# Regolamento per l'utilizzo degli strumenti informatici

**Campo d'applicazione**

1. Tutti gli utenti dell'infrastruttura informatica messa a disposizione da Vebego SA (hardware, software e servizi). Tutti i dati generati e accessibili utilizzando l'infrastruttura informatica.

**Fondamenti giuridici**

2. Per l'impiego degli strumenti informatici vanno rispettate le direttive di sicurezza in materia di protezione dei dati ai sensi della "Legge federale sulla protezione dei dati" (LPD).

**Installazione e configurazione degli strumenti informatici**

3.1 Gli strumenti informatici vengono impostati e sottoposti a manutenzione dal reparto IT in base ai propri standard e direttive.

3.2 È vietato installare hardware e/o software privati.

**Utilizzo professionale di strumenti informatici**

4.1 Tutti i dispositivi informatici (ad es. PC, computer portatili, telefono cellulare ecc.) e le applicazioni devono essere impiegati esclusivamente per fini lavorativi, ad es. per svolgere i compiti aziendali assegnati.

4.2 In particolare l'utilizzo del telefono cellulare, e il relativo abbonamento, messo a disposizione dei collaboratori da Vebego SA deve avvenire esclusivamente per fini lavorativi. Il collaboratore acconsente espressamente che vengano detratti dal proprio salario i costi di chiamata eccedenti CHF 100.– al mese, senza consultazione. Qualora i costi eccedenti CHF 100.– al mese siano motivati per lavoro, verrà richiesto un dettaglio dei costi e gli eventuali scostamenti verranno discussi personalmente con i collaboratori. I collaboratori operanti nell'area di confine con gli stati limitrofi devono attivare manualmente la modalità di selezione della rete sul proprio cellulare. In tal modo si evita di chiamare con un provider estero, generando inutilmente costi elevati di roaming.

4.3 I collaboratori che hanno ricevuto un tablet dichiarano di acconsentire che, in caso di danneggiamento o perdita del dispositivo, vengano dedotti dal salario i costi elencati di seguito:

a) il primo anno (fino a 12 mesi dalla data di messa in funzione del dispositivo): CHF 200.– (2/3 del prezzo dell'apparecchio)
b) il secondo anno (fino a 24 mesi dalla data di messa in funzione del dispositivo): CHF 150.– (1/2 del prezzo dell'apparecchio)

4.4 In linea generale i dispositivi devono essere trattati con la dovuta cura.

4.5 I superiori dal livello di responsabile di esercizio possono autorizzare l'uso dei dispositivi informatici al di fuori del posto di lavoro, in presenza di una esigenza aziendale. Sono responsabili per l'istruzione completa e corretta dei collaboratori.

**Procedura per l'utilizzo degli strumenti informatici**

5.1 I collaboratori ricevono il presente regolamento con il primo utilizzo degli strumenti informatici e apponendo la propria firma dichiarano di aver preso nota del contenuto e di attenersi a quanto specificato.

5.2 Per ciascun collaboratore viene successivamente creato un login personale per accedere alla rete, per le e-mail e la navigazione in Internet (ove necessario).

**Utilizzo del codice utente e delle password**

6.1 I collaboratori sono tenuti ad assicurarsi che terze persone non abbiano accesso ai dati e alle informazioni trasmessi mediante gli strumenti informatici; garantiscono quanto sopra impiegando in modo coerente dispositivi e misure idonei per il controllo degli accessi (ad es. password, scelta, struttura e conservazione della password ecc.).

6.2 Non è consentito trasmettere a terzi i codici utente personali e le rispettive password.

**Internet**

7.1 Tutti i dispositivi collegati alla rete aziendale devono utilizzare esclusivamente l'accesso Internet predisposto a livello centrale.

7.2 Non sussiste alcun diritto d'accesso a Internet. La direzione si riserva la facoltà di bloccare o filtrare informazioni/pubblicazioni dal contenuto inappropriato (ad es. pornografico, razzista, non etico, immorale) o con rischi riconoscibili per l'azienda (pericolo di virus).

**E-mail**

8.1 L'inoltro automatico di e-mail a indirizzi di posta elettronica esterni all'azienda (ad es. alla propria casella di posta privata) non è consentito. In casi giustificati viene allestito un accesso alternativo.

8.2 Le informazioni particolarmente sensibili, quali dati personali, non possono essere inviate all'esterno via e-mail senza codifica. Quanto sopra si applica non solo al contenuto delle e-mail, ma anche ai documenti/allegati acclusi (attachment).

**Accesso da remoto**

9.1 L'accesso da remoto indica l'accesso alla rete aziendale, o ai dispositivi a essa collegati, da un luogo esterno ai locali di Vebego SA.

9.2 Vengono supportati solo i dispositivi designati dal reparto IT.

9.3 Il software che consente di accedere alla rete aziendale può essere installato unicamente dal reparto IT.

**Utilizzo inappropriato e privato**

10.1 L'utilizzo dei calcolatori, di Internet e della posta elettronica deve avvenire tenendo conto degli interessi di Vebego SA, escludendo in particolare rischi giuridici e operativi.

10.2 È espressamente vietato accedere a, o diffondere, materiale dal contenuto illecito, che viola il diritto d'autore, razzista, offensivo, pornografico o sprezzante.

10.3 L'utilizzo privato delle applicazioni Office, di Internet e della posta elettronica è consentito laddove le risorse utilizzate (tempo di lavoro, capacità della rete, spazio di memoria) siano trascurabili. L'utilizzo privato non può compromettere lo svolgimento dei compiti assegnati e va limitato al minimo assolutamente necessario.

10.4 I dati privati (incluse le e-mail private) devono essere archiviati in una cartella separata resa riconoscibile dalla denominazione "Privato" o "Personale".

10.5 Vebego SA si riserva la facoltà di apportare limitazioni tecniche o di bloccare singoli codici utente in caso di utilizzo inappropriato.

**Scaricare (download) o copiare informazioni**

11.1 Ai collaboratori è vietato copiare o scaricare programmi software da Internet risp. e-mail o da altri supporti dati, per poi installarli o distribuirli.

11.2. Altri dati (inclusi quelli con contenuti multimediali) possono essere scaricati sulla rete della gestione unicamente alle condizioni seguenti:

a) i dati devono essere rilevanti per l'azienda e non devono violare le disposizioni speciali in materia di utilizzo privato (di cui sopra, punto 10.1-4);
b) i dati devono essere acquisti o utilizzati rispettando tutti i requisiti di Vebego SA e le disposizioni di legge;
c) i dati non devono essere segnalati come critici per la sicurezza dall'antivirus installato su tutti i computer di Vebego SA.

**Newsletter**

12 I servizi della newsletter devono essere disdetti al momento in cui si lascia l'azienda.

**Eventi rilevanti ai fini della sicurezza**

13 Tutti gli eventi rilevanti ai fini della sicurezza (ad es. smarrimento di un dispositivo, comportamento inspiegabile del sistema, perdita o modifica di dati e programmi, disponibilità di servizi non esplicitamente abilitati, sospetto di uso improprio del proprio codice utente ecc.) devono essere segnalati tempestivamente all'help desk IT. Nota bene: salvo nel caso di smarrimento del dispositivo, non intraprendere alcun tentativo di individuazione perché in tal modo si potrebbero cancellare o perdere eventuali indicazioni e tracce preziose.

**Controlli e registrazione**

14.1 I dati di protocollo servono esclusivamente a conservare i dati e ad assicurare un funzionamento regolare, ai fini del controllo della protezione dei dati e della revisione IT. Non vengono utilizzati ai fini di una valutazione preventiva del comportamento o della prestazione.

14.2 La registrazione avviene nel quadro delle direttive della Legge federale sulla protezione dei dati (Legge sulla protezione dei dati, LPD; RS 235.1), sulla protezione della sfera privata nel quadro delle disposizioni di legge applicabili e altre disposizioni in materia di conservazione dei documenti.

14.3 Al fine di garantire i requisiti di sicurezza di Vebego SA, l'help desk IT verifica periodicamente una valutazione sommaria (senza riferimento a determinate persone) dell'utilizzo di sistemi, applicazioni, reti, e-mail, accesso da remoto e Internet, nonché delle raccolte di dati archiviate sui server. Se da tale verifica emerge il sospetto di un'infrazione al presente regolamento, resta riservata la facoltà di effettuare adeguati controlli riferiti alle persone. Non è consentito un controllo preventivo riferito alle persone.

14.4 In linea di principio i collaboratori vengono informati preventivamente quando viene effettuato un controllo riferito alla persona. Si può rinunciare al preavviso nel caso in cui

a) non sia più possibile garantire la sicurezza dei dati, in particolare la disponibilità del sistema, oppure
b) vi siano indizi di un operato contrario alla legge, in particolare punibile.

14.5 Qualora sulla scorta del controllo riferito alla persona venga riscontrato un uso improprio, verrà informato l'ufficio competente o l'autorità incaricata dell'azione penale.

14.6 Il superiore può verificare i dati aziendali, laddove sia necessario per la propria attività di sorveglianza. Restano impregiudicate disposizioni specifiche in materia di riservatezza.

**Entrata in vigore**

15.1 Il presente regolamento è stato messo in vigore dalla direzione il 1° gennaio 2004 ed è stato rielaborato il 17.05.2019.

15.2 Il presente regolamento per l'utilizzo degli strumenti informatici deve essere sottoscritto da tutti i collaboratori che utilizzano strumenti informatici. L'ultima pagina (pagina 3) viene consegnata in duplice copia, la copia con la firma viene archiviata nella cartella del personale.

Per presa visione:

Data: _____ Firma: _____