Procedura per l'utilizzo dei sistemi e strumenti informatici di Anselmi & C. Srl

Indice

Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet da Personal Computer, tablet e smartphone, espone *Anselmi & C. Srl* e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e disciplina sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa.

Peraltro, anche lo sviluppo delle reti sociali on-line incide, direttamente o indirettamente, sulle attività dell'Azienda, sulla sua immagine e sulle relazioni commerciali instaurate. Infatti, l'uso dei *social media*, quali Facebook™, Twitter™, Linkedin™, Instagram™, ecc., dei blog e dei forum, anche professionali, costituisce un efficace strumento di condivisione di contenuti (testi, immagini, video) da parte degli utenti e, allo stesso tempo, un'evidente opportunità per l'Azienda, in particolare in ambito commerciale e di marketing. Risulta però necessario che, al fine di evitare il sorgere di rischi derivanti dalla presenza della denominazione dell'Azienda e/o di altri riferimenti ad essa riconducibili, eventualmente solo indiretta, sui *social media*, si tenga pure conto di questo preciso aspetto nella presente Procedura.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, *Anselmi & C. Srl* ha adottato una Procedura interna diretta ad evitare che comportamenti anche inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e quindi del proprio sistema informatico. La Procedura svolge anche la funzione di informare compiutamente gli utenti sugli specifici trattamenti dei loro dati personali che vengono effettuati, e delle modalità adottate.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati o persone autorizzate al trattamento, in attuazione del Regolamento UE 2016/679 (di seguito il "GDPR") contenenti anche le misure di sicurezza, nonché integrano le informazioni già fornite agli interessati ai sensi dell'art. 13 del GDPR, anche in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse, come previsto dall'art. 4, 3°comma dello Statuto dei lavoratori.

Considerato inoltre che *Anselmi & C. Srl*, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo messo a disposizione dei propri collaboratori che ne necessitino per il tipo di funzioni svolte, telefoni, telefoni cellulari, computer portatili, tablet e smartphone, ecc., sono state inserite nella Procedura alcune clausole relative alle modalità ed ai doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

1. Entrata in vigore della Procedura e pubblicità

1.1 La nuova Procedura entrerà in vigore il 25/03/2024. Con l'entrata in vigore della presente Procedura tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate, qualora incompatibili o difformi, poiché sostituite dalle presenti.

1.2 Copia della Procedura, oltre ad essere affissa nella bacheca aziendale anche per quanto prevede l'art.7 della Legge n. 300/1970, verrà consegnata via mail o via whats up a ciascun dipendente, anche ai fini dell'art. 13 del GDPR e dell'art.4, comma 3°, dello Statuto dei lavoratori, oltre che a collaboratori, consulenti, agenti od altri incaricati esterni (es. incaricati software house, incaricati dei professionisti di cui si avvale l'Azienda, etc.) che venissero autorizzati a far uso di strumenti tecnologici dell'Azienda o ad accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati.[1] Pertanto, la presente Procedura entra a far parte, per quanto occorra, del Regolamento aziendale.

[1] L'informativa agli interessati sui trattamenti effettuati rappresenta un obbligo fondamentale inderogabile in base al Regolamento UE 2016/679 (art .13) ed è necessaria per l'utilizzo anche a fini disciplinari nel rapporto di lavoro, in base all'art. 4, 3°comma dello Statuto dei lavoratori.
La consegna di una copia a ciascun collaboratore è una scelta facoltativa del datore di lavoro: in caso di consegna a mano, la premessa della presente Procedura può anche essere riportata in un'eventuale lettera di accompagnamento. Si ricorda infatti che ai sensi dell'art. 7 Legge n. 300/1970 l'unico obbligo a carico del datore di lavoro, **ai fini dell'esercizio del potere disciplinare**, è quello di dare adeguata pubblicità delle norme mediante l'affissione in luogo accessibile a tutti: per poter agire disciplinarmente nei confronti del **dipendente**, la Procedura dovrà pertanto essere affissa in luogo accessibile a tutti.

2. Campo di applicazione della Procedura

2.1 La nuova Procedura si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori e consulenti dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori coordinati e continuativi, in stage, agenti di commercio, prestatori d'opera intellettuale, etc.) che venissero autorizzati a far uso di strumenti tecnologici dell'Azienda o perfino di accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati. Pertanto, le regole di seguito previste devono intendersi a carico tanto dei primi quanto dei secondi, ferma restando la necessità che si dia opportuno conto della presente Procedura nel contratto concluso con quest'ultimi. Le disposizioni della presente Procedura si applicano anche ai lavoratori che eseguono la prestazione lavorativa, parzialmente od esclusivamente, a tempo determinato od indeterminato, in modalità di "lavoro agile", a norma degli articoli da 18 a 23 del D.lgs. n. 231/2017, eventualmente integrate da ulteriori prescrizioni fornite allo stesso lavoratore in occasione dell'avvio dello "smart working".

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve così intendersi ogni dipendente, collaboratore e/o consulente (come sopra già precisato) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "responsabile del trattamento" o "incaricato o persona autorizzata al trattamento", ai fini del Regolamento generale n. 679/2016, in ragione delle attività e degli impegni che si assume nell'organizzazione aziendale od a favore dell'Azienda stessa.

3. Utilizzo del Personal Computer

3.1 **Il Personal Computer affidato all'utente è uno strumento di lavoro**. Il personal computer deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento.

3.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete di *Anselmi & C. Srl* solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto 4 della presente Procedura.

3.3 Anselmi & C. Srl rende noto che il personale incaricato che opera presso il servizio Information and Comunication Technology[2] (nel seguito per brevità "servizio ICT") della stessa Anselmi & C. Srl è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.). La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata o impedimento dell'utente. Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC, il servizio ICT ne darà comunicazione agli utenti interessati, preventivamente ovvero, nel caso di urgenza dell'intervento stesso, successivamente ad esso.

3.4 Il personale incaricato del servizio ICT ha la facoltà di collegarsi e visualizzare in remoto i contenuti delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità**,** a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

3.5 **Non è consentito** l'uso di programmi diversi da quelli ufficialmente installati dal personale del servizio ICT per conto della *Anselmi & C. Srl* né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la stessa *Anselmi & C. Srl* a

---

Si rammenta però che il potere disciplinare non può comunque essere esercitato nei confronti dei collaboratori e dei tirocinanti od altri consulenti o lavoratori autonomi che potrebbero venir autorizzati all'utilizzo di strumenti tecnologici aziendali, se non perfino ad accedere alla rete informatica aziendale, mentre nei confronti dei lavoratori somministrati (ex interinali) va esercitato per il tramite dell'agenzia di somministrazione.

[2] O altra figura aziendale preposta alla gestione del sistema informatico aziendale, quale l'"amministratore di sistema" delineato dal provvedimento del Garante privacy del 27.11.2008, indipendentemente da una sua nomina a Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679. Nel caso la gestione del sistema ICT (o di alcune fasi di esso) siano affidate a terzi, questi dovrà essere individuato quale "responsabile del trattamento" e, di conseguenza, dovranno essere adottate idonee clausole contrattuali volte a formalizzare l'attribuzione delle relative responsabilità ed obblighi, conformemente a quanto indicato nel citato art. 28.

gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico della *Anselmi & C. Srl)*, come disposta dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie ed interdittive.

3.6 Salvo preventiva espressa autorizzazione del personale del servizio ICT, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem).

3.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del servizio ICT nel caso in cui siano rilevati virus e adottando quanto previsto dal successivo punto 10 della presente Procedura relativo alle procedure di protezione antivirus.

3.8 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.[3]

4. Gestione e assegnazione delle credenziali di autenticazione

4.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del servizio ICT, previa espressa indicazione della Direzione aziendale ovvero previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal servizio ICT, associato ad una parola chiave (password) riservata che dovrà venir **custodita dall'incaricato con la massima diligenza e non divulgata**. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del servizio ICT.

4.3 La parola chiave sarà formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno 8 caratteri.

4.4 È definito che il servizio ICT procederà all'impostazione della parola chiave, al primo utilizzo e, successivamente, alla modifica per un numero di utenti programmato, almeno ogni 6 mesi. La nuova password sarà comunicata dal servizio ICT all'utente.

4.5 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso a cura del personale del servizio ICT.

4.6 Soggetto preposto alla custodia delle credenziali di autenticazione è il personale incaricato del servizio ICT di *Anselmi & C. Srl.*

5. Utilizzo della rete di *Anselmi & C. Srl*

5.1 Per l'accesso alla rete di *Anselmi & C. Srl* ciascun utente deve utilizzare la propria credenziale di autenticazione. Lì dove sia possibile accedere alla rete aziendale da remoto, con accesso anche ai dati attinenti all'attività dell'utente presenti nel server ed alla sua casella posta elettronica, questo potrà avvenire solo a seguito di autorizzata installazione e configurazione nel proprio pc portatile (personale od in dotazione) di apposita VPN aziendale e

[3] Una modalità automatica che evita di lasciare incustodito il pc, anche in caso di mancato spegnimento da parte dell'utente è quello di adottare il savescreen a tempo con obbligo di reintrodurre la password per l'accesso.

mediante la propria credenziale di autenticazione (od altra credenziale assegnata dal personale del servizio ICT), o mediante sistemi di connessione che garantiscano un livello idoneo di sicurezza.[4]

5.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

5.3 Le cartelle utenti presenti nei server di *Anselmi & C. Srl* 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. Su queste unità vengono svolte regolari attività di manutenzione, amministrazione e back up da parte del personale del servizio ICT.

5.4 Il personale del servizio ICT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.

5.5 Risulta opportuno che, con regolare periodicità (almeno ogni sei mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

5.6 Nella gestione dei sistemi informatici aziendali, il servizio ICT potrà acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali, ad esempio, le 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, ai sensi del successivo punto 12.2, per tutti i fini connessi al rapporto di lavoro, sempre nell'ambito delle finalità individuate nel precedente punto 3.3., e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.[5]

5.7. L'utente è infine tenuto a far uso degli applicativi riferibili alle piattaforme di comunicazione e condivisione di documenti appositamente installate dal servizio ICT. In tal senso, non potrà avvalersi, anche nelle comunicazioni con i terzi esterni all'Azienda, di piattaforme terze non preventivamente valutate, anche sotto il profilo della sicurezza, dal servizio ICT (servizi cloud di file sharing).

6. Utilizzo di altri dispositivi elettronici[6]

6.1 **Tutti i dispositivi elettronici dati in dotazione al personale di Anselmi & C. Srl devono considerarsi strumenti di lavoro:** ne viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative, non essendo quindi consentiti utilizzi a carattere personale o comunque non strettamente inerenti le attività lavorative. Fra i dispositivi

[4] In base al principio di "responsabilizzazione" che impone anche l'adozione di idonee misure di sicurezza (art. 5,1°paragrafo, lettera f, 2° paragrafo, e art. 32 del GDPR) viene consigliata l'adozione di una connessione tramite VPN aziendale. In ogni caso il sistema di connessione adottato deve garantire un livello adeguato alla natura dei dati trattati ed al livello di rischio.

[5] L'impresa ha l'obbligo di informare, ai sensi del Regolamento UE 2016/679 (art.13), circa l'utilizzo di tutti i dati, riconducibili agli utenti, acquisiti tramite il sistema informatico, anche di quelli rilevati automaticamente. Inoltre, ai sensi dell'art. 4, 3°comma dello Statuto dei lavoratori (Legge n. 300/1970), se si vogliono utilizzare per tutti i fini connessi al rapporto di lavoro gli stessi dati acquisiti, è necessario informare sulle modalità d'uso degli strumenti e di effettuazione dei controlli. Ciò detto, l'impresa dovrà valutare quali specifici strumenti, insiti nei propri sistemi informatici, esistano nella propria realtà aziendale e dai quali possano derivare trattamenti di dati; la clausola, in questo senso, vuole costituire semplicemente un esempio da utilizzare nel proprio Regolamento aziendale, fermo restando che solo l'effettiva valutazione di cui sopra potrà permettere di redigere una clausola più corretta e completa, ovvero di implementare quella qui proposta e adempiere così agli obblighi dettati dal Regolamento generale e dallo Statuto dei lavoratori. In ogni caso, quindi, va data piena informativa sui trattamenti dei dati personali effettuati mediante il software e gli applicativi presenti nella rete aziendale.
Inoltre, qualora vi sia la possibilità che, tramite il software esistente, sorga la possibilità di un controllo a distanza, si dovrà procedere, ai sensi del 1° comma dell'art. 4 dello Statuto, al preventivo accordo sindacale o, in assenza, all'ottenimento della autorizzazione dell'Ispettorato Territoriale del Lavoro

[6] La Procedura può anche essere utilizzata per informare circa l'utilizzo di altri strumenti di lavoro assegnati ai dipendenti o di sistemi presenti in azienda. Il sistema di gestione di questi dispositivi mobili aziendali (**M**obile **D**evice **M**anagement - MDM) deve garantire che la possibilità di localizzare a distanza i dispositivi non configuri un monitoraggio continuo dei dipendenti (vedi punto 5.4.3 del parere n. 2/2017 del WP29). Ancor di più, qualora si gestisca un sistema BYOD (**B**ring **Y**our **O**wn **D**evice), ove andrà rigorosamente tenuta separata e non accessibile la parte privata, al fine di evitare un monitoraggio della vita privata del dipendente (vedi punto 5.4.2 del parere 2/2017 del WP 29).

in questione vanno annoverati i telefoni aziendali, PC portatili, tablet, telefoni cellulari, smartphone, etc., indipendentemente dal fatto che l'utente abbia o meno la possibilità di accedere alla rete di Anselmi & C. Srl o di condividere documenti, dati e materiali ivi conservati e/o trattati.

6.2 L'utente resta responsabile del singolo dispositivo assegnato e deve custodirlo con diligenza sia durante trasferte e spostamenti sia durante l'utilizzo nel luogo di lavoro; va sempre adottata ogni cautela per evitare danni o sottrazioni.[7] Inoltre, non può comunque avvenire alla guida di autovettura, se non, per quest'ultimo caso, in conformità alle prescrizioni disposte al riguardo dal Codice della strada - ovvero, conformemente all'art.173 del Codice della strada, con l'uso di apparecchi a viva voce o dotati di auricolare purché il conducente abbia adeguate capacità uditive ad entrambe le orecchie (che non richiedono per il loro funzionamento l'uso delle mani) -, assumendosene di conseguenza l'utente tutte le responsabilità ed i rischi per un uso non conforme.

6.3 Con riferimento ai telefoni aziendali e telefoni cellulari, fermo restando quanto sopra già disposto circa il loro uso e custodia, la ricezione o l'effettuazione di telefonate personali, così come l'invio o la ricezione di SMS, MMS, whatsapp di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, viene consentita solo nel caso di uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal personale del servizio ICT. L'Azienda si riserva il diritto di verificare le fatturazioni concernenti le chiamate in uscita compiute dal dipendente, oltre alle sole in entrata in roaming se dovessero comportare un costo per l'Azienda stessa, ai soli fini di riduzione dei costi aziendali e di verifica dell'adeguatezza del contratto sottoscritto con il fornitore dei servizi telefonici. La conservazione dei dati relativi al traffico telefonico verrà conservata per sei mesi; l'Azienda procederà infine, per quanto possibile, all'anonimizzazione dei dati in questione[8].]

6.4 Si precisa, peraltro, che le disposizioni previste nella presente Procedura ai punti 3, 7, 8, 9, 10 e 11 della stessa trovano applicazione anche nell'uso dei dispositivi elettronici qui considerati.

6.5 Ferma restando la gestione della specifica sicurezza informatica, posta in capo al personale del Servizio ICT, ogni utente del sistema di stampanti in rete deve adottare comportamenti atti a proteggere il know-how aziendale a la riservatezza dei dati personali. Si deve, quindi, evitare di lasciare abbandonate le stampe presso la stampante, stampe che devono essere ritirate tempestivamente. In caso di scannerizzazione di documenti cartacei, l'invio all'esterno tramite la stessa stampante in rete deve essere motivato da esigenze lavorative e, nel caso di contenuti riservati (contraddistinti dalla dicitura "strettamente riservati" o analoghe apposte sul documento) deve essere autorizzato dal responsabile di ufficio.

7. Utilizzo e conservazione dei supporti rimovibili

7.1 Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

7.2 L'utente resta, in ogni caso responsabile della custodia dei supporti e dei dati aziendali in essi contenuti; in particolare, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

7.3 Viene vietato l'utilizzo di supporti rimovibili personali se non previamente concordato.

[7] Si raccomanda, anche ai fini di evitare casi di "data breach" e conseguente obbligo di notifica al Garante, di procedere ad implementare sistemi di crittografia dei dati personali memorizzati nei dispositivi aziendali (tablet, smartphone, …).

[8] Il legittimo interesse datoriale posto a base di questo eventuale trattamento di dati personali al fine del controllo e riduzione dei costi di servizio, è imperniato, quale base giuridica di liceità, sulle esigenze organizzative e di tutela del patrimonio aziendale. Secondo il Garante - vedi provvedimento 11 gennaio 2018 - il "bilanciamento di interessi" è raggiunto anche in forza dell'accordo sindacale stipulato ex art. 4, 1° comma Statuto dei lavoratori, per il potenziale controllo a distanza che potrebbe derivare dai dati personali trattati. Secondo i principi generali (art. 5 del Regolamento UE 2016/679) il trattamento deve essere strettamente necessario in relazione alla finalità lecita individuata: un servizio basato su tariffe "flat" potrebbe non giustificare il controllo incrociato sui nominativi dei singoli dipendenti. Per un'analisi complessiva di un sistema di gestione e controllo della fatturazione delle sim aziendali, si rinvia al citato provvedimento del 11 gennaio 2018.

7.4 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del servizio ICT e seguire le istruzioni da questo impartite. Nel caso di dispositivi elettronici, con riferimento in particolare a PC portatili, tablet ed altri dispositivi sui quali possano venir salvati documenti, dati ed altro materiale, dovrà farsi particolare attenzione al salvataggio in opportuni supporti esterni di tale materiale oppure alla sua rimozione effettiva prima della riconsegna del dispositivo, concordata comunque ogni opportuna azione al riguardo con il personale del servizio ICT[9].

8. Uso della posta elettronica

8.1 **La casella di posta elettronica assegnata all'utente è uno strumento di lavoro.** Le archiviazioni dei messaggi avvengono su server in disponibilità dell'Azienda. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2 È fatto divieto di utilizzare le caselle di posta elettronica ***nome.cognome@nomeazienda.it*** [10] per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:
- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o c.d. "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si dovrebbe comunicarlo immediatamente al personale del servizio ICT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.3 Poiché la casella di posta assegnata costituisce strumento di lavoro, è opportuno evidenziare che solo i messaggi di corrispondenza commerciale, verranno conservati nei server in disponibilità dell'Azienda stessa per 10 anni, a norma dell'art. 2220 del Codice civile. I messaggi privi di valenza commerciale o lavorativa, di conseguenza, dovranno essere selezionati e periodicamente cancellati a cura ed onere dell'utente della casella.

8.4 In ogni caso, la casella di posta deve essere mantenuta in ordine, cancellando documenti inutili (anche allegati ingombranti.[11]), o non costituenti corrispondenza commerciale e lavorativa che, come tale, deve essere sottoposta al sistema di gestione documentale aziendale come disposto al precedente punto 8.3 In caso di cessazione del rapporto di lavoro, il singolo dipendente è tenuto ad eliminare dalle proprie cartelle tutti i messaggi di posta elettronica ed i documenti non pertinenti l'attività aziendale e non utili alle esigenze aziendali, mantenendo integra, invece, tutta la corrispondenza e documentazione inerente all'attività lavorativa. Resta inteso che, di conseguenza, la documentazione presente nel profilo del singolo utente che cessa il rapporto di lavoro verrà considerata presuntivamente dall'azienda quale corrispondenza e documentazione lavorativa e non personale. Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per *Anselmi & C. S.r.l.* ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Responsabile d'ufficio.

8.5 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

8.6 È obbligatorio porre la massima attenzione nell'aprire i file attachment di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

8.7 Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate o esigenze professionali specifiche, quali ad esempio la condivisione di attività relative a clienti\fornitori da parte di più utenti, invierà automaticamente messaggi di risposta contenenti le coordinate di posta elettronica di un altro soggetto o

[9] Per le cautele e modalità per la dismissione o smaltimento di apparecchi elettronici, si veda il provvedimento del Garante privacy del 13.10.2008.
[10] Ovvero potrà essere realizzato un sistema di indirizzi di posta elettronica condivisi tra più utenti (ad es. *ufficiovendite@nomeazienda.it*, *ufficioreclami@nomeazienda.it* al posto di un sistema basato sull'identità personale).
[11] Sarebbe opportuno introdurre un limite massimo della dimensione del database di posta: ad es. 200 MB.

altre utili modalità di contatto della struttura. In tal caso, la funzionalità può essere attivata e disattivata dall'utente e dal servizio ICT.

8.8 In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni - verrà attivata a cura del servizio ICT.

8.9 Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dall'azienda, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui al punto 8.7; assenza non programmata di cui al punto 8.8), per le sole esigenze organizzative di lavoro dell'Azienda.

8.10 Il personale del servizio ICT, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 3.3. [12]

8.11 Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato della Anselmi & C. Srl potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella policy aziendale.

8.12 Anselmi & C. Srl si riserva la facoltà, a proprio insindacabile giudizio, di assegnare o ritirare l'utilizzo della casella di posta elettronica in base alla propria esclusiva e insindacabile valutazione della necessità di utilizzo della stessa per lo svolgimento delle attività lavorative. Di ogni eventuale disattivazione o sospensione della casella di posta elettronica assegnata verrà data informativa al singolo interessato.

8.13 Al momento della conclusione/sospensione del rapporto di lavoro:

- verrà in automatico generata una mail ai mittenti di mancato inoltro e con indicazione della diversa casella di posta elettronica aziendale cui trasmettere i messaggi da recapitare;

- viene escluso, comunque, l'invio di messaggi da tale casella di posta.

8.14 Nel caso in cui venisse assegnato all'utente anche la gestione di uno o più indirizzi di posta elettronica certificata di cui l'Azienda si fosse dotata, tale utente dovrà attenersi alle regole previste nell'ulteriore apposita Procedura aziendale a ciò dedicato e che va comunque a completare ed integrare la presente Procedura.[13]

8.15 Nel caso di invio di messaggi rivolti a più persone, al fine di garantire la riservatezza dei singoli destinatari, l'elenco degli indirizzi non dovrà comparire in chiaro né tra i destinatari, né in copia (C.C.), ma solo in copia nascosta o riservata (C.C.N. o C.C.R.), in modo che ogni destinatario non venga a conoscenza degli altri indirizzi. Naturalmente, qualora l'invio condiviso sia, invece, lecito in forza di una specifica base giuridica di trattamento, l'elenco dei destinatari potrà essere riportato in chiaro tra i destinatari o in copia.

[12] L'accesso ai contenuti della corrispondenza nella casella di posta elettronica avviene esclusivamente in caso di assenza prolungata o impedimento dell'utente che rendono indispensabile ed indifferibile per esclusive finalità di operatività e sicurezza del sistema, informando successivamente lo stesso utente.
[13] Quest'ultima previsione potrà essere mantenuta solo se effettivamente è stato adottato un apposito protocollo di gestione e presidio del "domicilio digitale" aziendale, ed in genere delle caselle PEC attivate dall'azienda.

9. Navigazione in Internet

9.1 **Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa**.

9.2 In questo senso, a titolo puramente esemplificativo, **l'utente non dovrà utilizzare internet** per:
- l'upload o il download di software anche gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del servizio ICT);
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione Generale (o eventualmente dal Responsabile d'ufficio e/o del servizio ICT) e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa
- la partecipazione a Forum non professionali, l'iscrizione con account aziendale e la partecipazione personale a social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio
- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.[14]

9.3 Gli eventuali controlli, compiuti dal personale incaricato del servizio ICT ai sensi del precedente punto 3.3, 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 ed i file stessi vengono conservati non oltre sei mesi[15], ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Azienda.

9.5 L'utilizzo di tutte le reti WiFi presenti in Azienda è limitato agli utenti autorizzati. A tale scopo si precisa che l'utilizzo di qualsiasi rete WiFi disponibile in Azienda e dalla stessa configurata è possibile solo a seguito di digitazione di specifiche credenziali che vengono assegnate dal responsabile/servizio ICT.

9.6 L'accesso da remoto alla rete aziendale è possibile agli utenti abilitati solo a seguito di comunicazione di specifiche credenziali o dell'installazione di software che lo abilita sui dispositivi in uso.

9.7 L'accesso da remoto alla rete aziendale è possibile solo utilizzando i dispositivi previsti. A tale scopo vengono svolti controlli automatici che impediscono l'accesso utilizzando dispositivi non abilitati.

10. Protezione antivirus

10.1 Il sistema informatico di *Anselmi & C. S.r.l.* è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

10.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del servizio ICT.

10.3 Ogni dispositivo magnetico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del servizio ICT.

[14] Ovvero, in alternativa, se viene prevista dall'azienda la possibilità di accedere a caselle webmail di posta elettronica personale al di fuori dell'orario di lavoro si potrà dire: "- accesso, tramite internet, a caselle webmail di posta elettronica personale durante l'orario di lavoro, venendo pertanto consentito all'utente di accedervi nelle ore extralavorative. Nel qual caso, l'utente dovrà comunque porre la massima attenzione nell'aprire i file attachments di posta elettronica prima del loro utilizzo.".

[15] Deve essere definita una durata massima di conservazione che, in base al principio di pertinenza temporale del trattamento (art. 5, 1° paragrafo, lettera e) del Regolamento UE 2016/679) sia effettivamente congrua e giustificabile alla luce delle esigenze tecniche di gestione del sistema informatico.

11. Partecipazioni a social media

11.1 L'utilizzo a fini promozionali e commerciali dei social media – quali Facebook™, Twitter™, Linkedin™, Instagram™, dei blog e dei forum, anche professionali – verrà gestito ed organizzato esclusivamente dall'Azienda attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti (conformemente a quanto disposto al precedente punto 9.2).

11.2 Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, l'Azienda ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio aziendale, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che viene vietata la partecipazione agli stessi social media durante l'orario di lavoro. La policy qui dettata deve venir seguita dagli utenti sia che utilizzino dispositivi messi a disposizione dall'Azienda, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti della stessa Azienda.

11.3 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni aziendali considerate dall'Azienda riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni finanziarie ed economiche, commerciali, sui piani industriali, sui clienti, sui fornitori ed altri partners dell'Azienda stessa. Inoltre, 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 dell'Azienda; l'utente, nelle proprie comunicazioni, non potrà quindi inserire marchi od altri segni distintivi dell'Azienda, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione Generale dell'Azienda.

11.4 L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori aziendali, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con il preventivo consenso del Responsabile d'ufficio.

11.5 L'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso l'Azienda, i colleghi, i clienti ed i fornitori, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito aziendale.

11.6 Infine, in via generale ed ove non autorizzato in senso diverso dal proprio Responsabile d'ufficio, l'utente, nell'uso dei social network, esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Azienda, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Azienda.

12. Osservanza delle disposizioni in materia di Privacy

12.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato o persona autorizzata al trattamento dei dati ai sensi del Regolamento generale UE 2016/679.

12.2 Gli strumenti tecnologici considerati nella presente Procedura costituiscono tutti 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[16]; conseguentemente, le informazioni raccolte sulla base di quanto indicato nella Procedura, anche conformemente al successivo punto 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 che potessero venir eventualmente compiuti (conformemente al successivo punto 14), fermo restando il rispetto della normativa in materia di protezione dei dati personali.

12.3 Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori; peraltro, lì dove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio aziendale, Anselmi & C. Srl provvederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n.300/1970, dandone anche opportuna informazione agli utenti stessi.[17]

13. Accesso ai dati trattati dall'utente

13.1 Oltre che per motivi di sicurezza del sistema informatico, compresi i motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.), per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione aziendale, tramite il personale del servizio ICT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy e delle procedure di cui ai precedenti 3.3. e 3.4 e 8.5 a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

14. Incidenti e Data Breach

14.1 Oltre a quanto previso al punto 10 circa i virus rilevati, ogni malfunzionamento o anomalia del sistema informatico e dei dispositivi assegnati deve essere tempestivamente segnalato al servizio ICT per gli eventuali interventi tecnici e di protezione del sistema.

14.2 In caso di incidenti che possono determinare una violazione di dati personali ("Data Breach"), l'utente dovrà immediatamente comunicare la possibile violazione al servizio ICT, al fine di permettere a Anselmi & C. Srl di attivare la procedura aziendale di verifica degli eventi e di adempiere, se del caso, agli obblighi di notifica e di comunicazione previsti dagli articoli 33 e 34 del Regolamento UE 2016/679 a carico del titolare del trattamento. Si tenga a mente che per "Data Breach" ai sensi del GDPR si intende qualsiasi violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso abusivo (cioè non autorizzato) ai dati personali gestiti dall'Azienda, siano essi archiviati, trasmessi o comunque in altro modo trattati.

15. Sistemi di controlli graduali

15.1 In caso di anomalie, il personale incaricato del servizio ICT effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti 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 e alle istruzioni impartite. Controlli su base più ristretta o anche individuale potranno essere computi solo in caso di successive ulteriori anomalie.

[16] Per quanto già detto, se, invece, in base agli applicativi, ai software e, quindi alle finalità definite, tali strumenti possono determinare un controllo a distanza, sarà necessario esperire il regolamento sindacale od autorizzativa del 1° comma dell'art. 4.

[17] Vedi nota precedente. Qualora si configuri un uso di strumenti aziendali che non può rientrare nelle ipotesi del comma 2° dell'art. 4 dello Statuto, la società dovrà applicare il regolamento di accordo sindacale o autorizzazione preventive previste dal 1° comma dell'art. 4.

15.2 In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

16. Sanzioni

16.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con la presente Procedura. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL metalmeccanico, e nei confronti dei collaboratori, consulenti, agenti ed incaricati esterni di cui all'1.2, verificata la gravità della violazione contestata, con la risoluzione od il recesso dal contratto ad essi relativo nonché con tutte le azioni civili e penali consentite.[18]

17. Aggiornamento e revisione

17.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate alla presente Procedura. Le proposte verranno esaminate dalla Direzione Generale.

17.2 La presente Procedura è soggetto periodicamente a revisione.

Data **La Direzione**

25/03/2024

[18] Si rammenta che il potere disciplinare non può comunque essere esercitato nei confronti dei collaboratori coordinati e continuativi, dei tirocinanti, degli agenti e dei consulenti in genere esterni di cui l'azienda si avvalesse, mentre nei confronti dei lavoratori somministrati va esercitato per il tramite dell'agenzia di somministrazione. Con riferimento ai collaboratori, ai consulenti esterni, agli agenti, qualora questi per l'espletamento del loro incarico si servissero degli strumenti aziendali considerati dalla Procedura, si propone di prevedere nell'ambito del contratto ad essi relativo l'obbligo di rispettare la Procedura in questione, con diritto della committente, nei casi di violazione di particolare gravità, di risolvere il contratto stesso.