Règlement sur l'utilisation des moyens informatiques

1. Champ d’application

Le présent règlement s’applique à tous les collaborateurs fixes d’Allianz Suisse Société d’Assurances SA, d’Allianz Suisse Société d’Assurances sur la Vie SA et de toutes les filiales ayant droit d’accès aux données et aux applications des sociétés d’Allianz Suisse.

Ce règlement est également valable pour les collaborateurs des agences générales, agences principales incluses, d’Allianz Suisse.

2. Objet et étendue

Le présent règlement régit l’utilisation des moyens informatiques au sein d’Allianz Suisse. Les dispositions qu’il contient ont force obligatoire. Il est conforme aux dispositions minimales de politique de sécurité de l’information édictées par le groupe (Group Information Security Policy).

Le terme « moyens informatiques » désigne tout équipement matériel, tout support de données ainsi que tout logiciel.

3. Dispositions générales

- L’employé a l’obligation de prendre soin des moyens informatiques qui lui sont confiés, notamment de les protéger contre le vol, les détériorations et l’utilisation abusive.
- Les moyens informatiques servent avant tout à traiter et enregistrer des opérations et des données commerciales. Leur utilisation à des fins privées est autorisée pour autant qu’elle se fasse dans les limites du raisonnable et de la proportionnalité, qu’elle ne porte pas préjudice aux activités professionnelles et qu’elle n’enfreigne aucune disposition légale ou réglementaire. Allianz Suisse peut décréter une interdiction d’utiliser les moyens informatiques à des fins privées.
- Il est strictement interdit d’utiliser les moyens informatiques mis à disposition par Allianz Suisse à des fins illicites, déloyales, contraires à l’éthique et à la morale ou abusives.
- L’utilisation des moyens informatiques d’Allianz Suisse à des fins d’activité professionnelle accessoire n’est pas autorisée. Il en va de même pour l’utilisation de l’infrastructure informatique à des fins privées commerciales.
- Il n’est pas permis d’enregistrer des documents et des fichiers privés sur des ordinateurs portables, des PC, serveurs et autres supports de données d’Allianz Suisse. Toutes les données sauvegardées sur les moyens informatiques d’Allianz Suisse sont considérées comme propriété d’Allianz Suisse. De ce fait, Allianz Suisse peut, à tout moment et sans en avertir le collaborateur, supprimer d’éventuels fichiers privés de celui–ci.
- L’enregistrement et la retransmission de contenus pornographiques, sexistes, racistes, violents, offensants, dégradants, contraires à l’éthique ou à la morale, ou portant atteinte aux droits d’auteur sont interdits.
- L’utilisation de matériels et de logiciels privés est en principe interdite. Toutefois, des dérogations peuvent être accordées par l’Information Security Officer (ISO) (p. ex. pour l’utilisation d’agendas électroniques, moniteurs, claviers, hub USB, etc.).
- Il est interdit de connecter aux réseaux d’Allianz Suisse des appareils appartenant à d’autres sociétés.

- Le transfert de données et de logiciels commerciaux vers des ordinateurs et des supports de données de tiers est uniquement autorisé dans le cadre de relations commerciales licites avec le tiers concerné. Toute dérogation à cette règle requiert l'approbation de l'ISO.
- L'accès à ces données et équipements est limité à l'utilisation pour laquelle il a été autorisé.
- Il est interdit d'ouvrir une session sur des systèmes avec l'identité d'un tiers.
- Toute infraction au présent règlement ainsi que tout incident ou lacune compromettant la sécurité doivent être annoncés à l'ISO.

4. Ordinateurs portables et PC

- Sur la place de travail, l'ordinateur portable doit être sécurisé au moyen du câble Kensington ou conservé sous clé. En déplacement, il y a lieu de veiller à ce qu'il ne soit pas laissé sans surveillance ni accessible à des tiers.
- L'employé peut avoir à répondre de détériorations ou de perte par suite de négligence grave ou d'une utilisation inappropriée.
- Il est interdit de laisser l'ordinateur portable ou le PC en mode activé, bloqué ou de veille pendant la nuit sans raison impérieuse. Sauf instruction contraire, l'appareil doit être éteint et mis hors tension à la fin de la journée de travail. En cas d'absence de courte durée, le verrouillage d'écran doit être activé.
- La cession l'ordinateur portable à des tiers, sauf à des fins de support informatique, est interdite.
- L'employé a l'obligation de copier sur un serveur de données (lecteur réseau, serveur Lotus Notes), à intervalles réguliers, toutes les données professionnelles se trouvant sur son ordinateur portable ou PC. Des lecteurs communs et personnels sont mis à sa disposition à cet effet.
- Toute modification ou extension du matériel sur les ordinateurs portables et PC utilisés de manière productive se fait uniquement sur ordre dûment approuvé par la personne habilitée à cet effet.
- L'employé vérifie que le matériel qui lui est remis est complet et confirme sa réception par écrit. À la restitution du matériel, tout élément manquant est facturé à l'employé.

5. Utilisation de terminaux et supports de données mobiles

- Il est interdit de connecter à des systèmes d'Allianz Suisse des terminaux mobiles privés; tels que assistants numériques personnels (PDFA), smartphones, ordinateurs de poche, lecteurs MP3, appareils photos, etc.. Font exception à cette règle les modèles d'appareils officiellement autorisés selon la liste publiée sur l'intranet.
- L'utilisation professionnelle de PDA, smartphones, ordinateurs de poche et autres appareils est limitée à la réplication et au traitement d'entrées de calendrier, de listes de tâches, de données d'adresses, de notes et, le cas échéant, de courriers électroniques. Toute autre utilisation requiert l'autorisation de l'ISO. L'enregistrement, sur ces appareils, de données professionnelles autres que celles susmentionnées est interdit. L'accès aux données conservées sur ces appareils doit être protégé par un mot de passe ou un code personnel (PIN). L'appareil et les données d'accès doivent être conservés séparément. Si l'appareil en est doté, la fonction de désactivation automatique en cas d'inactivité doit être activée.

- Les données professionnelles enregistrées sur des supports de données externes doivent être protégées au moyen d'un mot de passe ou d'un procédé de cryptage (p. ex. cryptage WinZip) lorsque ce support de données est sorti des locaux d'Allianz Suisse. Les supports de données mobiles contenant des données professionnelles doivent être conservés sous clé. Dans la mesure du possible, les informations suivantes doivent figurer sur le support de données, sur le boîtier ou sur une étiquette : contenu, degré de confidentialité (s'il ne s'agit pas de données internes), date de création.
- Il est strictement interdit de connecter aux appareils d'Allianz Suisse des supports de données mobiles, en particulier des clés binaires, dont l'origine et le contenu sont inconnus.
- En cas de présence avérée ou supposée de virus, il y a lieu de s'abstenir de tout échange de données avec le support de données mobile ou l'appareil concerné. Dans ce cas, l'ISO doit être informé.
- En cas de départ définitif de l'entreprise, les données professionnelles enregistrées sur des supports de données mobiles doivent être immédiatement effacées. S'il n'est pas possible de les effacer (c'est le cas, par exemple, avec un CD-R), le support de données doit être détruit ou remis à Allianz Suisse (en règle générale au supérieur hiérarchique).
- La perte ou le vol de supports de données mobiles et de terminaux contenant des données professionnelles doit être immédiatement annoncé à l'ISO.

6. Logiciels

- Tout logiciel, de quelque type qu'il soit (système d'exploitation, logiciel système, logiciel d'application, environnement de développement, utilitaire, programme, système de banque de données, pilote, logiciel de service, etc.), ne doit être installé, activé et adapté que par des personnes du service informatique dûment habilitées. Des dérogations sont possibles, moyennant l'approbation de l'ISO.
- Il est strictement interdit de modifier et d'adapter la configuration standard au détriment de la sécurité informatique. En particulier, il est interdit de désactiver ou de désinstaller des logiciels essentiels à la sécurité (p. ex. programmes antivirus, pare-feu ou logiciels de chiffrement) ou encore d'en modifier la configuration.
- La copie et la transmission à des tiers de logiciels commercialisés sont interdites.
- Sur des systèmes productifs, seuls peuvent être installés et utilisés des logiciels officiellement autorisés. L'utilisation de logiciels libres (freeware) et de partagiciels (shareware) doit faire l'objet d'une demande préalable dûment justifiée à l'ISO et requiert l'approbation de ce dernier. Allianz Suisse est en droit, à tout moment, d'éliminer de tous ses systèmes tout logiciel non autorisé.
- L'installation et/ou l'exécution de jeux informatiques, de quelque nature qu'ils soient, sont interdites.

7. Utilisation d'Internet

- Le téléchargement d'informations et de données depuis Internet ou depuis la Toile (Worldwide Web, www) est limité à l'usage professionnel avéré, c'est-à-dire à l'accomplissement des tâches professionnelles confiées aux employés. L'accès à Internet peut être retiré en tout temps.

- L’utilisation privée, non commerciale, des médias électroniques est autorisée pour autant qu’elle reste dans les limites du raisonnable, respecte les principes applicables en la matière, tels que l’éthique, la proportionnalité, etc. et ne se fasse pas au préjudice de l’activité professionnelle. Pendant les heures de travail, Internet ne peut pas être utilisé pour effectuer des transactions financières personnelles (télébanque, transmission d’ordres boursiers et autres opérations).
- La consultation et l’envoi de contenus illégaux, pornographiques, racistes, violents, offensants, dégradants ou portant atteinte aux droits d’auteur sont explicitement interdits.
- Sur un système à usage professionnel, il est interdit de télécharger à partir d’Internet, de copier, d’enregistrer ou d’installer des enregistrements audio ou vidéo, des jeux électroniques, des images, des logiciels et des plug-in qui sont sans rapport avec l’activité professionnelle.
- L’utilisation de systèmes de messagerie instantanée et de forums de clavardage (chat) non autorisés est interdite.
- Allianz Suisse se réserve le droit de bloquer l’accès à des sites Internet qui ne sont manifestement pas en rapport avec les activités professionnelles de l’employé.

8. Messagerie électronique (courriel)

- Les employés sont tenus de relever leur boîte à lettres électronique quotidiennement, si possible. En cas d’absence prolongée, le message d’absence automatique doit être activé.
- Pour les besoins professionnels, seuls les systèmes de messagerie électronique d’Allianz peuvent être utilisés. La retransmission de messages électroniques (courriels) à des adresses électroniques externes est interdite.
- L’envoi de messages électroniques sous une identité de tiers, une identité différente, falsifiée ou cachée est interdit.
- Dans des cas justifiés (maladie, accident, départ définitif de l’entreprise, décès), l’ISO peut autoriser, après accord du supérieur hiérarchique, l’accès à des tiers.
- En ce qui concerne leur traitement informatique, les courriels privés sont soumis aux mêmes règles que les courriels professionnels. Autrement dit, Allianz Suisse est en droit de journaliser l’ensemble du trafic courriel, de sauvegarder les messages et de les archiver.
- Les chaînes de lettres et les messages publicitaires (spam) doivent être supprimés sans délai. Il est interdit de retransmettre des messages électroniques en masse, à la chaîne ou publicitaires.
- Les fichiers d’origine inconnue ou douteuse, annexés à des messages électroniques, ne doivent pas être ouverts ni exécutés, car ils présentent un risque très élevé de contamination par des programmes malveillants (virus, chevaux de Troie, logiciels espions, etc.).
- Lors du départ définitif d’un employé, son compte de messagerie et son adresse électroniques sont, en règle générale, supprimés au dernier jour de travail.

9. Mots de passe

- Les mots de passe et codes d’identification personnels (PIN) sont confidentiels et secrets. Ils ne doivent pas être communiqués ou rendus accessibles à des tiers.
- Il est interdit de permettre à un tiers d’accéder à des données ou des systèmes au moyen de sa propre identité, sauf lors d’interventions par le service d’assistance, qui accède directement au

système de l'utilisateur concerné en présence de ce dernier. L'employé répond de toutes les transactions effectuées sous son identification d'utilisateur.

- Si un mot de passe a été divulgué ou si l'on soupçonne qu'il l'a été, il doit être immédiatement modifié.
- Le mot de passe standard ou par défaut doit être changé lors de la première ouverture de session.
- Afin d'offrir une sécurité suffisante contre les tentatives de piratage informatique, le choix du mot de passe doit répondre aux conditions suivantes :
  – longueur minimale de 8 caractères, mélange de minuscules et de majuscules, de chiffres et de caractères spéciaux ;
  – ne pas utiliser de noms propres, de mots du dictionnaire, de dates de naissance, numéros de plaques d'immatriculation, ou autres expressions et combinaisons faciles à deviner ;
  – ne pas utiliser de suites de lettres dans l'ordre alphabétique ou dans l'ordre de la disposition des touches du clavier (p. ex. QWERTZ) ;
  – changer le mot de passe à intervalles réguliers, en choisissant un nouveau mot de passe qui ne soit pas trop semblable à l'ancien.

10. Mesures en cas d'infraction au présent règlement

L'utilisation illicite ou contraire au règlement des moyens informatiques ainsi que tout comportement constituant une violation des obligations découlant des rapports de travail peuvent entraîner des sanctions disciplinaires et/ou des sanctions relevant du droit du travail. L'employé devra répondre des dommages causés à Allianz Suisse.

S'il existe des soupçons fondés qu'une infraction relevant du droit pénal a été commise via Internet, la messagerie électronique ou en utilisant ses moyens informatiques, Allianz Suisse est habilitée à déposer une plainte pénale.

11. Entrée en vigueur

Le présent règlement entre en vigueur au 1er septembre 2009.