernachtung in Anspruch nehmen. Sollte die Ankunftszeit einer Rückreise vom Kunden später als 22:00 Uhr betragen, kann der Mitarbeiter eine Hotelübernachtung in Anspruch nehmen und die Rückreise am nächsten Tag antreten.

5 Bahnfahrt

Für eine Bahnfahrt zum Kunden kann ein Ticket 2. Klasse inklusive Sitzplatzreservierung in Anspruch genommen werden, sofern nicht anders mit dem Kunden abgestimmt. Für eine Bahnfahrt zu anderen geschäftlichen Zwecken kann ebenfalls ein Ticket 2. Klasse inklusive Sitzplatzreservierung in Anspruch genommen werden, sofern nichts anderes mit der Teamleitung/Geschäftsführung abgestimmt wurde.

6 Flug

Für einen Flug zum Kunden kann ein Ticket der Economy Klasse in Anspruch genommen werden, sofern nicht anders mit dem Kunden abgestimmt. Für einen Flug zu anderen geschäftlichen Zwecken kann ebenfalls ein Ticket der Economy Klasse in Anspruch genommen werden, sofern nichts anderes mit der Teamleitung/Geschäftsführung abgestimmt wurde.

7 Anreise mit einem Personenkraftwagen

Ein Leihwagen sollte nur in Anspruch genommen werden, wenn das Ziel ohne eigenes Kraftfahrzeug schwer zu erreichen ist. Für eine Fahrt zum Kunden sind eventuelle Anforderungen des Kunden zu beachten (z.B: Fahrzeugklasse). Hat der Kunden keine Anforderungen an den Leihwagen, oder wird der Leihwagen für sonstige geschäftliche Reisen für Software4You angemietet, darf der Mitarbeiter ein Fahrzeug bis maximal VW-Golf-Klasse auswählen, sofern mit der Teamleitung/Geschäftsführung nichts anderes abgestimmt wurde. Mitarbeiter mit einem Firmenwagen haben für die Anreise mit dem PKW nichts Weiteres zu beachten.

**Wichtig:** Bei einem Unfall/Schaden mit einem Leihwagen/Interimsfahrzeug (Ersatzfahrzeug Reparatur des Firmenwagens) erfolgt die Schadenmeldung nicht an Software4You, sondern nach den jeweiligen Regularien sowie an die zuständige Stelle des Autovermieters.

8 Sonstiges

Für die Anreise und Abreise, sowohl zu Kunden als auch für sonstige geschäftliche Reisen gilt, dass öffentliche Verkehrsmittel vorzuziehen sind. Sollte der Kunde allerdings schwer mit den öffentlichen Verkehrsmitteln zu erreichen sein, oder die Nutzung von öffentlichen Verkehrsmitteln eine unverhältnismäßige Erhöhung der Reisezeit bedeuten, so kann der Mitarbeiter nach eigenem Ermessen ein Taxi benutzen.

9 Hotelübernachtung

Werden für eine Reise zum Kunden Hotelübernachtungen benötigt, so überprüft der Mitarbeiter zuerst, ob es mit dem Kunden spezielle Vereinbarungen bezüglich des Preises oder des Hotels gibt. (z.B. Einige Kunden buchen das Hotel selbst, da Kontingente bei bestimmten Ketten bestehen, andere geben vor maximal 100€ pro Übernachtung usw.). Gibt es keine speziellen Regelungen mit dem Kunden, so darf eine Übernachtung maximal 120€ inklusive Frühstück kosten. Diese Regelung gilt ebenfalls für geschäftliche Reisen, mit anderem Zweck als den Kundenbesuch. Benötigt der Mitarbeiter ein teureres Hotelzimmer, so ist dies vom Teamleiter zu genehmigen und muss begründet werden (z.B: es finden zur selben Zeit Großveranstaltungen statt oder andere Hotels sind vom Kunden unverhältnismäßig weit entfernt).

10 Durchsetzung

Jeder Angestellte/Arbeiter, der diese Richtlinie verletzt, muss mit disziplinarischen Maßnahmen bis hin zu Abmahnung und Kündigung rechnen und kann für Software4You entstandenen Mehrkosten zur Rechenschaft gezogen werden.

# Anhang H: Informationssicherheitsleitlinie

**Kontext der Organisation**

Die Software4You Planungssysteme GmbH ist führender Anbieter von Softwareprodukten und Dienstleistungen im Bereich Personalkostenplanung und -controlling. Die branchenübergreifenden Lösungen werden an mittelständische und große Unternehmen adressiert.

Mit seiner jahrzehntelangen Erfahrung (Gründung 1999) im Bereich Personalcontrolling-Systemen und Personalkostenplanung bietet Software4you mit ihrem selbst entwickelten Produkt 4PLAN HR eine zuverlässige Lösung für die Personalkostenplanung, Personalplanung und Personalcontrolling an, die sich dank Solution Packs schnell und unkompliziert implementieren lässt. Dabei erfüllen diese [Produkte](https://www.software4you.com/produkte/) unternehmensspezifische Anforderungen und reagieren jederzeit flexibel auf Veränderungen in Unternehmensabläufen.

[(](https://80.151.127.252:10443/proxy/4dec94ec/https/www.inside-computer.de)/)siehe <https://www.software4you.com/unternehmen/>)

Mit der Einführung eines Managementsystems nach der DIN EN ISO 27001:2023, wollen wir die steigenden Anforderungen der Gesellschaft und unserer Kunden nach Transparenz und Sicherheit in der Branche und vor allem im SaaS Umfeld erfüllen. Durch die offene Darstellung der Prozesse und Abläufe in unserem Unternehmen können sich alle Mitarbeiter an einer ständigen Weiterentwicklung und Verbesserung beteiligen. Durch sorgfältige Zielsetzung, Planung, Umsetzung, Kontrolle und Korrektur in den verschiedenen Bereichen unseres Unternehmens sind wir in der Lage auf die schnelle Entwicklung am Markt zu reagieren und langfristig erfolgreich zu bleiben. Informationssicherheit wird im Unternehmen ernst genommen und achtet stets auf Vertraulichkeit, Verfügbarkeit und Integrität.

Die Software4You Planungssysteme GmbH in München bietet die folgenden Leistungen an:

* Lizenzierung von 4PLAN HR
* Consulting
* 4PLAN as a Service (SaaS)
* Technischer Support

Unsere Kunden sind vorwiegend

* Großkonzerne
* Mittelstand

Das Mission Statement der Software4You Planungssysteme GmbH lautet:

|  |
| --- |
| „Unser Motto ist „World Class HR Controlling“. Darunter verstehen wir, dass unsere Software einen HR-Fokus besitzt, zuverlässig und sicher nachvollziehbare Ergebnisse liefert sowie eine produktive Arbeitsumgebung für unsere Kunden bietet. Um in den Punkten Sicherheit, Zuverlässigkeit und Produktivität noch stärker zu werden, haben wir uns entschieden den Software as a Service (SaaS) Bereich sowie die Softwareentwicklung nach ISO27001 zertifizieren zu lassen und ein entsprechendes Informationssicherheitsmanagementsystem aufzubauen. |

Aus unserem Mission Statement ergibt sich der folgende externe und interne Kontext, den wir beachten müssen:

* Externe Themen: Wir bewegen uns im Markt der Speziallösungen im Bereich Personalcontrolling. Unsere Kunden im SaaS-Bereich sind Unternehmen im nationalen als auch im internationalen Raum. In diesem Umfeld beraten wir unsere Kunden inhaltlich und bieten technischen Support an. Von unseren Kunden wird die Software im Regelfall zur Planung und Budgetierung und KPI-Analyse im HR-Bereich genutzt. Unsere Kunden vertrauen uns in diesem Zusammenhang Mitarbeiter-Daten, wie z.B. Gehalt, Geburtsdatum, Tarif usw. an.
* Interne Themen: Im SaaS-Bereich unseres Unternehmens betreiben wir auf Kundenwunsch die von Software4You erworbene oder gemietete Software 4PLAN sowie deren Module. Unser Anspruch an uns ist, dass die Kundensysteme bei uns sicher, zuverlässig und produktiv laufen. Intern betrachten wir hier v.a. die Themen Datenschutz und Informationssicherheit im SaaS-Betrieb, sowie die sichere Entwicklung unserer Software 4PLAN. Alle drei Themen sind für uns gleichermaßen wichtig.

**Informationssicherheitspolitik**

Wir betrachten Informationssicherheit als einen wesentlichen Wert, den wir anbieten möchten. Von der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) von Informationen, die von unseren Lösungen verarbeitet werden, hängt viel ab. Dies bringen wir durch die folgende Selbstverpflichtung zum Ausdruck:

1. Wir verpflichten uns, alle gesetzlichen und durch Kunden und Partner vertraglich vorgegebenen Regelungen zur Informationssicherheit einzuhalten und die von Behörden und anderen Organisationen bereitgestellten Informationen zur kontinuierlichen Verbesserung der Informationssicherheit zu nutzen.
2. Wir bilden alle Mitarbeiter, die Tätigkeiten im Anwendungsbereich der Informationssicherheit durchführen, so aus, dass sie sicher und bewusst im Sinne der Informationssicherheit agieren können.
3. Wir schaffen notwendige technische und organisatorische Voraussetzungen (TOM), die es uns ermöglichen, Informationssicherheit zu leben.
4. Wir möchten erreichen, dass Informationssicherheit bei uns allen nicht als „lästige Mehrarbeit“ begriffen wird, sondern als wichtig und wesentlich für unsere Kunden. Und dass wir zu jeder Zeit – trotz aller Regeln in diesem Bereich – unseren Kopf einschalten müssen und uns nicht darauf verlassen dürfen, dass in jeder Situation das Befolgen der festgelegten Regeln ausreicht. Wenn wir vor der Wahl stehen, etwas richtig sicher zu machen oder eine Regel zu befolgen, dann machen wir es lieber richtig sicher – und passen danach ggf. die Regel an.
5. Wir wollen in unserer Informationssicherheit immer besser werden!
6. Wir verpflichten uns die Anforderungen der ISO27001 zu erfüllen.
7. Wir verpflichten uns, die Informationssicherheit bei S4U kontinuierlich zu verbessern.

Für die o.g. Dinge stellen wir Ressourcen bereit.

**Interessierte Parteien**

Basierend auf unserem Kontext gibt es bei uns die folgenden an Informationssicherheit interessierten Parteien:

|  |  |  |  |
| --- | --- | --- | --- |
| **Interessierte Partei** | **Erwartungen hinsichtlich…** | | |
| **Vertraulichkeit** | **Integrität** | **Verfügbarkeit** |
| Unserer Kunden  (extern) | Wir verwahren im SaaS-Betrieb Mitarbeiter-Daten unserer Kunden. Diese unterliegen einer hohen Vertraulichkeit. Zudem erwarten unsere Kunden eine Software, die keine größeren Fehler aufweist. | Unsere Kunden wünschen sich, dass Ergebnisse in 4PLAN korrekt angezeigt werden. Zudem müssen alle Änderungen an den Informationen in 4PLAN transparent dargestellt werden. | Unsere Anwendung wird im Regelfall während der normalen Arbeitszeiten Mo-Fr 7:00-19:00 genutzt. Trotzdem versprechen wir unseren Kunden eine Verfügbarkeit von 99% im Jahresmittel (SLA). |

|  |  |  |  |
| --- | --- | --- | --- |
| Gesetzgeber  (extern) | Einhaltung aller Gesetze bzgl. Vertraulichkeit von personenbezogenen Daten. | Der Gesetzgeber wünscht sich zudem die Unverfälschbarkeit von Nachweisdokumenten, wie z.B. steuerlich relevante Dokumente (Rechnungen) | Der Gesetzgeber hat die Verfügbarkeit von diversen Dokumenten klar geregelt und entsprechend hat S4U sicherzustellen, dass die Dokumente innerhalb der gesetzlichen Aufbewahrungsfristen verfügbar bleiben. |
| Lieferanten  Prozesspartner (extern) | Unsere Lieferanten erwarten einen vertraulichen Umgang mit den im Rahmen der Auftragserfüllung zur Verfügung gestellten Informationen | Unsere Prozesspartner und Lieferanten könnten ebenfalls darunter leiden, wenn es zu Sicherheitsvorfällen wegen mangelnder Integrität kommt (z.B: externes Rechenzentrum). Deshalb ist es wichtig, dass wir auch in der Arbeitsbeziehung mit unseren Lieferanten ein höchstmögliches Maß an Integrität herstellen. | Unsere Lieferanten benötigen für die Auftragserfüllung Informationen von uns, deren Verfügbarkeit durch S4U sicherzustellen ist, damit der Lieferant seinen Verpflichtungen nachkommen kann. |
| Mitarbeiter und Mitarbeiterinnen  (intern) | Es ist schädlich für das Geschäft der Firma und damit für die Arbeitsplatzsicherheit, wenn unsere Software unabsichtlich oder durch gezieltes Hacking Informationen offenlegt, die besser vertraulich bleiben sollten. Zudem erwarten unsere Mitarbeiter, dass wir mit persönlichen Informationen, die uns im Rahmen des Arbeitsverhältnisses mitgeteilt werden, vertraulich umgehen. | Es ist schädlich für das Geschäft der Firma und damit für die Arbeitsplatzsicherheit, wenn unsere Software unabsichtlich oder durch gezieltes Hacking Informationen darin verändern kann, die besser dagegen sicher sein sollten. Zudem ist es Mitarbeitern wichtig, dass Sie nicht fälschlich für Änderungen an Systemen und Informationen verantwortlich gemacht werden können. | Es ist gut für das Geschäft der Firma und damit für die Arbeitsplatzsicherheit, wenn unsere Software alle darin verarbeiteten Informationen den Kunden auch ständig zur Verfügung stehen. Zudem ist es Mitarbeitern wichtig, dass die Arbeitsumgebung während der Arbeitszeit verfügbar ist. |
| Geschäftsführung (intern)  Gesellschafter | Unsere Softwarelösung wird am Markt nur dann akzeptiert, wenn sie nicht unabsichtlich oder durch gezieltes Hacking Informationen offenlegt, die besser vertraulich bleiben sollten. | Unsere Softwarelösung wird nur dann am Markt akzeptiert, wenn man nicht unabsichtlich oder durch gezieltes Hacking Informationen verändern kann, die besser dagegen sicher sein sollten. | Unsere Softwarelösung wird nur dann am Markt akzeptiert, wenn alle darin verarbeiteten Informationen unseren Kunden auch ständig zur Verfügung stehen. |

**Informationssicherheitsziele**

Abgeleitet aus den Interessen der Stakeholder leiten wir die folgenden Informationssicherheitsziele ab:

**Vertraulichkeit:**

**SaaS Betrieb:**Wir streben an, dass alle Informationen, die durch unsere Softwarelösung 4PLAN verarbeitet werden, während der Verarbeitung im SaaS-Betrieb vertraulich sind und niemandem Unbefugten offengelegt werden.

**Software Development:** Wir streben an, dass unsere Software 4PLAN HR keine Eigenschaften hat, die zu einer Offenlegung der Informationen in unseren Kundensystemen an unbefugte Personen führt.

**Dies werden wir daran messen,** wie viele Vorkommnisse wir von unseren Kunden gemeldet bekommen, in denen Informationen in 4PLAN in unserem SaaS-Betrieb unberechtigterweise nicht vertraulich behandelt worden sind. Wir streben an: maximal 1 pro Major Release Zyklus (im Regelfall von Juli bis Juli).

**Integrität:**

**SaaS Betrieb:** Wir streben an, dass alle Informationen, die durch unsere Softwarelösung 4PLAN verarbeitet werden, während der Verarbeitung im SaaS-Betrieb sicher sind gegen unbefugte und unbeabsichtigte Veränderung/Verfälschung.

**Software Development:**Wir streben an, dass unsere Software 4PLAN HR keine Eigenschaften aufweist, die zu einer bewussten oder unbewussten Verfälschung der Informationen in unseren Kundensystemen führen.

**Dies werden wir daran messen,** wie viele Vorkommnisse wir von unseren Kunden gemeldet bekommen, in denen Informationen in 4PLAN unberechtigterweise oder unbeabsichtigter-weise verändert wurden bzw. verändert werden konnten und wie viele Fälle wir selbst bei unseren internen Abnahmetests vor Auslieferung davon entdecken. Wir streben an: 0 Vorfälle pro Jahr.

**Verfügbarkeit:**

**SaaS Betrieb:** Wir streben an, im SaaS-Betrieb von 4PLAN sicherzustellen, dass die Applikation jederzeit verfügbar ist.

**Software Development:**Wir streben an, die Software ohne Fehler auszuliefern, die zu einer Einschränkung der Verfügbarkeit oder einer Nichtverfügbarkeit der in den Kundensystemen hinterlegten Informationen führen.

**Dies werden wir im SaaS Betrieb daran messen,** ob wir es schaffen, eine „von-außen“-Verfügbarkeit von 4PLAN in der SaaS-Variante hinzubekommen, die 99% gerechnet über das Jahr (365 Tage) beträgt. (vgl. Service-Level-Agreement)

**Dies werden wir im Software Development daran messen,** ob wir es schaffen, vier oder weniger Wartungsfenster für 4PLAN-Updates im Jahr zu benötigen.

**Anwendungsbereich (Scope)**

Dieses Informationssicherheitsmanagementsystem (ISMS) soll getroffenen Maßnahmen zum Betrieb und Schutz von IT-Einrichtungen und Daten vor unbefugter Kenntnisnahme durch Dritte oder nichtberechtigte Mitarbeiter unterstützen und darüber hinaus eine grundlegende Information für alle Mitarbeiter im Hinblick auf den Umgang mit IT-Einrichtungen und Daten sein. Dieses ISMS gilt für alle Beschäftigte der **Software4You Planungssysteme GmbH. Als besonders schützenswerte Assets haben wir die Informationen unserer Kunden, die von uns im Rahmen des SaaS Betriebs verarbeitet werden, sowie den Quellcode von 4PLAN HR definiert.**

Dazu gehören alle Festangestellten, Teilzeitangestellten, Werksstudenten sowie Aushilfskräften etc. Auch externe Personen, die für unser Unternehmen tätig sind, sind verpflichtet, sich an dieses System zu halten. Zudem gilt das ISMS auch für alle Netzwerke des Unternehmens. Das Unternehmen wird entsprechende Vorkehrungen treffen, damit dieses System auch für die externen Personen verbindlichen Charakter hat. Der Informationssicherheitsbeauftragte führt das System in Zusammenarbeit mit der Geschäftsleitung. Alle Dokumente werden im Abstand von 12 Monaten auf notwendige Änderungen oder Ergänzungen überprüft. Verstöße gegen das ISMS werden durch Ermahnung oder Abmahnung geahndet.

**Scope auf der Zertifizierung:** Entwicklung einer HR-Controlling-Lösung sie deren Betrieb und Beratung zu deren Implementierung und HR-Controlling im Allgemeinen.

**Ausschlüsse aus dem Statement of Applicability**

Es ergeben sich keine Ausschlüsse aus dem Statement of Applicability.

**Richtlinien des ISMS**

**Richtlinie : Personalsicherheit**

**Richtlinie: Informationsklassifizierung und Umgang mit Werten**

**Richtlinie: Zugangssteuerung**

**Richtlinie: Kryptographie**

**Richtlinie: Physische und umgebungsbezogene Sicherheit**

**Richtline - Testen von 4PLAN HR und der dazugehörigen Systemlandschaft im 4PLAN.net Rechenzentrum**

**Richtlinie für sichere Entwicklung**

**Richtlinie: Lieferantenbeziehungen**

**Richtlinie: Verhalten bei einem Informationssicherheitsereignis oder einem Informationssicherheitsvorfall**