Reglement für die Nutzung von IT-Mitteln

1. Geltungsbereich

Die nachfolgenden Bestimmungen gelten für alle fest angestellten Mitarbeiter der Allianz Suisse Versicherungs-Gesellschaft AG und der Allianz Suisse Lebensversicherungs-Gesellschaft AG sowie für alle Tochtergesellschaften, die auf Daten und Anwendungen der Allianz Suisse Gesellschaften zugreifen können.

Das Reglement gilt ebenfalls für die Mitarbeiter der Generalagenturen inkl. Hauptagenturen der Allianz Suisse.

2. Inhalt und Umfang

Dieses Reglement beinhaltet verbindliche Regelungen im Zusammenhang mit dem Umgang und der Nutzung von IT-Mitteln. Es ist abgestimmt auf die im Rahmen der „Group Information Security Policy“ vom Konzern vorgegebenen Minimalbestimmungen.

Der Begriff „ IT-Mittel“ umfasst sämtliche Hardware, Speichermedien und Software.

3. Allgemeine Regelungen

- Die Mitarbeitenden sind verpflichtet, mit den ihnen anvertrauten IT-Mitteln sorgfältig umzugehen. Diese sind vor Diebstahl, Beschädigung und Missbrauch zu schützen.
- Die IT-Mittel dienen in erster Linie der Verarbeitung und Speicherung geschäftlicher Vorgänge und Daten. Die Nutzung für private Zwecke wird gestattet, sofern sich diese in einem vertretbaren, verhältnismässigen Ausmass bewegt, sich in keiner Form störend auf die Geschäftstätigkeiten auswirkt und keine gesetzlichen oder reglementarischen Bestimmungen verletzt. Die private Nutzung kann jederzeit durch die Allianz Suisse verboten werden.
- Es ist strikte verboten, die von der Allianz Suisse zur Verfügung gestellten Mittel für gesetzeswidrige, unlautere oder gegen die Ethik und Moral verstossende Aktivitäten und missbräuchliche Zwecke einzusetzen.
- Der Einsatz von Allianz Suisse eigenen IT-Mitteln für nebenberufliche Tätigkeiten ist nicht gestattet. Ebenso ist es nicht erlaubt, die IT-Infrastruktur privat kommerziell zu nutzen.
- Private Dokumente und Dateien dürfen nicht auf Notebooks, PC’s, Servern und anderen Speichermedien der Allianz Suisse abgespeichert werden. Sämtliche auf IT-Mitteln der Allianz Suisse abgespeicherten Daten sind Geschäftsakten und befinden sich im Eigentum der Allianz Suisse. Allfällige private Dateien können somit jederzeit von der Allianz Suisse ohne vorgängige Information des Mitarbeitenden gelöscht werden.
- Das Abspeichern und die Weiterleitung von Dateien mit urheberrechtsverletzendem, pornografischem, rassistischem, sexistischem, gewaltdarstellendem, beleidigendem, herabwürdigendem oder gegen Ethik und Moral verstossendem Inhalt ist verboten.
- Der Einsatz privater Hard- und Software ist grundsätzlich nicht erlaubt. Ausnahmen können durch den Information Security Officer (ISO) genehmigt werden (z.B. elektronische Agenden, Monitore, Tastaturen, USB-Hubs etc.).
- Es ist untersagt, firmenfremde Geräte an die Allianz Suisse Netzwerke anzuschliessen.

- Die Übertragung von geschäftlichen Daten und Software auf firmenfremde Rechner und Speichermedien ist nicht gestattet, ausser im Rahmen einer rechtmässigen, geschäftlichen Beziehung mit der betroffenen Partei. Ausnahmen bedürfen der Genehmigung durch den ISO.
- Der Zugang zu Daten und Geräten darf nur im Rahmen der erteilten Berechtigungen erfolgen.
- Es ist verboten, sich mit einer fremden Identität an Systemen anzumelden.
- Verstösse gegen dieses Reglement und andere sicherheitsrelevante Vorfälle und Schwachstellen sind dem ISO zu melden.

4. Umgang mit Notebook und PC

- Am Arbeitsplatz ist das Notebook mit dem Kensington-Kabel zu sichern oder unter Verschluss zu verwahren. Unterwegs darf das Notebook nicht unbeaufsichtigt dem Zugriff Dritter ausgesetzt sein.
- Bei Beschädigung oder Verlust infolge grober Fahrlässigkeit oder unsachgemässem Gebrauch kann der Mitarbeiter haftbar gemacht werden.
- Es ist nicht gestattet, das Notebook / PC über Nacht ohne zwingenden Grund im aktiven, gesperrten rsp. im Standby-Modus zu halten. Ohne anders lautende Anweisung ist das Gerät bei Arbeitsschluss herunter zu fahren und auszuschalten. Beim kurzfristigen Verlassen des Arbeitsplatzes ist die Bildschirmsperre zu aktivieren.
- Die Überlassung des Notebooks an Dritte ist, mit Ausnahme von IT-Support-Fällen, unzulässig.
- Die Mitarbeitenden sind verpflichtet, sämtliche geschäftsrelevanten Daten auf dem Notebook / PC regelmässig auf einen Datenserver (Netzlaufwerk, Lotus Notes Server) zu kopieren. Zu diesem Zweck stehen sowohl gemeinsame als auch persönliche Laufwerke zur Verfügung.
- Veränderungen und Erweiterungen der Hardware auf produktiv eingesetzten Notebooks und PC's dürfen nur aufgrund eines genehmigten Antrags rsp. gültigen Auftrags durch dafür autorisierte Personen vorgenommen werden.
- Abgegebenes Material muss vom Empfänger auf Vollständigkeit überprüft und dessen Erhalt schriftlich bestätigt werden. Bei der Rückgabe fehlendes Material wird dem Empfänger in Rechnung gestellt.

5. Nutzung von mobilen Endgeräten und Datenträgern

- Private, mobile Endgeräte (PDA's, Smartphones, Pocket-PC, MP3-Player, Kameras etc.) dürfen nicht mit Allianz Suisse Systemen verbunden werden. Ausnahmen bilden die offiziell zugelassenen Gerätetypen gemäss im Intranet veröffentlichter Liste.
- Die geschäftliche Nutzung von PDA's, Smartphones, Pocket-PC und ähnlichen Geräten beschränkt sich auf die Replikation und Bearbeitung von Kalendereinträgen, Aufgabenlisten, Adressdaten, Notizen und ggf. E-Mails. Weitere Anwendungen können durch den ISO bewilligt werden. Das Abspeichern von anderen geschäftlichen Daten auf diesen Geräten ist untersagt. Der Zugang zu den auf diesen Geräten gehaltenen Daten muss über ein Passwort oder einen PIN geschützt sein. Das Gerät und die Zugangsdaten dürfen unter keinen Umständen zusammen aufbewahrt werden. Falls es das Gerät erlaubt, ist eine automatische Sperre bei Inaktivität zu aktivieren.

- Geschäftliche Daten, die auf externe Speichermedien geladen werden, müssen entweder verschlüsselt abgespeichert (z.B. mit WinZip-Verschlüsselung) oder mit einem Passwort geschützt werden, wenn das Medium ausser Haus gebracht wird. Mobile Datenträger mit geschäftlichen Daten sind unter Verschluss aufzubewahren. Folgende Informationen sind wenn möglich auf dem Datenträger, auf der Hülle oder einer Etikette anzubringen: Inhalt, Vertraulichkeitsstufe (falls nicht intern), Erstellungsdatum.
- Es ist ausdrücklich verboten, mobile Datenträger, insbesondere USB-Sticks, deren Herkunft und Inhalt unbekannt sind, an Geräte der Allianz Suisse anzuschliessen.
- Bei Virenbefall oder Verdacht auf Virenverseuchung auf mobilen Datenträgern und Geräten ist jeglicher Datenaustausch mit diesen zu unterlassen. In diesem Fall ist eine Meldung an den ISO erforderlich.
- Geschäftliche Daten auf persönlichen mobilen Datenträgern müssen beim Austritt aus der Firma unverzüglich gelöscht werden. Ist dies nicht möglich (z.B. bei CD-R), so ist der Datenträger zu vernichten oder der Allianz Suisse (i.d.R. dem Linienvorgesetzten) zu übergeben.
- Verlust oder Diebstahl von mobilen Datenträgern und Endgeräten mit geschäftlichen Daten sind dem ISO unverzüglich zu melden.

6. Einsatz von Software

- Sämtliche Software (Betriebssystem, Systemsoftware, Anwendungssoftware, Entwicklungsumgebungen, Tools, Programme, Datenbanksysteme, Treiber, Dienste etc.) darf nur durch dafür autorisierte Personen aus der Informatik installiert, aktiviert und angepasst werden. Ausnahmen können durch den ISO bewilligt werden.
- Es ist strikte untersagt, die Standard-Einstellungen zu Ungunsten der IT-Sicherheit anders zu konfigurieren oder zu verändern. Insbesondere ist es nicht erlaubt, sicherheitsrelevante Software (z.B. Virenscanner, Firewall, Verschlüsselungssoftware) zu deaktivieren, zu deinstallieren oder zu manipulieren.
- Die Vervielfältigung und Weitergabe von kommerziell gehandelter Software ist verboten.
- Auf den produktiv eingesetzten Systemen darf nur offiziell bewilligte Software installiert und genutzt werden. Die Nutzung von Freeware und Shareware muss mit Begründung beantragt und vom ISO genehmigt werden. Unbewilligte Software kann durch die Allianz Suisse jederzeit und auf allen Systemen eliminiert werden.
- Die Installation und/oder die Ausführung jeder Art von Computerspielen ist nicht gestattet.

7. Nutzung von Internet

- Das Abrufen von Informationen und Daten aus dem Internet rsp. www. ist in erster Linie auf geschäftlich begründete Zwecke beschränkt, d.h. zur Erfüllung der zugewiesenen beruflichen Aufgaben einzusetzen. Der Zugang kann jederzeit entzogen werden.
- Die private, nicht kommerzielle Nutzung der elektronischen Medien ist in vertretbarem Rahmen unter Beachtung der dafür geltenden Grundsätze wie Ethik, Verhältnismässigkeit etc. gestattet, darf aber die berufliche Tätigkeit nicht beeinträchtigen. Das Internet darf während der Arbeitszeit

nicht für persönliche Finanztransaktionen (Telebanking, Börsengeschäfte oder ähnliches) eingesetzt werden.

- Es ist explizit verboten, auf Material mit widerrechtlichem, urheberrechtsverletzendem, pornografischem, rassistischem, gewaltdarstellendem, beleidigendem oder herabwürdigendem Inhalt zuzugreifen oder solches zu verbreiten.
- Den Mitarbeitenden ist es untersagt, Software oder Plug-ins, namentlich Audio- und Videodateien, Computerspiele, Bilder und Software, die keinen Zusammenhang mit der beruflichen Tätigkeit haben, aus dem Internet auf geschäftlich genutzte Systeme zu kopieren oder zu installieren.
- Die Nutzung von nicht genehmigten Instant Messaging Systemen und Chat-Foren ist nicht erlaubt.
- Die Allianz Suisse behält sich vor, den Zugriff auf offensichtlich nicht mit der Geschäftstätigkeit in Zusammenhang stehende Internet-Seiten zu sperren.

8. Nutzung von E-Mail

- Die Mitarbeitenden haben ihren elektronischen Briefkasten wenn möglich täglich auf den Eingang von E-Mails zu überprüfen. Bei längeren Abwesenheiten ist der Abwesenheitsassistent einzuschalten.
- Für geschäftliche Zwecke dürfen nur Allianz Mail-Systeme verwendet werden. Eine Umleitung von E-Mails an externe E-Mail-Adressen ist nicht erlaubt.
- Der Versand von E-Mails unter fremder, geänderter, falsch dargestellter oder unterdrückter Identität ist verboten.
- Der ISO kann im Bedarfsfall (z.B. bei Krankheit, Unfall, Austritt oder Tod des Mitarbeitenden) die Zugriffsbrechtigung nach Absprache mit dem Vorgesetzten Dritten erteilen.
- In Bezug auf die informationstechnische Verarbeitung werden private E-Mails den Regeln des Geschäftsverkehrs unterstellt. D.h., die Allianz Suisse ist berechtigt, den gesamten E-Mail-Verkehr zu protokollieren, zu sichern und zu archivieren
- Kettenbriefe bzw. Werbe-E-Mails (Spam) sind unverzüglich zu löschen. Es ist verboten, Massen-, Ketten- oder Werbe-E-Mails weiter zu versenden.
- Mail-Attachments unbekannter oder nicht vertrauenswürdiger Herkunft dürfen nicht geöffnet rsp. aktiviert werden, da solche Dateien ein enormes Sicherheitsrisiko in Bezug auf Malware (Viren, Trojaner, Spyware etc.) darstellen.
- Bei Austritt eines Mitarbeitenden werden das E-Mail Konto und die E-Mail-Adresse i.d.R. am letzten Arbeitstag gelöscht.

9. Umgang mit Passwörtern

- Passwörter und PIN’s sind persönlich und geheim und dürfen nicht an Dritte weitergegeben oder zugänglich gemacht werden.
- Es ist nicht gestattet, Drittpersonen den Zugang zu Daten und Systemen unter der eigenen Identität zu gewähren. Eine Ausnahme bildet der Supportfall im Beisein des betroffenen Benut-

zers. Der Mitarbeitende haftet für sämtliche Transaktionen, die mit seiner User-ID durchgeführt werden.

- Ist ein Passwort bekannt geworden oder besteht der Verdacht darauf, so ist es unverzüglich zu ändern.
- Standardpasswörter oder voreingestellte Passwörter sind beim ersten Logon zu wechseln.
- Um gegenüber Knackversuchen eine angemessene Sicherheit zu erhalten, sollten folgende Passwortregeln beachtet werden:
  - mindestens 8 Zeichen, gemischt aus Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen
  - keine Eigennamen, Lexikonwörter, Geburtsdatum, Telefon- oder Autonummern und andere einfach zu erratende Ausdrücke und Kombinationen verwenden
  - keine Alphabet- oder Tastaturreihenfolgen (z.B. QWERTZ) verwenden
  - das Passwort muss regelmässig geändert werden, wobei das neue dem alten nicht zu ähnlich sein darf

10. Massnahmen bei Verstössen gegen das vorliegende Reglement

Widerrechtliches oder reglementwidriges Benützen der elektronischen Medien oder jedes andere Verhalten, das einen Verstoss gegen die Pflichten aus dem Arbeitsverhältnis darstellt, können arbeitsrechtliche Sanktionen zur Folge haben. Der Mitarbeitende wird für die der Allianz Suisse entstandenen Schäden haftbar.

Bei einem konkreten begründeten Verdacht, dass eine Straftat per Internet, E-Mail oder unter Nutzung firmeneigener IT-Mittel begangen worden ist, kann die Allianz Suisse Strafanzeige erstatten.

11. Inkrafttreten

Das vorliegende Reglement tritt am 1. September 2009 in Kraft.