REGOLAMENTO DOTAZIONI ICT

DESCRIZIONE	APPROVAZIONE	Data approvazione	Entrata in vigore
Regolamento Utilizzo strumenti informatici aziendali Versione 1.1	Consiglio di Amministrazione	30/09/2022	30/09/2022 per la Capogruppo
			13/10/2022 per le SOL

Sommario

1. SCOPO E AMBITO DI APPLICAZIONE

Lo scopo del presente regolamento è di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione informatica da parte degli utenti assegnatari (dipendenti, collaboratori etc.), al fine di tutelare i beni aziendali ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre il Gruppo RetiAmbiente (in seguito anche la "**Società**") a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi. Il presente regolamento mira anche a garantire la sicurezza dei dati personali trattati dalla Società mediante una puntuale e dettagliata disciplina delle modalità di accesso e di utilizzo dei sistemi informativi aziendali a cui il personale è abilitato, e degli strumenti informatici che la Società può assegnare ai propri utenti.

Gli utenti dei sistemi informativi (in seguito anche gli "**Utenti**") sono i dipendenti e collaboratori esterni autorizzati all'accesso ai medesimi sistemi informativi o ai dati di Retiambiente o delle Società Operative Locali (in seguito anche SOL).

Retiambiente può mettere a disposizione dei propri Utenti i seguenti strumenti di lavoro informatici (di seguito anche "**dotazioni ICT**") in funzione del ruolo e delle esigenze lavorative di volta in volta valutate:

- strumenti di informatica individuale: personal computer e relativi accessori, smartphone, tablet/palmari, etc. (di seguito anche i "**dispositivi**");
- apparati e servizi, anche condivisi: rete aziendale, posta elettronica, accesso internet, stampanti di rete, file server, etc.;
- applicativi gestionali e/o di office automation.

Le risorse informatiche aziendali affidate all'utente sono strumenti di lavoro e come tali possono essere utilizzate solo per scopi strettamente professionali, in relazione alle mansioni assegnate. Ciò vale sia per le risorse condivise (risorse di rete, stampanti di rete, ecc.), sia per quelle affidate al singolo dipendente (smartphone, personal computer, periferiche, stampanti locali, ecc.). Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di gestione e/o manutenzione e, soprattutto, minacce alla sicurezza. Si ricorda che le risorse informatiche aziendali sono strumenti di lavoro appartenenti al patrimonio aziendale e pertanto vanno custoditi in modo appropriato; il furto, il danneggiamento o lo smarrimento di tali strumenti debbono essere prontamente segnalati all'ufficio ICT ed al proprio responsabile.

Nell'utilizzo delle risorse informatiche il personale aziendale deve astenersi da comportamenti che possa determinare degli illeciti anche ai sensi del D.Lgs. 231/2001. In particolare, è fatto divieto di istallare programmi informatici in violazione del diritto di autore, utilizzare le risorse informatiche aziendali per compiere delitti informatici previsti nel Modello 231 (es. accesso abusivo ad un sistema informatico altrui, danneggiamento di sistemi informatici di rete) o altre fattispecie di reato presupposto della responsabilità amministrativa dell'ente.

La Società declina ogni responsabilità per un eventuale utilizzo degli strumenti aziendali non rispondente alla normativa in essere. Si ricorda che il CCNL Utilitalia dei Servizi Ambientali, all'art. 66, lettera f, prevede quanto segue: … "*il lavoratore deve[…] aver cura dei locali, nonché di tutto quanto a lui affidato (mobili, attrezzi, macchinari, strumenti, automezzi, eccetera)*". Il mancato

rispetto del dettato contrattuale comporta l'attivazione di una procedura disciplinare in conformità al sistema disciplinare aziendale.

2. RIFERIMENTI NORMATIVI

Il quadro normativo di riferimento è rappresentato da:

- Il Regolamento Generale sulla protezione dei dati personali UE n.679/2016 (in breve, **"GDPR"**);
- D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018 (c.d. Codice Privacy, in breve anche il **"Codice"**);
- L. 300/'70 c.d. Statuto dei lavoratori;
- Provvedimenti del Comitato europeo per la protezione dei dati personali (EDPB);
- Provvedimento del Working Party art. 29, laddove compatibili con la normativa vigente
- I Provvedimenti del Garante per la protezione dei dati personali (in breve il **"Garante"**);
- CCNL Utilitalia Servizi Ambientali;
- Modello di organizzazione 231/01.

3. MODALITÀ DI ACCESSO ALLA RETE AZIENDALE

3.1 Accessi da rete aziendale cablata

I locali delle sedi delle società del Gruppo Retiambiente sono generalmente dotati di accesso alla rete aziendale. I dispositivi appartenenti al dominio aziendale vengono autorizzati all'accesso alla rete dalla Unità Organizzativa ICT; eventuali dispositivi non appartenenti al dominio aziendale avranno accesso esclusivamente alla rete guest/ospiti che permetterà un insieme limitato di funzionalità (p.e. solo l'accesso ad internet) e autorizzati dalla Direzione Generale.

3.2 Accessi alla rete wifi

Le sedi possono essere dotate di una o più reti wifi con protocollo di sicurezza WPA2 o successivi. Inoltre, laddove sia necessario, sarà presente una rete wifi "ospiti" che non consente in nessun caso l'accesso alla rete aziendale, ma solo l'accesso ad internet (con le caratteristiche descritte ai successivi 4.9, 4.10) con eventualmente un limite temporale oltre il quale la connessione verrà interrotta, che dovrà essere utilizzata solo per scopi lavorativi.

3.3 Accessi dall'esterno

L'accesso alle risorse informatiche e alla rete locale effettuato dall'esterno ovvero da internet (anche da collegamenti mobili) può avvenire, per gli utenti abilitati ed autorizzati dalla Direzione, tramite collegamenti VPN cifrati e con doppio fattore di autenticazione. E' fatto divieto scaricare file aziendali, se non per lo stretto periodo di utilizzo, su dispositivi non di proprietà aziendale; specifiche direttive sono riportate al punto 4.13 prestazione lavorativa svolta fuori dalle sedi aziendali.

3.4 Accessi da parte di terzi

Gli accessi di terzi devono essere regolamentati con apposita procedura.

3.5 Assistenza da remoto

Per facilitare le operazioni di aggiornamento del software e per garantire la sicurezza dei dispositivi, delle applicazioni e dei dati, il personale incaricato della U.O. ICT può avvalersi di strumenti di controllo remoto che consentano di compiere le operazioni necessarie attraverso la rete locale. Tali strumenti non sono comunque utilizzati per avere accesso a dati o documenti. L'assistenza tecnica per malfunzionamenti ordinari o diagnosi di sistema attraverso strumenti di controllo remoto avviene di norma previa autorizzazione dell'utilizzatore e in presenza dell'utilizzatore stesso. In caso di malfunzionamenti straordinari e in situazioni di emergenza, il personale incaricato della U.O. ICT ha comunque facoltà di accedere in qualunque momento ai sistemi informatici per l'espletamento delle proprie funzioni.

4. LE POSTAZIONI DI LAVORO

4.1 Definizione delle postazioni di lavoro

Le postazioni di lavoro standard della Società non richiedono la sottoscrizione di verbale di consegna e prevedono:

Per tutti gli Utenti:

- N. 1 Personal Computer (anche portatile), monitor, tastiera, mouse, con accesso alla rete dati della Società;
- N. 1 Telefono fisso.

Tutti i dispositivi che vanno a formare dotazione di lavoro, ad esclusione delle postazioni standard, sono assegnati al dipendente o alla U.O. e sono consegnati previa sottoscrizione di un apposito verbale (in caso di assegnazione alla U.O. sarà il Responsabile a firmare per la consegna).

4.2 Utilizzo delle postazioni di lavoro

La U.O. ICT fornisce il necessario supporto agli Utenti per il corretto utilizzo delle postazioni di lavoro.

Gli Utenti sono tenuti a conservare le postazioni di lavoro nella configurazione loro assegnata.

Ogni modifica delle postazioni di lavoro deve essere richiesta alla U.O. ICT, la quale provvede a porla in essere dopo aver ottenuto le eventuali autorizzazioni.

È quindi vietato, senza la preventiva autorizzazione della U.O. ICT:

- togliere/aggiungere/modificare le componenti hardware e software;
- cambiare l'ubicazione delle apparecchiature fisse (PC, telefoni, fotocopiatrici, scanner, etc.).

Non è consentito asportare dalle sedi aziendali hardware e supporti magnetici, ottici o cartacei, se non preventivamente autorizzati; l'autorizzazione è data dalla U.O. ICT relativamente all'hardware e dal proprio Responsabile di U.O. relativamente al trasferimento di dati o nel caso di documentazione cartacea.

4.3 Installazione di software

Sulle postazioni di lavoro può essere installato esclusivamente software acquisiti regolarmente, in osservanza alle normative vigenti. Tali software vengono installati dalla U.O. ICT e la stessa U.O., periodicamente, verifica i software installati e rileva eventuali programmi non autorizzati, che

saranno immediatamente disinstallati, ferma restando la possibilità di attivazione di una procedura sanzionatoria, in conformità al sistema disciplinare aziendale.

4.4 Autenticazione dell'Utente

Le credenziali di autenticazione per l'accesso ai dispositivi, alla rete e agli applicativi vengono assegnate dalla U.O. ICT, previa formale richiesta del Responsabile della U.O. interessata.

Ciascun Utente è autenticato tramite delle credenziali (Username e Password) mediante le quali ha accesso alle risorse ed è personalmente responsabile per tutte le attività effettuate con tali credenziali.

Ogni Utente deve avere massima cura alla custodia ed alla riservatezza delle proprie credenziali.

Le password devono possedere i seguenti requisiti:

- deve contenere minimo 8 caratteri;
- di default deve essere cambiata almeno e non oltre ogni 180 giorni;
- non può contenere parte del proprio nome o username utente (ad esempio, Mario123 o Rossi123 non sono password accettabili) in modo che non sia agevolmente riconducibile all'identità del medesimo; si sconsiglia di usare anche i nomi dei familiari
- deve contenere minimo 3 tipi di caratteri compresi fra questi 4: maiuscole, minuscole, numeri, caratteri speciali (~! @ # $% ^& * -+ =' | \ \ (){}\ []:; "' <>,.? /)

L'Utente è tenuto a conservare nella massima segretezza la/le password e qualsiasi altra informazione legata al processo di autenticazione.

Si raccomanda di non utilizzare le password usate per l'accesso ai sistemi della Società anche per sistemi di autenticazione esterni, come ad esempio l'accesso al proprio conto corrente bancario o alla propria Web Mail privata, o a quella utilizzata per la registrazione a siti o servizi Web di varia natura (e-commerce, etc.)

In caso di non utilizzo della postazione per un periodo (tale impostazione non dovrà superare 15 minuti) dovrà essere impostato un blocco del PC/portatile, per la disattivazione del quale sarà necessario digitare nuovamente la password.

Ogni Utente è responsabile delle operazioni eseguite ed è tenuto a:

- provvedere sempre alla corretta "uscita" dall'applicazione in uso, disattivando l'abilitazione prima di lasciare la postazione di lavoro (ad esempio mediante la disconnessione);
- disconnettersi dal sistema o attivare il blocco protetto da password, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la postazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima. Lasciare un elaboratore incustodito connesso alla rete può comportarne l'utilizzo da parte di terzi senza che vi sia la possibilità di provarne, in seguito, l'indebito uso;
- sostituire immediatamente la password nel caso si sospetti la perdita di segretezza, informandone quanto prima l'U.O. ICT;
- spegnere, ogni fine turno, il proprio elaboratore prima di lasciare gli uffici salvo diverse disposizioni o in caso di particolari necessità previamente concordate con la U.O. ICT.

4.5 Archivio file

Tutti i file, anche temporanei, che si riferiscono all'attività lavorativa e per i quali vi è la necessità di un salvataggio ai fini di garantirne la costante disponibilità, dovranno essere memorizzati sulle unità di rete appositamente predisposte. La disposizione vale soprattutto per i file contenenti dati personali per i quali, per obbligo di Legge, va garantito un salvataggio costante.

È sconsigliato archiviare file nelle cartelle personali (come la cartella "Documenti" o il Desktop) pregiudicandone in tal modo il backup ed impedendo che i file siano disponibili per i colleghi della rispettiva U.O. e per l'Azienda.

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi in queste unità, sulle quali vengono svolte regolari attività di amministrazione, controllo e backup.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante. La U.O. ICT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza della rete aziendale. L'archiviazione di file e documenti sui fileserver aziendali prevede la creazione di cartelle di rete dedicate alle singole U.O. Per regola, l'accesso a ciascuna cartella di rete è consentito esclusivamente al personale della U.O. cui la cartella di rete si riferisce ed al Dirigente/Soggetto apicale cui il Responsabile della U.O. in questione riporta.

I soggetti di cui sopra sono, dunque, gli unici abilitati ad effettuare operazioni di trattamento dei dati sui file contenuti nella cartella di rete come ad esempio: apertura file, salvataggio, modifica, cancellazione, copia, etc..

Nell'eventualità in cui un Responsabile o un addetto di altra e diversa U.O., per scopi lavorativi, abbia la necessità di accedere anche solo temporaneamente alla/e cartella/a di rete specificamente riferita/e ad altra U.O., è necessario seguire la seguente procedura:

I. il Responsabile della U.O. che ha tale esigenza ne informa adeguatamente il Responsabile della U.O. alla cui cartella è necessario accedere, il quale valuterà e autorizzerà o meno l'accesso, dandone informazione alla U.O. ICT affinché provveda all'abilitazione; in caso di utilizzo di strumenti di file sharing e collaboration in cloud (tipo Microsoft 365) l'utente, previa autorizzazione del proprio responsabile, può dare accesso alla cartella/file ad un altro utente di altro U.O (tale attività verrà registrata su apposito log);

II. in caso di mancata autorizzazione, il Responsabile della U.O. richiedente ha facoltà di interpellare la Direzione Generale, la quale assumerà le decisioni del caso;

III. In caso di presenza di strumenti che consentono la condivisione all'esterno dell'azienda di file/cartelle tramite invio di link per lo scarico, anche temporanei e/o protetti da password, tale abilitazione sarà consentita solo ai responsabili delle U.O. (anche questa attività verrà registrata su apposito log);

Nel caso in cui – per esigenze lavorative – sia necessario creare cartelle di rete condivise da diverse U.O., i rispettivi Responsabili ne daranno comunicazione al responsabile della U.O. ICT, indicando i nominativi dei soggetti cui concedere l'accesso, con le specifiche riguardo alle modalità di trattamento dei dati contenuti nelle cartelle medesime (sola lettura, modifica, etc.), il periodo per

cui viene dato l'accesso (in caso di accesso solo temporaneo) ed il nome della cartella cui dare accesso condiviso.

4.6 Utilizzo di sistemi di trasferimento dati in cloud e di dispositivi di memorizzazione di massa esterni

Non è consentito l'uso di dispositivi di memorizzazione rimovibili, se non autorizzati dal proprio Responsabile U.O. e salvo il rispetto di quanto previsto dal presente paragrafo.

Per "Dispositivo di memorizzazione rimovibile" si intende qualunque dispositivo/supporto di memorizzazione asportabile. Ad esempio:

- disco fisso esterno;
- memoria USB;
- cd o dvd;
- Flash Card, Compact Flash, SD Card, Memory Stick, etc.

L'Azienda promuove l'utilizzo di sistemi di trasferimento di dati attraverso sistemi aziendali, quali la posta elettronica oppure i servizi cloud adottati dall'Azienda.

Qualora non sia possibile trasferire i dati con l'utilizzo dei detti sistemi, l'Azienda mette a disposizione i dispositivi di memorizzazione esterni crittografati, che vengono consegnati temporaneamente dalla U.O. ICT, attraverso la sottoscrizione di apposito verbale.

I dispositivi di memorizzazione esterna, se utilizzati sui PC aziendali, sono sottoposti a controlli di sicurezza informatici relativamente alla presenza di virus.

L'utilizzo dei dispositivi crittografati evita che, in caso di eventuale perdita o smarrimento dei medesimi, i dati e le informazioni ivi memorizzati siano accessibili da soggetti terzi, in conformità alle disposizioni e principi enucleati dal GDPR.

È vietato l'utilizzo di dispositivi di memorizzazione rimovibili esterni personali o comunque non autorizzati dalla Società.

E' fatto divieto utilizzare per il trasferimento di file aziendali, con particolare riferimento a quelli che contengono dati personali, servizi di cloud pubblici e sistemi di messaggistica non adottati ufficialmente dall'Azienda.

4.7 Applicativi

La Società ha cura di garantire che la sicurezza e la privacy siano elementi progettuali essenziali nel ciclo di vita degli applicativi.

Lo sviluppo/test di ogni nuovo software, o modifiche a moduli in uso, deve essere compiuto in ambienti diversi da quelli di produzione.

Il trasferimento di dati dall'ambiente di produzione all'ambiente di test deve essere effettuato dalla U.O. ICT. Qualora il trasferimento suddetto debba essere eseguito esclusivamente da personale della software house, la U.O. ICT deve autorizzarlo.

In casi eccezionali, per la soluzione di problemi in emergenza, agli sviluppatori possono essere fornite autorizzazioni di accesso in modifica a sistemi di produzione, per tempi limitati e sotto controllo diretto di personale della U.O. ICT o del personale della U.O. che ha richiesto l'intervento.

4.8 Posta Elettronica

L'abilitazione all'utilizzo della posta elettronica deve essere preceduta da regolare richiesta del Responsabile di U.O. al Responsabile U.O. ICT, che a sua volta richiederà l'autorizzazione a procedere alla Direzione.

La casella di posta elettronica, eventualmente assegnata dall'Azienda all'Utente (con un indirizzo che richiami il nome e cognome del dipendente, possibilmente del seguente tipo: nome.cognome@nomesocietà.it), è uno strumento di lavoro e deve essere utilizzata esclusivamente per le mansioni e funzioni assegnate per lo svolgimento dell'attività lavorativa. È espressamente vietato l'utilizzo dell'account di posta elettronica assegnato dalla Società per qualsivoglia altro fine che esula dallo svolgimento dell'attività lavorativa.

Per tutti i soggetti esterni alla Società, compresi i consulenti, qualora venga riconosciuta dalla Direzione l'assegnazione di una casella di posta elettronica, quest'ultima dovrà essere configurata con un indirizzo del seguente tipo: nome.cognome@esterni.nomesocietà.it.

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del loro corretto utilizzo.

Ogni Utente deve assicurare che il contenuto dei messaggi non sia diffamatorio, offensivo o pregiudizievole nei confronti della reputazione aziendale e personale. La Direzione può fornire, oltre alle caselle di posta sopra indicate, anche caselle di posta elettronica associate a gruppi di lavoro e/o unità operative.

La casella di posta elettronica deve essere mantenuta in ordine, cancellando periodicamente i messaggi contenenti soprattutto allegati ingombranti. Periodicamente, con cadenza almeno semestrale, ogni Utente deve provvedere a verificare lo stato della propria casella e ad eliminare i messaggi superati o vecchi.

Per quanto concerne la gestione dei documenti, si ricorda che quelli riguardanti l'attività lavorativa devono essere progressivamente archiviati e conservati all'interno dell'archivio di rete aziendale e le comunicazioni con soggetti esterni devono avvenire nel rispetto di quanto stabilito dalla procedura di gestione del protocollo. Le comunicazioni che contengono messaggi commerciali tali da impegnare giuridicamente la Società verso l'esterno devono essere preparate tramite il protocollo aziendale.

Gli allegati scambiati solo internamente tra il personale, nonché le stesse mail se necessario, vanno memorizzati secondo quanto stabilito dal par. 4.5 "Archivio file".

Ciascun Utente deve prestare la massima attenzione quando utilizza la posta elettronica.

In caso di e-mail sospette (per provenienza, contenuto, estensione o altro) occorre:

- evitare assolutamente di aprire allegati e/o link;
- ogni anomalia o problematica relativa a virus/malware ed antivirus dovrà essere prontamente segnalata all'U.O ICT.

Nel caso di messaggi provenienti da mittenti conosciuti ma che tuttavia contengono allegati sospetti (ad esempio file con estensione .exe .scr .pif .bat .cmd, etc.), questi non devono essere aperti e i messaggi devono essere cancellati.

È vietata la diffusione incontrollata di sistemi per propagare messaggi che inducono il destinatario a produrne molteplici copie da spedire, a propria volta, a nuovi destinatari. In tal senso sono espressamente vietati i messaggi a diffusione capillare e moltiplicata (c.d. "catene di Sant'Antonio").

Nel caso di invio di allegati pesanti è necessario utilizzare i formati compressi (ad esempio: .zip, .7z, .rar, etc.).

L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali.

4.9 Conservazione dei dati e delle comunicazioni scambiate con posta elettronica

Resta fermo che al database relativo all'account di posta elettronica può avere accesso solo l'intestatario dell'account stesso.

Il trattamento dei dati personali contenuti negli account di posta elettronica da parte della Società avviene nel rispetto dell'art. 4 della Legge n. 300/1970 (c.d. Statuto dei Lavoratori), delle disposizioni contenute nel GDPR e dei principi emanati dal Garante nelle "Linee guida per posta elettronica ed internet" (Provvedimento 1 marzo 2007, n. 13) e eventuali, successive modificazioni ed integrazioni.

L'Azienda richiede che le comunicazioni scambiate attraverso la posta elettronica siano selezionate periodicamente e siano via via cancellate, eliminando quelle superflue, al fine di evitare eccessivi appesantimenti del sistema di gestione della posta elettronica.

Il servizio di posta elettronica è soggetto a sistemi di logging per il corretto esercizio del servizio stesso, che consentono all'Azienda la conservazione dei soli dati esteriori del messaggio, c.d. "envelope del messaggio".

In caso di assenza programmata, ad esempio per ferie, il personale è tenuto ad inserire, tramite le funzionalità del servizio di posta elettronica, appositi messaggi di risposta contenenti le "coordinate" (elettroniche o telefoniche) della U.O. o di altro collega o del Responsabile per poter contattare l'Azienda.

In caso di assenza non programmata, ad esempio per malattia, qualora il lavoratore non possa attivare la procedura descritta, anche avvalendosi del servizio web mail, perdurando l'assenza per oltre 5 giorni, la Società si riserva la possibilità, laddove necessario mediante la U.O. ICT, di attivare l'analogo accorgimento sopra descritto per dare le coordinate della U.O. o di un altro soggetto di riferimento, quando possibile comunicandolo all'interessato. L'Amministratore di sistema effettuerà tale attività senza accedere ai contenuti della posta elettronica dell'interessato, nel rispetto della privacy di quest'ultimo. In caso, invece, di assenza improvvisa o prolungata del lavoratore e sempre che sussistano improrogabili necessità legate all'operatività aziendale, la Società potrà accedere all'account di posta elettronica assegnato al lavoratore alla presenza di un collega di fiducia, delegato a tal fine dal lavoratore stesso. In questi casi, il fiduciario – in conformità a quanto indicato nelle sopra citate Linee guida – provvederà ad accedere all'account di posta elettronica del lavoratore assente, verificando il contenuto dei messaggi e inoltrando eventuali comunicazioni la cui conoscenza sia necessaria per l'attività lavorativa, o ad assistere a tali operazioni che potranno essere svolte dalla U.O. ICT. A tal fine ciascun lavoratore può comunicare alla U.O. ICT il nominativo di un collega di fiducia; in difetto di tale comunicazione le operazioni di accesso all'account di posta elettronica saranno effettuate alla presenza del DPO o di soggetto da quest'ultimo delegato.

Dopo la cessazione del rapporto di lavoro/collaborazione, la Direzione, per mezzo della U.O. ICT, rimuove, previa disattivazione, gli account di posta elettronica di ex dipendenti e/o di ex collaboratori, secondo le modalità e le tempistiche di seguito specificate ed in conformità ai principi in materia di protezione dei dati personali sanciti dal Garante per la Protezione dei Dati Personali.

Contestualmente alla disattivazione dell'account, la U.O. ICT attiva una regola di posta elettronica volta ad informare i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'Azienda. Nello

specifico la U.O. ICT imposta una risposta automatica che viene trasmessa a tutti i messaggi che arrivano alla casella dell'account in fase di cessazione. La risposta automatica dirà "*l'account nome.cognome@nomesocietà.it è in fase di disattivazione, siete pregati di rivolgervi alla U.O. o colleghi della U.O. (indicazioni che deve fornire il responsabile di U.O. presso cui l'utente in cessazione prestava servizio) oppure a segreteria@nomesocietà.it/protocollo@nomesocietà.it*". Questa procedura rimane attiva per 30 giorni, al fine di consentire a terzi, che tentino di contattare l'account cessato, di essere reindirizzati alla U.O. di riferimento.
Fermo restando quanto sopra, alla data di cessazione del rapporto di lavoro, l'account viene sospeso, in modo che sin da subito l'utente non possa accedere alle risorse ICT, e viene rimosso, decorsi 30 giorni dalla cessazione del rapporto di lavoro, insieme a tutto il contenuto ad esso relativo (cartelle personali, messaggi di posta elettronica, altri dati eventuali). Il termine può essere prolungato a 60 giorni qualora la cessazione del rapporto di lavoro interessi soggetti in posizione apicale (quali, dirigenti, amministratori, responsabili di funzione).

In conformità ai provvedimenti del Garante ed ai principi in essi affermati, nonché alla normativa privacy, l'account del dipendente/collaboratore cessato potrà essere conservato sul server aziendale, previo parere dell'U.O. Affari Legali e del DPO nel caso in cui siano pendenti eventuali procedimenti giudiziari/ispezioni di Autorità/simili o specifiche e concrete situazioni precontenziose riguardanti la Società e/o il dipendente o collaboratore, ed anche al fine di poter eventualmente soddisfare richieste del lavoratore di accesso al contenuto dell'account di posta elettronica pervenute prima della cancellazione dello stesso.

4.10 Internet

L'accesso a Internet è garantito agli Utenti della Società al solo fine di accedere a informazioni e servizi inerenti all'attività lavorativa; di conseguenza, agli Utenti è fatto divieto di accedere ai siti di contenuto improprio o comunque estranei all'attività lavorativa stessa.

Al fine di controllare che la navigazione Internet avvenga verso siti utili all'attività lavorativa e per impedire l'accesso a quelli ritenuti pericolosi (siti di pedofilia, pornografia, terrorismo e altro), potranno essere utilizzati degli strumenti per selezionare e limitare gli accessi ad alcune tipologie di siti o impedire l'esecuzione o lo scaricamento di alcune tipologie di file. In caso il sistema di filtro blocchi erroneamente un sito o una risorsa online necessaria all'attività lavorativa, è possibile richiederne l'accesso tramite richiesta alla U.O. ICT.

Gli Utenti dovranno avere, inoltre, la massima cura nel segnalare possibili attività a carattere fraudolento o criminale.

È vietato l'uso di Internet tramite accesso aziendale per finalità che esulano dallo svolgimento delle proprie mansioni, con particolare riferimento alle attività di:

i. trading;
ii. downloading di file di notevole dimensione;
iii. utilizzo di applicativi per la condivisione e lo scambio di file multimediali (quali musica, immagini, video, etc.).
iv. streaming video e audio non inerente l'attività lavorativa (quindi sono permessi web call, conference, e corsi on-line, sono vietati web radio, spotify, etc.)

4.11 Documentazione dell'attività di navigazione

I sistemi informatici e le procedure software preposte al funzionamento del sistema di accesso a Internet producono, nel corso del loro normale esercizio, alcuni dati la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet (file di log). Si tratta di informazioni che per loro stessa natura permetterebbero, attraverso elaborazioni ed associazioni, di identificare gli utenti. In questa categoria di dati rientrano, ad esempio, gli indirizzi dei siti visitati, l'orario della visita, la tipologia di file visualizzato. Il trattamento di tali file di log è ispirato ai principi di pertinenza e non eccedenza e ne è prevista la conservazione per un massimo di 60 giorni. In presenza di gravi anomalie o problemi tecnici dovuti al comportamento degli utenti, si procederà alla loro conservazione per un periodo di tempo maggiore controllando, in prima battuta e quando possibile, i dati in forma aggregata, riferiti all'intera struttura lavorativa o a sue aree. Tale controllo si concluderà preferibilmente con l'applicazione di filtri o limitazioni per tutti o per gruppi omogenei di utenti, con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito generale ad attenersi scrupolosamente a compiti assegnati e alle istruzioni impartite. L'avviso potrà essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. Se a seguito di tali provvedimenti le gravi anomalie dovessero ripetersi, si procederà con controlli su base individuale.

4.12 Uso di Notebook e dispositivi mobili

L'assegnazione di portatili, è effettuato dalla U.O. ICT ed è autorizzato dalla Direzione.

L'Utente è responsabile dei dispositivi assegnati dall'Azienda e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

I dispositivi utilizzati all'esterno non devono essere mai lasciati incustoditi e sugli stessi devono essere conservati solo i file strettamente necessari; non appena sia consentito l'accesso alla rete aziendale tutti i file devono essere spostati in archivio, come previsto nel Par. 4.5 Archivio file.

È necessario collegarsi periodicamente e, in ogni caso, con cadenza settimanale alla rete interna per consentire l'aggiornamento dell'antivirus e di altri software di sistema.

La U.O. ICT provvederà a verificare periodicamente gli accessi alla rete dei dispositivi portatili e, in caso di mancato accesso per periodi superiori ad un mese, provvederà a contattare l'Utente per le azioni opportune.

La U.O. ICT si riserva, comunque, la facoltà di richiedere periodicamente la riconsegna dei dispositivi portatili per le opportune verifiche tecniche e gli aggiornamenti di sistema, fornendo all'Utente una postazione di lavoro alternativa.

L'uso di dispositivi propri è vietato per l'accesso ai sistemi aziendali ed il trattamento di dati personali, salvo casi espressamente autorizzati dalla Direzione e comunicati all'U.O. ICT. E' fatto divieto in ogni caso collegare dispositivi propri, quali per esempio personal computer portatili, alla rete aziendale presente nei locali delle Società, sia tramite cavo, sia in wifi, è consentito invece collegare tali dispositivi non di proprietà dell'azienda alla una rete wifi "ospiti" laddove presente.

4.13 Prestazione lavorativa svolta al di fuori delle sedi aziendali.

Se la prestazione lavorativa avviene al di fuori dei locali aziendali (ad esempio presso il domicilio del lavoratore in caso di telelavoro e anche in luoghi pubblici in caso di smartworking) il lavoratore, per

accedere al sistema di dati aziendale, dovrà seguire dettagliate istruzioni impartite dal Responsabile ITC e a controllare la presenza di una protezione antivirus aggiornata. Il lavoratore inoltre dovrà: 1.porre ogni cura per evitare che ai dati aziendali messi a sua disposizione possano accedere persone non autorizzate presenti nel suo luogo di prestazione fuori sede; 2.procedere a bloccare il PC in dotazione in caso di allontanamento dalla sua postazione di lavoro, anche per un intervallo limitato di tempo; 3.alla conclusione della prestazione lavorativa giornaliera, archiviare e conservare i documenti eventualmente stampati in cassetti/armadi o altri contenitori chiusi muniti di apposita serratura; 4.distruggere eventuali minute, documenti non necessari.

5. BACKUP

È prevista la pianificazione e la realizzazione di salvataggi centralizzati dei dati registrati in tutti gli ambienti informatici centrali.

I dati ed i sistemi sono soggetti almeno al backup giornaliero dei DB completi, Virtual Machine, File server, i backup giornalieri sono archiviati per almeno 7(sette) giorni;

6. ANTIVIRUS / ANTIMALWARE

I sistemi anti-malware sono centralizzati e la loro gestione è responsabilità della U.O. ICT.

L'aggiornamento dei sistemi antivirus e anti-malware sulle postazioni di lavoro (fisse e mobili) è garantito tramite collegamento alla rete aziendale e/o cloud.

L'Utente è tenuto a prestare attenzione, con gli strumenti messi a disposizione, alla presenza di virus/malware sulla propria postazione e su eventuali supporti magnetici provenienti da soggetti esterni e/o di proprietà delle Società del gruppo.

Non è consentito disabilitare gli strumenti antivirus/anti-malware.

In caso di anomalie o dubbi l'Utente è tenuto ad informare la U.O. ICT, che provvederà agli interventi del caso.

7. TELEFONIA MOBILE

7.1 Dotazioni standard

Le dotazioni standard di telefonia mobile sono le seguenti:

- Smartphone per gli Utenti che necessitano di accesso alle e-mail aziendali da dispositivo mobile e/o di installazione di APP.

La consegna delle dotazioni avviene su richiesta del responsabile della U.O. alla U.O. ICT, l'autorizzazione è concessa dalla Direzione, in funzione del ruolo e delle esigenze lavorative di volta in volta valutate.

I dispositivi per telefonia mobile sono assegnati direttamente all'Utente ed al momento della consegna è sottoscritto dalla U.O. ICT e dall'Utente stesso un apposito verbale.

I dispositivi assegnati devono essere dotati di sistema di autenticazione/accesso tramite credenziali, pin o altri sistemi di autenticazione previsti dai dispositivi che ne impedisca l'utilizzo da parte di soggetti non autorizzati. La password o il codice pin deve essere modificato dall'assegnatario con cadenza al massimo semestrale e non deve essere disattivato.

I dispositivi di telefonia mobile possono essere consegnati anche come dotazione condivisa su un automezzo e/o sede di lavoro; in tali casi la sottoscrizione del verbale è effettuata dal Responsabile della U.O./sede di lavoro.

7.2 Classi di abilitazione SIM

Le classi di abilitazione previste sono le seguenti:

- Classe D – abilitazione alle chiamate in Rete Aziendale Mobile (RAM) e ad un gruppo di numeri non in RAM predefiniti. Per default tutte le SIM sono in questa classe.
- Classe E – abilitazione a tutte le chiamate sul territorio nazionale, verso telefoni fissi e mobili. La Direzione valuta ed autorizza caso per caso l'attribuzione, anche temporanea, di tale classe alla SIM.
- Classe G – abilitazione al traffico da e per l'estero. Questa classe di abilitazione è concessa temporaneamente a seguito di specifiche necessità che la Direzione valuterà di volta in volta.

Si ricorda che il telefono cellulare aziendale è uno strumento di lavoro e quindi deve essere utilizzato con cura e diligenza. In caso di smarrimento/furto l'assegnatario dovrà provvedere far a bloccare la SIM e in caso di furto dovrà attivarsi per presentare la regolare denuncia alle forze dell'ordine (Polizia, Carabinieri). Anche i dispositivi mobili sono da ritenersi strumenti necessari allo svolgimento della prestazione lavorativa e pertanto i dati raccolti potranno essere utilizzati secondo quanto previsto dall'art. 4, co. 2 della legge 300/70 così come novellato dal D.Lgs. 151/2015.

8. STAMPANTI E FOTOCOPIATRICI

L'utilizzo dei suddetti strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati.

È richiesta una particolare attenzione quando si inviano su una stampante condivisa documenti aventi ad oggetto informazioni riservate; ciò al fine di evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di non lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampa.

9. GUASTI, MALFUNZIONAMENTI E SEGNALAZIONI

Ogni Utente deve provvedere a segnalare, con tempestività, eventuali guasti o malfunzionamenti della/e dotazione/i ICT assegnata/e alla U.O. ICT, che provvederà alle azioni opportune.

10. DATA BREACH

Ciascun utente o Amministratore di Retiambiente o del Gruppo che rileva una violazione dei dati personali (c.d. "Data breach"), anche solo potenziale, è tenuto a darne notizia, nel più breve tempo possibile e, comunque, entro tre ore da quando ne è venuto a conoscenza, alla Direzione, al DPO (Responsabile della Protezione Dati – dpo@retiambiente.it) e nel rispetto di quanto previsto dalla apposita proceduta aziendale.

11. CODICE DISCIPLINARE

Saranno oggetto di contestazione disciplinare ed eventuale conseguente sanzione, i seguenti comportamenti:

- Mancato rispetto delle prescrizioni previste dal presente Regolamento
- Utilizzo inappropriato di attrezzature e strumenti di lavoro. Al dipendente che per lo svolgimento della propria mansione viene dotato di strumenti quali postazioni informatiche fisse di lavoro o personal computer o telefoni o tablet etc. è fatto divieto di attivare software e/o programmi e/o applicazioni di qualunque tipo non autorizzati dall'Azienda o comunque non conformi a quelli indicati ed in uso dell'Azienda.
- Violazione della riservatezza dei dati aziendali. Al dipendente è fatto divieto di estrarre copia di documenti, per conto proprio o di terzi, per un utilizzo non riconducibile alla mansione svolta, ovvero portare al di fuori dell'Azienda documenti aziendali o copia di essi, di qualunque genere senza la dovuta autorizzazione, ovvero consultare senza la dovuta autorizzazione documenti e informazioni aziendali, anche su file elettronici, non inerenti la mansione svolta o di competenza di altre aree/uffici.

Ove la violazione costituisca reato o sia tenuta in danno di terzi o della società, possono essere avviate azioni civili o penali nei confronti del trasgressore.

12. DISPOSIZIONI FINALI

Gli strumenti informatici/tecnologici considerati nel presente Regolamento sono da considerarsi 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; conseguentemente le informazioni raccolte sulla base di quanto qui indicato, anche conformemente al successivo art. 13, possono essere utilizzate a tutti 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 e sui conseguenti sistemi di controllo, fermo restando il rispetto della normativa in materia di protezione dei dati personali.

13. CONTROLLI

La Società, preso atto del divieto di utilizzo di strumenti informatici/tecnologici per il controllo dell'attività lavorativa del dipendente, assicura che tutti i predetti strumenti saranno installati esclusivamente per esigenze organizzative / produttive e per tutte le finalità previste dal rapporto di lavoro. Ferme restando le modalità di controllo specificate negli articoli precedenti, in caso di anomalie il personale incaricato dell'U.O. ICT, nel rispetto della normativa sulla protezione dei dati personali, potrà effettuare controlli su tutti gli strumenti informatici/tecnologici forniti dalla Società e sui documenti ivi contenuti. In particolare, potranno essere effettuati controlli per le seguenti finalità:

- tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati aziendali;
- evitare la commissione di illeciti;
- compiere attività di carattere difensivo e/o preventivo;
- svolgere controlli e programmazione dei costi aziendali;

- verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche mediante audit e vulnerability assesment del sistema informatico. Per tali controlli la Società si riserva di avvalersi di soggetti esterni.

Il personale incaricato effettuerà, in prima battuta, controlli anonimi che si concluderanno con avvisi generalizzati diretti agli incaricati dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite. Controlli su base individuale potranno essere computi solo in caso di successive ulteriori anomalie.

In presenza di seri indizi, il personale incaricato potrà anche effettuare controlli rivolti ad accertare condotte illecite del singolo lavoratore (c.d. controllo difensivo del datore di lavoro), anche mediante verifica dei file log presenti sulle risorse di rete o sui singoli dispositivi in uso all'utente.

I dati personali raccolti dalla Società nell'ambito delle attività descritte non saranno oggetto di diffusione e potranno essere conosciuti da personale autorizzato o da soggetti legati alla Società da stretti vincoli contrattuali che garantiscono la riservatezza e l'integrità delle informazioni trattate. Tutti i dipendenti e/o collaboratori sono titolari dei diritti previsti dal capo III del Regolamento UE 679/2016, che possono essere esercitati con richiesta rivolta alla Società.

14. ENTRATA IN VIGORE

Il presente Regolamento entra in vigore il giorno successivo alla sua approvazione da parte dell'organo amministrativo di Retiambiente ed è portato a conoscenza degli utenti tramite pubblicazione in area condivisa.