ALTO VICENTINO AMBIENTE S.R.L.

Regolamento per l'utilizzo dei sistemi informatici

GENNAIO 2022

REV. 3

SOMMARIO

1. FINALITA'

1.1 Il presente documento disciplina le norme comportamentali cui ciascun lavoratore e collaboratore di Alto Vicentino Ambiente S.r.l. (di seguito, la "**AVA**" o "**Società**") si deve attenere nell'utilizzo delle risorse informatiche e telematiche di cui la Società ha concesso l'utilizzo.

1.2 L'adozione di un regolamento per l'utilizzo dei sistemi informatici è finalizzato alla prevenzione di reati previsti dal D. Lgs. 08 giugno 2001 n. 231 e ss.mm.ii. e a limitare i rischi di indebita diffusione di informazioni sensibili per il *core business* aziendale e l'immagine pubblica della Società.

1.3 La Società inoltre, in qualità di Titolare del trattamento dei dati personali, ritiene necessario dotarsi del Regolamento allo scopo di adempiere agli obblighi fissati dal Regolamento Europeo UE 2016/679 (GDPR), dal D. Lgs. 196/2003 e ss.mm.ii., Codice in materia di protezione dei dati personali, dal suo Disciplinare Tecnico – Allegato B, e dalle "Linee guida del Garante per posta elettronica e internet – 10 marzo 2007" emanato dal Garante per la protezione dei dati personali.

1.5 Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia dalla Società, in qualsiasi forma comunicate, devono intendersi abrogate, qualora incompatibili o difformi, poiché sostituite dalle presenti.

1.6 La Società si riserva la facoltà di apportare, in qualsiasi momento, modifiche al presente documento, dandone comunicazione a tutti i lavoratori interessati con le modalità che riterrà opportune.

1.7 Il Regolamento è stato predisposto a uso esclusivamente interno della Società e, pertanto, non potrà essere riprodotto, divulgato, copiato, utilizzato e/o altrimenti reso pubblico o essere diffuso a terzi in assenza di una previa autorizzazione scritta, né potrà costituire base informativa e/o valutativa per finalità diverse da quelle per le quali è stato predisposto.

2. DESTINATARI

2.1 Il Regolamento si applica ai lavoratori e a tutti coloro che, in virtù di un rapporto di lavoro o di un contratto, trattano informazioni ovvero utilizzano sistemi informativi o apparecchiature elettroniche di proprietà di AVA. Il Regolamento si applica a tutte le sedi della Società che siano state dotate e utilizzino qualsiasi sistema informatico o telematico.

2.2 Il Regolamento, oltre a essere affisso nella bacheca aziendale conformemente alla disciplina di cui all'art.7 della Legge n. 300/1970, verrà consegnato a ciascun lavoratore, anche ai fini dell'art. 13 del Regolamento generale n. 679/2016 e dell'art.4, comma 3°, dello Statuto dei lavoratori. Il Regolamento verrà consegnato, al momento dell'assunzione, a ciascun lavoratore che utilizzi sistemi informativi o apparecchiature elettroniche di proprietà di AVA. Il Regolamento sarà reso noto nelle forme più opportune anche a collaboratori, consulenti, agenti o altri incaricati esterni che siano autorizzati a far uso di strumenti tecnologici di AVA o ad accedere alla rete informatica aziendale e a eventuali dati ed informazioni ivi conservati e trattati.

2.3 È dovere di ogni lavoratore applicare quanto stabilito dal Regolamento, al fine di contribuire personalmente alla tutela del patrimonio delle informazioni aziendali e alla sicurezza dei suoi sistemi informatici, mantenendo la riservatezza sulle caratteristiche del sistema informatico e sulle misure di sicurezza adottate per la sua protezione. Anche dove non disciplinato espressamente dal Regolamento, l'utilizzo delle strumentazioni informatiche e telematiche

dovrà sempre ispirarsi ai principi di legalità, diligenza e correttezza e, più in generale, ai principi stabiliti nel Codice Etico adottato dalla Società.

2.4 La mancata applicazione delle norme contenute nel Regolamento costituisce inadempimento disciplinare e potrà essere sanzionato nei modi e nei termini stabiliti dai contratti nazionali di lavoro applicabili ai lavoratori della Società.

3. GLOSSARIO

Badge identificativo personale: tesserino identificativo personale assegnato in uso al lavoratore o al collaboratore, da utilizzarsi con la finalità di riconoscimento dello stesso (anche presso terzi datori di lavoro), accesso ai siti aziendali e registrazione delle presenze. Il badge identificativo contiene i seguenti dati identificativi del lavoratore: nome, cognome, numero di matricola.

Badge emergenza: tesserino che consente l'accesso indifferenziato a tutti i varchi aziendali presidiati. Il badge emergenza non contiene dati identificativi della persona fisica che lo detiene.

Badge magazzino: tesserino che consente l'accesso al magazzino manutenzione impianto, ubicato presso il sito di Schio, via Lago di Pusiano, 4. Il badge magazzino non contiene dati identificativi della persona fisica che lo detiene.

Badge reperibilità: tesserino che consente l'accesso al sito di Schio, via Lago di Molveno, 23 e assegnato al personale il servizio di reperibilità. Il tesserino non contiene dati identificativi della persona fisica che lo detiene.

Credenziali di autenticazione: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

Dati giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato del trattamento.

Dati personali: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Incaricati del trattamento: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato: la persona fisica cui si riferiscono i dati personali.

Lavoratore: la persona fisica che ha in corso con AVA un rapporto di lavoro subordinato o che utilizza strumenti informatici di proprietà di AVA in forza di un contratto di collaborazione, compresi gli Amministratori.

Responsabile del trattamento: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Titolare del trattamento: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Ufficio Sistemi Informativi: le persone fisiche che sono impiegate nell'Ufficio Sistemi Informativi di AVA e che sono abilitati a intervenire sui sistemi hardware e software della Società.

Violazione di dati personali: violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico.

4. RESPONSABILITA' DELLA SOCIETÀ

4.1 Gli strumenti tecnologici considerati nel presente Regolamento costituiscono strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n.300/1970. Le informazioni raccolte sulla base di quanto indicato nel Regolamento possono essere utilizzate per i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico aziendale ovvero nel singolo strumento, oltre che sulle attività di controllo messe in atto dalla Società.

4.2 I trattamenti effettuati dalla Società rispettano le garanzie poste in essere dal legislatore in materia di protezione dei dati e si svolgono nell'osservanza dei seguenti principi:

a) principio di necessità, secondo cui, in relazione alle finalità perseguite, i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi;
b) principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori, in modo da evitare lo svolgimento di trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa ed effettuati all'insaputa o senza la piena consapevolezza dei lavoratori;
c) principio del trattamento per finalità determinate, esplicite e legittime, secondo un criterio di pertinenza e non eccedenza. In quest'ottica, la Società tratta i dati dei lavoratori nella misura meno invasiva possibile, affidando eventuali attività di monitoraggio esclusivamente a soggetti opportunamente preposti ed effettuando controlli esclusivamente in maniera mirata sull'area di rischio.

4.3 Il trattamento dei dati deve essere ispirato a un canone di trasparenza. Grava quindi sul datore di lavoro l'onere di indicare le corrette modalità di utilizzo degli strumenti informatici messi a disposizione del lavoratore e le modalità di effettuazione di eventuali controlli.

4.4 La Società adotta le necessarie misure per evitare che siano installati o configurati sui sistemi informatici in uso ai lavoratori apparati hardware o strumenti software aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori. Dove l'adozione di tali apparati risultasse necessaria per esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio aziendale, AVA provvederà a darne comunicazione ai lavoratori nelle forme stabilite dalla Legge n. 300/1970, assicurando che il trattamento dei dati contenuti sia effettuato, ove possibile, in forma anonima.

4.5 La Società adotta tutte le misure necessarie affinché i dati personali contenuti nelle postazioni di lavoro informatiche siano protetti contro il rischio d'intrusione – tanto dall'esterno (Internet) che dall'interno (rete locale) – e dall'azione di programmi diretti a danneggiare o interrompere il sistema informatico, di cui all'art. 615-quinquies del codice penale. La Società provvede all'aggiornamento dei software installati sui dispositivi in dotazione ai lavoratori, al fine di prevenire le vulnerabilità degli strumenti elettronici e correggerne i difetti.

4.6 La Società adotta le opportune azioni tecnologiche e organizzative volte ad assicurare il salvataggio dei dati con frequenza almeno settimanale e a garantire il ripristino dell'accesso alle informazioni o agli strumenti elettronici danneggiati in un arco di tempo non superiore ai 7 (sette) giorni.

4.7 Il Responsabile dei Servizi Amministrativi, avvalendosi dell'Ufficio Sistemi Informativi, adotta le misure necessarie a dare attuazione ai presidi di cui di cui ai punti 4.5. e 4.6.

5. RESPONSABILITÀ DEI LAVORATORI

5.1 L'assegnazione e l'utilizzo delle dotazioni informatiche di cui il presente Regolamento e l'utilizzo delle stesse da parte dei lavoratori devono essere improntate ai principi di legalità, imparzialità, correttezza, trasparenza, riservatezza, diligenza, lealtà e buona fede e, più in generale, devono essere coerenti con le disposizioni del codice etico adottato da AVA.

5.2 La Direzione Generale, avvalendosi delle competenti funzioni aziendali, definisce i fabbisogni del personale e stabilisce la dotazione hardware, software e l'accesso alle banche dati aziendali da assegnare a ciascun lavoratore.

5.3 Ciascun lavoratore è responsabile della custodia e del corretto utilizzo di tutta la dotazione assegnata per l'esercizio delle attività lavorative. I dispositivi devono essere utilizzati nell'ambito delle attività lavorative e nei limiti di cui al presente Regolamento. Le dotazioni devono essere custodite con cura da parte degli assegnatari, adottando ogni cautela al fine di evitare danni o sottrazioni delle dotazioni informatiche. Le password e/o gli account assegnati per l'accesso ai dispositivi e/o servizi informatici sono riservati e vanno custodite a cura del lavoratore con la massima diligenza, evitando ogni azione che ne comprometta la riservatezza.

5.4 Eventuali guasti, danneggiamenti, smarrimenti e furti dovranno essere tempestivamente segnalati al Responsabile di Settore/Servizio e al Responsabile Ufficio Sistemi Informativi. La Società si riserva di adottare provvedimenti disciplinari e/o di addebitare al lavoratore i costi di riparazione o di sostituzione dei dispositivi assegnati in uso nei casi di dolo, uso improprio e reiterate rotture/smarrimenti.

5.5 A conclusione del rapporto di lavoro, il lavoratore riconsegnerà la dotazione assegnata al personale dell'Ufficio Sistemi Informativi, che deterrà tale dotazione in custodia.

6. PERSONAL COMPUTER

6.1 Il personal computer è affidato al singolo lavoratore e permette l'accesso alla rete aziendale attraverso specifiche credenziali di autenticazione. Nel caso di personal computer a uso condiviso tra più lavoratori, ciascuno di essi dovrà utilizzare le proprie credenziali di autenticazione. Nel caso di personal computer a uso promiscuo (notebook a disposizione) il lavoratore che prende in carico il personal computer dovrà compilare l'apposito registro.

6.2 Il personale dell'Ufficio Sistemi Informativi è autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la manutenzione, la sicurezza e la salvaguardia del sistema stesso. Qualora lo specifico intervento dovesse comportare l'accesso a contenuti di singoli personal computer, l'Ufficio Sistemi Informativi ne darà preventiva comunicazione ai

lavoratori interessati. In caso di urgenza dell'intervento, l'Ufficio Sistemi Informativi ne darà comunicazione ai lavoratori successivamente alla conclusione dello stesso.

6.3 Il personale dell'Ufficio Sistemi Informativi ha la facoltà di collegarsi e visualizzare in remoto i contenuti dei singoli personal computer al fine di garantire l'assistenza tecnica e ripristinare la normale attività operativa. Gli accessi in remoto saranno effettuati esclusivamente previo consenso del lavoratore cui è assegnato il personal computer o ha in uso lo stesso. Gli interventi in remoto potranno essere effettuati anche in assenza di un preventivo consenso del lavoratore interessato, nei casi in cui sia necessario procedere tempestivamente al fine di assicurare la sicurezza del personal computer o della rete aziendale.

6.4 Non è consentito l'uso di programmi diversi da quelli installati dal personale dell'Ufficio Sistemi Informativi per conto della Società, né viene consentito ai lavoratori di installare autonomamente programmi provenienti dall'esterno.

6.5 Non è consentito ai lavoratori di modificare le componenti hardware del personal computer, né procedere a installare dispositivi esterni (quali, a titolo esemplificativo, hard disk, mouse, casse acustiche, tastiere, monitor o dispositivi di comunicazione tipo chiavette USB), salvo preventiva autorizzazione dell'Ufficio Sistemi Informativi. Non è consentito inoltre intervenire sulla configurazione preimpostata del sistema operativo come ad esempio il salva schermo, l'orologio di sistema o altro.

6.6 Ogni lavoratore dovrà dare tempestiva comunicazione al personale dell'Ufficio Sistemi Informativi nel caso in cui siano rilevati virus o comportamenti anomali del personal computer.

6.7 Il Personal Computer deve essere spento al termine del servizio, prima di lasciare gli uffici o in caso di prolungato inutilizzo.

6.8 Non è consentita l'attivazione della password di accensione (bios) senza preventiva autorizzazione da parte dell'Ufficio Sistemi Informativi.

7. GESTIONE DELLE PASSWORD

7.1 Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate a ciascun lavoratore da parte dell'Ufficio Sistemi Informativi.

7.2 Le credenziali di autenticazione alla rete aziendale LAN consistono in un codice per l'identificazione dell'utente (user id) e una parola chiave (password) riservata che dovrà essere custodita dal lavoratore assegnatario con la massima diligenza e non divulgata. La password, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'assegnatario delle credenziali.

7.3 Le credenziali di autenticazione alle altre risorse informatiche sono definite sulla base delle caratteristiche tecniche di ciascuna risorsa.

7.4 Il lavoratore assegnatario delle risorse che richiedano una autenticazione deve procedere alla modifica della password al primo utilizzo e, successivamente, almeno ogni sei mesi, o prima di tale termine nel caso di perdita di riservatezza.

7.5 Nel caso in cui il lavoratore assegnatario abbia smarrito le credenziali di autenticazione richiederà all'Ufficio Sistemi Informativi l'assegnazione di nuove credenziali di autenticazione.

8. RETE LAN (LOCAL AREA NETWORK)

8.1 Per l'accesso alla rete aziendale della Società ciascun lavoratore deve utilizzare le credenziali univoche di autenticazione assegnate dall'Ufficio Sistemi Informativi. È vietato accedere alla rete utilizzando credenziali di autentificazione diverse da quelle assegnate.

8.2 Le cartelle utenti presenti nei server della Società sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi: qualunque file che non sia legato all'attività lavorativa non può essere dislocato in queste unità. Ciascun lavoratore provvede con regolare periodicità (almeno ogni 3 mesi) alla pulizia delle cartelle di propria competenza dislocate sui server aziendali, con cancellazione dei file obsoleti, inutili o ridondanti. Il Responsabile dei Servizi Amministrativi, avvalendosi dell'Ufficio Sistemi Informativi, esegue le verifiche e i controlli per assicurare il rispetto delle presenti disposizioni.

8.3 L'Ufficio Sistemi Informativi svolge regolari attività di manutenzione, amministrazione e backup sulle cartelle presenti sui server. Diversamente, i dischi e le altre unità di memorizzazione locali non sono soggetti a backup.

8.4 Allo scopo di garantire la sicurezza del sistema informativo aziendale, l'Ufficio Sistemi Informativi esegue analisi sulla presenza di file o applicazioni potenzialmente pericolose che per natura o dimensioni possono compromettere il corretto funzionamento del file server. In questi casi il personale dell'Ufficio Sistemi Informativi procede alla rimozione dei file informando gli utenti riconducibili ai file individuati.

8.5 L'Ufficio Sistemi Informativi potrà acquisire informazioni generate dalle funzionalità insite negli apparati di rete, quali, a titolo esemplificativo, informazioni sugli orari di accensione e spegnimento dei personal computer rilevati automaticamente tramite il sistema di autenticazione al dominio di rete, e i log degli accessi a specifiche risorse di rete (file o cartelle). Tali informazioni potranno essere utilizzate al fine di consentire il corretto funzionamento e la sicurezza degli apparati di rete, con esclusione di qualsiasi forma di controllo sistematico nei confronti dei lavoratori.

8.6 Allo scopo di consentire l'accesso ai server aziendali da remoto, la Società attiva una connessione alla rete dati aziendale tramite VPN (Virtual Private Network). L'abilitazione alla connessione VPN è effettuata dall'Ufficio Sistemi Informativi su richiesta del Responsabile di Settore/Servizio. L'accesso alla VPN avviene mediante credenziali di autenticazione.

9. RETE WIFI

9.1 La Società è dotata di una rete Wi-Fi (PRIVATA) per la connessione wireless dei dispositivi aziendali (notebook, smartphone o altro). Tale rete consente la navigazione, la connessione ai server aziendali e l'utilizzo di tutte le risorse di rete (es. stampanti). La password di accesso alla rete Wi-Fi è definita dall'Ufficio Sistemi Informativi e comunicata ai lavoratori autorizzati. L'uso della rete Wi-Fi è consentito esclusivamente per dispositivi aziendali.

9.2 La Società è dotata inoltre di una rete Wi-Fi (PUBBLICA) ad uso di ospiti che occasionalmente intendono avvalersi del servizio Wi-Fi. Tale connessione pubblica è fruibile previa registrazione dell'ospite e consente esclusivamente l'accesso a internet, con inibizione dell'accesso ad altre risorse aziendali.

10. TELEFONI FISSI

10.1 Le chiamate in entrata dirette al numero di fonia fissa aziendale e provenienti dall'esterno sono centralizzate presso l'Ufficio di AVA incaricato della gestione del servizio (Centralino). L'Ufficio incaricato della gestione del Centralino provvede a inoltrare la chiamata alla numerazione interna interessata. Negli orari di chiusura degli uffici aziendali le numerazioni interne rimangono raggiungibili esclusivamente attraverso la digitazione del numero interno.

10.2 Per le chiamate in entrata dirette a uno specifico ufficio, i lavoratori appartenenti allo stesso sono tenuti a prendere in carico le chiamate dirette ai colleghi, in caso di assenza degli stessi.

11. TELEFONI CELLULARI

11.1 I telefoni cellulari sono assegnati al lavoratore in relazione a motivate esigenze di servizio. E' fatto obbligo al lavoratore di tenere acceso il dispositivo durante l'orario di servizio e custodirlo con diligenza.

11.2 La Sim in dotazione al lavoratore non può essere utilizzata su dispositivi diversi da quelli assegnati dalla Società.

11.3 A ciascuna Sim è associato un profilo tariffario che consente la fruizione dei servizi voce/dati entro specifici limiti stabiliti nel contratto di somministrazione vigente tempo per tempo stipulato da AVA con fornitori di tali servizi. L'assegnazione del profilo tariffario voce/dati è definito dall'Ufficio Sistemi Informativi in relazione agli specifici fabbisogni conseguenti alla mansione del lavoratore.

11.4 I telefoni cellulari e i relativi accessori assegnati in dotazione ai lavoratori devono considerarsi strumenti di lavoro: ne viene concesso l'uso per lo svolgimento delle attività lavorative. La ricezione o l'effettuazione di telefonate personali, così come l'invio o la ricezione di SMS o MMS di natura personale o comunque non pertinenti con lo svolgimento dell'attività lavorativa, viene consentita solo nel caso di necessità e urgenza.

11.5 I dispositivi cellulari assegnati in dotazione devono essere protetti mediante codice PIN al fine di evitare l'uso improprio del dispositivo da parte di soggetti diversi dell'assegnatario.

11.6 I dispositivi smartphone sono preconfigurati con un account di servizio al fine di garantire gli aggiornamenti del software e delle applicazioni installate. Le credenziali di accesso sono consegnate al lavoratore assegnatario del dispositivo a cura dell'Ufficio Sistemi Informativi. Per telefoni che consentono l'utilizzo della mail, la gestione della posta avviene come riportato al capitolo 14.

11.7 È consentito l'installazione e l'uso di applicazioni diverse da quelle già installate e predefinite purché le stesse siano funzionali all'esercizio alle mansioni assegnate al lavoratore.

11.8 Il lavoratore assegnatario di dispositivi smartphone dovrà tempestivamente avvisare il proprio responsabile di settore/servizio e l'Ufficio Sistemi Informativi in caso di smarrimento, furto o danneggiamento del telefono così come nel caso di problemi tecnici, traffico anomalo, mancata connettività o comportamenti anomali del dispositivo.

12. STAMPANTI E FOTOCOPIATRICI

12.1 L'utilizzo di dispositivi di stampa multifunzione è consentito previo inserimento di un codice di identificazione personale univoco attribuito a ciascun lavoratore dall'Ufficio Sistemi Informativi. Il medesimo codice è preconfigurato sui personal computer, fissi e portatili, assegnati al lavoratore.

12.2 Il codice personale consente l'utilizzo di tutti dispositivi di stampa multifunzione e consente di conteggiare il numero di fotocopie, stampe e scansioni eseguite da parte di ciascun lavoratore.

13. SUPPORTI RIMOVIBILI

13.1 È vietato l'utilizzo di supporti rimovibili diversi da quelli assegnati o autorizzati dalla Società.

13.2 Tutti i supporti rimovibili (CD, DVD, supporti USB, ecc.), contenenti dati aziendali devono essere trattati in modo tale da evitare che il loro contenuto possa essere trafugato, alterato e/o distrutto o, successivamente alla cancellazione, recuperato. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati aziendali, ciascun lavoratore dovrà seguire le disposizioni impartite dall'Ufficio Sistemi Informativi.

13.3 Il lavoratore resta in ogni caso responsabile della custodia dei supporti e dei dati aziendali in essi contenuti. A tal fine, i supporti rimovibili contenenti dati sensibili devono essere custoditi in armadi chiusi.

14. POSTA ELETTRONICA

14.1 La Società potrà assegnare o ritirare l'utilizzo della casella di posta elettronica al lavoratore in base alla propria esclusiva e insindacabile valutazione circa la necessità di utilizzo della stessa per lo svolgimento delle attività lavorative.

14.2 Le caselle di posta elettronica potranno essere assegnate a singoli lavoratori (in tal caso l'indirizzo di posta elettronica sarà composto come segue: nome.cognome@altovicentinoambiente.it) o a gruppi funzionali (es. info@altovicentinoambiente.it). Nel caso di mail funzionali, la casella di posta elettronica è assegnata a uno o più lavoratori che la gestiranno congiuntamente al fine di assicurare la continuità operativa della funzione aziendale cui corrisponde la casella di posta elettronica. Nel caso di cambio di mansione di un lavoratore assegnatario di una mail funzionale o di cessazione del rapporto di lavoro, l'intero archivio dei messaggi sarà trasferito ai nuovi lavoratori incaricato della gestione della cesella di posta.

14.3 L'archiviazione dei messaggi viene effettuata sui personal computer e server di AVA o su server esterni in disponibilità della Società.

14.4 I messaggi contenuti nella casella di posta assegnata a ciascun lavoratore sono archiviati sui personal computer locali e non sono soggetti a periodici backup. I messaggi aventi natura di corrispondenza istituzionale e commerciale dovranno essere gestiti attraverso le procedure di protocollo, al fine di garantirne la conservazione sui server aziendali per un periodo di 10 anni. Ciascun assegnatario della casella di posta elettronica dovrà provvedere a eliminare periodicamente i messaggi di posta elettronica per i quali non si ritenga necessaria la conservazione. Il Responsabile dei Servizi Amministrativi, avvalendosi dell'Ufficio Sistemi Informativi, esegue le verifiche e i controlli per assicurare il rispetto delle presenti disposizioni.

14.5 Al fine di ribadire ai terzi destinatari dei messaggi di posta elettronica la natura esclusivamente aziendale della casella di posta elettronica, i messaggi dovranno contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi, precisando che il personale debitamente incaricato della Società potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nel presente Regolamento.

14.6 È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo. È fatto divieto di effettuare il download di file eseguibili o documenti da siti Web o Ftp non conosciuti.

14.7 In caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella), l'assegnatario della casella di posta elettronica dovrà provvedere ad attivare un messaggio di risposta automatica con indicazione delle modalità di contatto del proprio ufficio in caso di assenza. In caso di assenza non programmata (ad es. per malattia) l'attivazione del messaggio di risposta automatica, qualora non possa essere effettuata direttamente dal lavoratore avvalendosi del servizio webmail, sarà effettuata a cura dell'Ufficio Sistemi Informativi.

14.8 Nei casi di assenza e limitatamente alla durata della stessa, ciascun lavoratore potrà autorizzare il proprio superiore gerarchico all'accesso alla propria casella di posta elettronica per i casi di urgenza e necessità. Tale autorizzazione dovrà essere formalizzata.

14.9 In caso di cessazione del lavoratore la casella di posta elettronica personale dovrà essere tempestivamente disattivata a cura dell'Ufficio Sistemi Informativi, unitamente alle credenziali di autenticazione per l'accesso alla rete. I messaggi di posta elettronica in entrata, successivamente alla disattivazione, dovranno generare un messaggio di risposta automatica nel quale si informa il mittente dell'avvenuta disattivazione della casella di posta. La corrispondenza contenuta nell'archivio di posta elettronica sarà conservata dalla Società a cura dell'Ufficio Sistemi Informativi per un periodo di sei mesi, decorrenti dalla data di cessazione del lavoratore. Nell'arco di tale periodo, in presenza di un interesse legittimo, concreto e attuale della Società o di un terzo, il titolare del trattamento potrà autorizzare l'accesso agli archivi di posta elettronica e la conservazione della sola corrispondenza necessaria a tutelare tale interesse, a condizione che lo stesso non violi i diritti e libertà fondamentali dell'assegnatario della casella di posta elettronica. Decorso il termine di sei mesi, l'Ufficio Sistemi Informativi provvede alla cancellazione definitiva dell'archivio di posta elettronica del lavoratore cessato.

15. NAVIGAZIONE IN INTERNET

15.1 La navigazione internet è consentita per finalità istituzionali inerenti alle mansioni svolte da ciascun lavoratore.

15.2 L'upload, il download e la condivisione di contenuti, ancorché gratuiti, è consentito esclusivamente per finalità attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione. È vietata l'effettuazione di ogni genere di transazione finanziaria via web, per finalità diverse da quelle istituzionali.

15.3 Le registrazioni a siti web, la partecipazione a forum, a social network, a chat line, sono ammessi esclusivamente per finalità istituzionali nell'ambito delle mansioni assegnate a ciascun lavoratore. Le credenziali d'accesso devono essere conservate a cura esclusiva del lavoratore che ha effettuato la registrazione. Nei casi in cui la registrazione sia effettuata a titolo aziendale e non sia riconducibile ad una specifica persona fisica, l'iscrizione dovrà essere autorizzata dal responsabile di settore\servizio e le credenziali di autentificazione dovranno essere conservate a cura dello stesso.

15.4 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, AVA adotta uno specifico sistema di blocco o filtro automatico che previene determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una "black list". Gli eventuali controlli, compiuti dal personale incaricato dell'Ufficio Sistemi Informativi, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della

navigazione svolta. Il controllo sui file di log non è continuativo e i file stessi saranno conservati non oltre sei mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza della Società.

16. PROTEZIONE ANTIVIRUS

16.1 Il sistema informatico della Società è protetto da software antivirus e aggiornato periodicamente. Ogni lavoratore deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro *malware*.

16.2 Nel caso in cui il software antivirus rilevi la presenza di un virus, il lavoratore dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto all'Ufficio Sistemi Informativi.

16.3 Ogni dispositivo rimovibile di provenienza esterna alla Società dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato al personale dell'Ufficio Sistemi Informativi.

17. PARTECIPAZIONE AI SOCIAL MEDIA

17.1 L'attivazione e l'utilizzo a fini istituzionali e commerciali dei profili aziendali sui social media – quali Facebook™, Twitter™, Linkedin™, dei blog e dei forum, anche professionali, saranno gestiti e organizzati esclusivamente dalla Società attraverso specifici ordini di servizio e istruzioni operative al personale a ciò espressamente dedicato.

17.2 Fermo restando il diritto della persona alla libertà di espressione e al libero scambio di idee e opinioni, tutti i soggetti destinatari del presente Regolamento sono tenuti ad adottare le seguenti regole comportamentali nell'utilizzo dei profili personali sui social media:

- dovrà essere garantita la segretezza delle informazioni aziendali riservate, con particolare riferimento a piani industriali, identificazione di clienti e fornitori, informazioni di natura commerciale e finanziaria;
- ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che della Società. L'utilizzo di marchi e altri segni distintivi della Società potrà avvenire solo previa autorizzazione specifica della Direzione Generale;
- dovrà essere garantita la privacy delle persone: non potranno essere comunicati o diffusi dati personali (quali dati anagrafici, immagini, video, suoni e voci) di altri lavoratori della Società, se non con il preventivo consenso di questi, e comunque non potranno esseri pubblicati sui social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro;
- ciascun lavoratore risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti della Società, Soci, lavoratori della stessa, clienti e fornitori, attività che possano essere penalmente o civilmente rilevanti, con particolare riferimento a comportamenti ingiuriosi, diffamatori e denigratori, discriminatori;
- ciascun lavoratore, nell'uso dei social media, esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario o opportuno per la possibile connessione con la Società (ad es. nell'ambito di forum professionali) il lavoratore dovrà precisare che le opinioni sono espresse esclusivamente a titolo personale e non in nome e per conto della Società.

18. FIRME DIGITALI

18.1 I possessori di dispositivi di firma digitale utilizzano tali dispositivi nell'ambito dei poteri, delle procure e delle deleghe loro assegnate dalla Società.

18.2 La corretta conservazione dei dispositivi di firma e delle associate credenziali è cura esclusiva del titolare della firma.

19. SISTEMA DI CONTROLLO ACCESSI

19.1 La Società assegna a ciascun lavoratore un badge identificativo personale, per le seguenti finalità:

- identificazione personale del lavoratore, anche al di fuori dei siti aziendali. Il badge identificativo dovrà essere custodito dal lavoratore ed esibito, ai fini del riconoscimento, su richiesta di terzi, nel caso di accesso in aree private per motivi di servizio o a organi di polizia;
- rilevazione delle presenze, al fine di registrare sistematicamente gli orari di inizio e fine del proprio orario di lavoro;
- consentire l'accesso ai siti aziendali e, all'interno degli stessi, a singole aree o locali, in base ad autorizzazioni di accesso e limiti temporali stabiliti dalla Società.

19.2 Il badge è di proprietà della Società e deve essere conservato con cura dal lavoratore, segnalando tempestivamente al Servizio Personale eventuali danneggiamenti o lo smarrimento dello stesso. E' vietata la cessione a terzi del badge identificativo personale.

19.3 AVA si avvale di un sistema elettronico di controllo degli accessi ai siti aziendali di Schio, via Lago di Pusiano, 4 e Schio, via Lago di Molveno, 23. I varchi esterni, carrai e pedonali e le porte di accesso ai locali aziendali sono dotati di lettori badge di prossimità o di antenne di prossimità mediante i quali sono attivate le elettro-serrature delle porte e i motori dei cancelli/sbarre carrai. I varchi sono riportati in una planimetria aggiornata a cura dell'Ufficio Sistemi Informativi. Il sistema di controllo accessi è centralizzato e gestito mediante software. L'accesso al software è riservato al Servizio personale per la definizione dei profili autorizzativi dei lavoratori e all'Ufficio Sistemi Informativi per la manutenzione del software.

19.4 Il badge identificativo personale è assegnato al lavoratore a cura del Servizio Personale, il quale provvede a stabilire i profili autorizzativi per l'accesso ai siti e ai locali aziendali, in funzione delle mansioni e dell'orario di lavoro. Unitamente al badge identificativo personale è rilasciato un tag RFID passivo per l'accesso con il proprio veicolo tramite i varchi carrai autorizzati.
Alla consegna del badge, il Servizio Personale comunica al lavoratore l'elenco dei varchi cui lo stesso è abilitato e i relativi orari autorizzati. Analoga comunicazione è effettuata in caso di modifica dei profili autorizzativi del lavoratore.
In caso di smarrimento o danneggiamento del badge identificativo o del tag RFID, il lavoratore provvederà a darne comunicazione al Servizio Personale, il quale provvederà a bloccare il dispositivo smarrito e a consegnarne uno nuovo al lavoratore.
I lavoratori potranno richiedere al Servizio personale il rilascio di n. 1 duplicato del tag RFID che sarà rilasciato dietro il pagamento di 5,00 euro a titolo di spese amministrative. Analogo corrispettivo sarà dovuto in caso di emissione di nuovi dispositivi in caso di smarrimento.
I badge "auto aziendali", "mezzi d'opera", "emergenza", "magazzino" e "reperibilità" sono emessi dal Servizio Personale.

19.5 I badge "auto aziendali" e "mezzi d'opera" sono dispositivi installati a bordo dei veicoli e mezzi d'opera aziendali e consentono l'accesso degli stessi agli impianti aziendali.

19.6 I badge "emergenza" sono custoditi presso la Sala Controllo dell'impianto di termovalorizzazione (per il sito di Schio, via Lago di Pusiano, 4) e presso ciascuno stabile per uffici per il sito di Schio, via Lago di Molveno, 23).
I badge di emergenza sono conservati all'interno di una scatola di emergenza sigillata, protetta con vetro frangibile e potranno essere prelevati soltanto in situazioni di emergenza.

19.7 I badge "magazzino" sono assegnati al Capoturno dell'impianto di termovalorizzazione e consentono l'accesso al magazzino della sede di via Lago di Pusiano, 4. Il badge è custodito dal Capoturno in servizio e consegnato al Capoturno entrante.

19.8 I badge "reperibilità" sono assegnati al personale in servizio di reperibilità e consentono l'accesso al sito di Schio, via Lago di Molveno, 23 durante negli orari di chiusura del sito. Il badge è custodito dal personale in servizio di reperibilità e consegnato al reperibile entrante.

19.9 L'accesso di fornitori, clienti e ospiti ai siti aziendali è preventivamente autorizzato dalla Società. L'accesso avviene previa identificazione presso:
- Ufficio Protocollo oppure Ufficio Ricevimento, per il sito di Schio, via Lago di Pusiano, 4;
- Ufficio Ricevimento e Ufficio Logistica-pianificazione, per la sede di Schio, via Lago di Molveno, 23.

Lo spostamento dei terzi all'interno dei siti è effettuato soltanto se accompagnati da personale della Società.

20. VIDEO SORVEGLIANZA

20.1 AVA si avvale di un impianto di videosorveglianza operativo 24 ore su 24 nelle aree di pertinenza delle sedi. Le immagini riprese dal sistema sono oggetto di trattamento con l'ausilio di strumenti elettronici e nel rispetto della normativa a tutela dei dati personali e della Legge n. 300/1970.

21. SERVIZIO DI MENSA SOSTITUTIVA

21.1 AVA organizza un servizio di mensa sostitutiva a favore dei lavoratori con turno spezzato. Il Servizio personale assegna ai lavoratori beneficiari un badge identificativo personale da utilizzare presso gli esercizi convenzionati nei giorni e nelle fasce orario stabilite dalla Società.

21.2 In caso di smarrimento o danneggiamento del badge, il lavoratore provvederà a darne comunicazione al Servizio Personale, il quale provvederà a bloccare il dispositivo smarrito e a consegnarne uno nuovo al lavoratore. In caso di smarrimento del badge, il rilascio del badge sostitutivo sarà effettuato dietro il pagamento di 5,00 euro a titolo di spese amministrative.

22. MONITORAGGIO E CONTROLLO

22.1 Il Responsabile dei Servizi Amministrativi, avvalendosi dell'Ufficio Sistemi Informativi, esegue le verifiche e i controlli per assicurare il funzionamento e garantire la sicurezza dei sistemi informatici di cui al presente Regolamento. Verifica altresì il rispetto dei limiti di spesa stabiliti dalla Società per il funzionamento dei sistemi informatici.

22.2 Le attività di controllo, che potranno essere effettuate sia in forma generalizzata sia su base individuale, danno luogo ad avvisi diretti ai lavoratori che utilizzano le risorse informatiche in cui è stata rilevata l'anomalia. Il contenuto di tali avvisi evidenzia l'utilizzo irregolare degli strumenti aziendali e invita i lavoratori ad attenersi ai compiti assegnati e alle istruzioni impartite.

22.3 In caso di riscontrate anomalie o violazioni, il Responsabile dei Servizi Amministrativi dispone le azioni per la messa in sicurezza e per il ripristino delle funzionalità e, ove ne ricorrano i presupposti, segnala i fatti alle competenti funzioni aziendali per l'adozione di provvedimenti di competenza.