Regolamento sull'uso dei mezzi informatici

1. Campo di applicazione

Le seguenti disposizioni sono valide per tutti i dipendenti fissi di Allianz Suisse Società di assicurazioni SA e di Allianz Suisse Società di Assicurazioni sulla Vita SA nonché per tutte le affiliate che abbiano accesso ai dati e alle applicazioni delle società riconducibili ad Allianz Suisse.

Il regolamento si applica anche al personale delle agenzie generali e delle agenzie principali di Allianz Suisse.

2. Oggetto e scopo

Il presente regolamento stabilisce norme vincolanti su gestione e uso dei mezzi informatici ed è conforme agli standard minimi in materia di sicurezza fissati dal Gruppo Allianz (Group Information Security Policy).

Nella fattispecie, il termine "mezzi informatici" include tutti i componenti hardware, i supporti di memorizzazione dati e i software.

3. Disposizioni generali

- Il dipendente è tenuto a gestire i mezzi informatici affidati con la dovuta diligenza, tutelandoli da eventuali furti, danni e abusi.
- I mezzi informatici servono principalmente all'elaborazione e al salvataggio di dati e processi attinenti alle attività aziendali. L'utilizzo privato è consentito entro limiti ragionevoli e sostenibili, a condizione che questo non influisca negativamente sull'attività lavorativa né violi le disposizioni legali e regolamentari. Allianz Suisse ha facoltà di sospendere tale autorizzazione in ogni momento.
- Vige il divieto tassativo di impiegare a fini illegali, illegittimi, contrari a etica e morale o abusivi i mezzi resi disponibili da Allianz Suisse.
- Non è consentito l'uso di mezzi informatici dell'azienda per eventuali attività lavorative extraaziendali. Allo stesso modo, è vietato usufruire dell'infrastruttura informatica aziendale a fini commerciali personali.
- Documenti e file personali non possono essere memorizzati su notebook, computer, server e altri supporti di memorizzazione dati di Allianz Suisse. Tutti i file memorizzati su mezzi informatici di Allianz Suisse costituiscono documenti inerenti alle attività aziendali e sono di proprietà di Allianz Suisse. Pertanto eventuali file personali possono essere cancellati da Allianz Suisse in qualsiasi momento senza avvisare preventivamente il dipendente.
- È vietato memorizzare e trasmettere file con contenuti pornografici, razzisti, sessisti, violenti, offensivi, degradanti, contrari a etica e morale o lesivi del diritto d'autore.
- In linea di principio non è consentito utilizzare hardware e software personali. L'Information Security Officer (ISO) può tuttavia concedere deroghe (es. agende elettroniche, schermi, tastiere, hub USB, ecc.).
- È vietato collegare alla rete Allianz Suisse apparecchi non aziendali.

- Non è consentito il trasferimento di dati e software aziendali su computer e supporti di memorizzazione dati non aziendali, salvo nell'ambito di un regolare rapporto di lavoro con la controparte. Eventuali deroghe sono soggette all'approvazione dell'ISO.
- L'accesso a dati e apparecchi è consentito solo entro i limiti fissati dalle autorizzazioni rilasciate.
- È vietato accedere ai sistemi utilizzando un identificativo di terzi.
- Violazioni contro il presente regolamento, fatti e lacune che potrebbero compromettere la sicurezza devono essere segnalati all'ISO.

4. Notebook e computer

- Il notebook va fissato alla postazione di lavoro tramite l'apposito cavo (detto "Kensington") o conservato sotto chiave. Nelle trasferte tenerlo al riparo dall'accesso di terzi.
- Il dipendente risponde per danni o perdita a seguito di colpa grave o uso improprio.
- Non è consentito tenere il notebook/computer in funzione, bloccato o in modalità "stand by" durante la notte senza ragioni impellenti. Di norma, a fine giornata occorre chiudere i programmi e spegnerlo. Attivare il bloccaschermo per brevi assenze.
- È vietato affidare il notebook a terzi, salvo ai tecnici dell'assistenza informatica.
- Il personale è tenuto a copiare regolarmente tutti i dati importanti contenuti nel notebook/computer su un server dati (drive di rete, server Lotus Notes). Utilizzare i drive condivisi e personali appositi.
- Modifiche ed espansioni hardware dei notebook/computer utilizzati per il lavoro sono consentite solo previa autorizzazione o richiesta del responsabile pertinente.
- Il dipendente è tenuto a verificare la completezza del materiale affidatogli, accusandone ricevuta per iscritto. Alla restituzione, l'eventuale materiale mancante gli verrà fatturato.

5. Apparecchi portatili e supporti dati

- È vietato connettere portatili personali (palmari, smartphone, pocket PC, lettori MP3, apparecchi foto/video) ai sistemi Allianz Suisse. Fanno eccezione gli apparecchi autorizzati ai sensi dell'elenco pubblicato sull'Intranet.
- L'utilizzo per lavoro di palmari, smartphone, pocket PC e simili si limita alla replicazione e gestione dell'agenda, promemoria attività, indirizzi, appunti ed eventualmente e-mail. Qualsiasi altro uso è soggetto ad approvazione dell'ISO. È vietato memorizzare altri dati di lavoro su tali apparecchi. L'accesso ai dati ivi memorizzati è consentito solo tramite password o codice personale (PIN). L'apparecchio e i dati d'accesso non devono essere custoditi assieme. Se l'apparecchio la prevede, attivare la funzione di blocco automatico in caso di non utilizzo.
- I dati di lavoro caricati su supporti esterni utilizzati fuori sede devono essere sottoposti a cifratura (es. WinZip) oppure protetti da una parola chiave. I supporti portatili contenenti dati di lavoro devono essere conservati sotto chiave. Se possibile, sul supporto oppure sull'apposita custodia o etichetta devono figurare le seguenti informazioni: contenuto, grado di riservatezza (se non si tratta di dati limitati alla circolazione interna), data di creazione.

- È espressamente vietato collegare supporti dati portatili alla rete Allianz Suisse, in particolar modo memory stick USB di provenienza e contenuto sconosciuti.
- In caso di attacco di virus sospetto o accertato a supporti portatili e apparecchi, evitare qualsiasi scambio di dati e segnalare obbligatoriamente il fatto all'ISO.
- Il personale dimissionario è tenuto a cancellare tempestivamente i dati professionali archiviati su supporti portatili personali. Qualora ciò non fosse possibile, come nel caso dei CD-R, il supporto deve essere distrutto o consegnato ad Allianz Suisse, di norma al superiore diretto.
- Lo smarrimento o il furto di supporti dati e apparecchi portatili contenenti dati di lavoro va immediatamente denunciato all'ISO.

6. Software

- I software (sistemi operativi, software di sistema e di servizio, applicativi, ambienti di sviluppo, tool, programmi, banche dati, driver, ecc.) devono essere installati, attivati e modificati esclusivamente dal personale informatico autorizzato. Eventuali deroghe richiedono l'approvazione dell'ISO.
- Vige il divieto tassativo di modificare la configurazione standard, poiché tali operazioni pregiudicherebbero la sicurezza informatica. Nello specifico non è consentito manipolare, disattivare o disinstallare quei software che costituiscono un ausilio in materia di sicurezza, ad esempio antivirus, firewall, programmi di cifratura.
- È vietato copiare e cedere software commerciali.
- Sui sistemi utilizzati per le ordinarie attività operative è possibile installare e utilizzare soltanto i programmi ufficialmente autorizzati. L'utilizzo di software gratuiti (freeware) e condivisi (shareware) è possibile solo su richiesta all'ISO che dovrà esprimersi in merito. Allianz Suisse si riserva il diritto di eliminare in ogni momento e da qualsiasi sistema i programmi non autorizzati.
- Non è ammesso installare e/o utilizzare videogiochi, di qualunque tipo essi siano.

7. Internet

- In linea di principio, dati e informazioni presenti in Internet possono essere consultati per fini legati al lavoro, ossia per l'espletamento delle mansioni assegnate. L'accesso è revocabile in qualsiasi momento.
- L'utilizzo dei mezzi elettronici per scopi personali ancorché non commerciali è consentito entro limiti ragionevoli e nel rispetto dei principi generali applicabili (etica, adeguatezza, ecc.), a patto che questo non comprometta l'attività di lavoro. Non è ammesso utilizzare Internet durante l'orario di lavoro per effettuare transazioni finanziarie (telebanking, operazioni borsistiche e simili) personali.
- È espressamente vietato consultare e diffondere materiale a carattere pornografico, razzista, violento, offensivo, degradante, illegale o lesivo del diritto d'autore.
- Non è consentito copiare o installare sui sistemi aziendali programmi o plug-in scaricati da Internet, ossia dati audio/video, videogiochi, immagini e software estranei all'attività lavorativa.
- È vietato utilizzare sistemi di messaggeria istantanea e gruppi di chat non autorizzati.

- Allianz Suisse si riserva il diritto di bloccare l'accesso a pagine Internet palesemente non attinenti all'attività di lavoro.

8. Posta elettronica

- Se possibile, i dipendenti sono tenuti a consultare quotidianamente la posta elettronica pervenuta nella propria casella. In caso di assenza prolungata occorre attivare l'apposita messaggeria automatica.
- Per le e-mail di lavoro è necessario avvalersi esclusivamente dei sistemi mail di Allianz. Non è ammessa la deviazione automatica di e-mail a indirizzi di posta elettronica esterni.
- Vige il divieto di spedire e-mail con identificativo di terzi, fittizio, alterato o dissimulato.
- Se necessario, ad es. in caso di malattia, infortunio, cessazione del rapporto di lavoro o morte del dipendente, l'ISO può, previa consultazione con il superiore, riassegnare a terzi le credenziali di accesso.
- Per quanto riguarda la gestione informatica, le e-mail private sono soggette alle medesime regole valide per le e-mail di lavoro; vale a dire che Allianz Suisse ha la facoltà di proteggere, registrare e archiviare l'intero traffico telematico.
- Cancellare immediatamente catene di sant'Antonio ovvero e-mail pubblicitarie (spam); non è ammesso l'invio di e-mail pubblicitarie, a gruppi di utenti e di catene di sant'Antonio.
- I file allegati di provenienza dubbia o sconosciuta non devono essere aperti né attivati poiché ad alto rischio di malware (virus, trojan, spyware, ecc.).
- In genere, account e indirizzo e-mail dei dipendenti dimissionari vengono cancellati l'ultimo giorno di servizio.

9. Password

- Password e PIN sono personali e segreti; pertanto non devono essere trasmessi o resi accessibili a terzi.
- È vietato abilitare terzi all'accesso di dati e sistemi sotto la propria identità, salvo per interventi del supporto informatico al computer dell'utente in presenza di quest'ultimo. Il dipendente risponde di tutte le transazioni eseguite con il suo user ID.
- Modificare immediatamente la parola chiave qualora sia trapelata o vi sia tale sospetto.
- Le parole chiave standard o predefinite devono essere sostituite al primo avvio del computer.
- Per difendersi adeguatamente dagli attacchi di hacker, creare una password in base a queste regole:
  - lunghezza minima 8 caratteri, in combinazione mista (maiuscole, minuscole, simboli e cifre)
  - evitare i nomi propri, vocaboli del dizionario, date di nascita, numeri di telefono e di targa e altre espressioni o combinazioni facilmente individuabili
  - non utilizzare lettere in ordine alfabetico né in quello della tastiera (es. QWERTZ)
  - modificare la password a cadenza regolare, badando che la nuova non sia troppo simile alla vecchia.

10. Misure in caso di violazione del presente regolamento

Un utilizzo di mezzi informatici illecito o contrario al regolamento, nonché qualsiasi altro comportamento che rappresenti una violazione degli obblighi inerenti al rapporto di lavoro possono incorrere nelle sanzioni previste dalla vigente normativa giuslavoristica. Il dipendente risponde dei danni causati ad Allianz Suisse.

Qualora sussista il fondato sospetto di infrazioni penali commesse via Internet, e-mail o avvalendosi dei mezzi informatici aziendali, Allianz Suisse si riserva di sporgere denuncia.

11. Entrata in vigore

Il presente regolamento entra in vigore il 1° settembre 2009.