REGOLAMENTO AZIENDALE

PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

Approvato dal Consiglio di Amministrazione in data 24.01.2018

Sommario

Premessa

Il presente Regolamento intende fornire ai dipendenti e collaboratori, denominati anche incaricati o utenti, di A & T 2000 S.p.A. le indicazioni per una corretta e adeguata gestione delle informazioni aziendali, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici della Società.
Ogni dipendente e collaboratore è tenuto a rispettare il Regolamento, che è reso disponibile secondo quanto previsto al successivo punto 1.3.
Si specifica che tutti gli strumenti utilizzati dal lavoratore (hardware, software, risorse, e-mail ecc.) sono messi a disposizione dalla Società per rendere la prestazione lavorativa. Gli Strumenti, nonché le relative reti della Società a cui è possibile accedere tramite gli Strumenti, sono domicilio informatico di A & T 2000 S.p.A..
I dati personali e le altre informazioni dell'Utente che sono registrati negli Strumenti o che si possono eventualmente raccogliere dall'uso degli Strumenti, sono utilizzate per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. Per tutela del patrimonio aziendale si intende altresì la sicurezza informatica e la tutela del sistema informatico aziendale. Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".
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 controllo a distanza dell'attività dei lavoratori.
Il presente Regolamento è adottato ai sensi dell'art. 4 comma 3 della L. 300/70 e delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007 ed integra l'informativa sul trattamento dei dati personali resa ai sensi dell'art. 13 del D.Lgs 196/03.

1. Entrata in vigore del Regolamento e pubblicità

1.1 Il presente Regolamento entra in vigore il 25.01.2018.
1.2 Con l'entrata in vigore del presente Regolamento tutte le norme e le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.
1.3 Copia del Regolamento, oltre ad essere affisso nella bacheca Aziendale, nonché viene reso disponibile presso i Servizi Informativi (di seguito anche "SI" o "Servizio IT").

2. Principi generali di riservatezza nelle comunicazioni

2.1. Il dipendente si attiene alle seguenti regole di trattamento

a) È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni aziendali dei quali il dipendente / collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno della Società. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile di area/funzione.
b) È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro.
c) È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni aziendali quando il dipendente/collaboratore si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti la pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office e di ricezione di Clienti / Fornitori o colleghi di lavoro.

d) Per le riunioni e gli incontri con Clienti, Fornitori, Consulenti e Collaboratori dell'Ente è necessario utilizzare le apposite Sale dedicate.

3. Trattamenti con Strumenti elettronici

3.1. Per "strumenti elettronici" si intendono i PC, tablet, smartphone, notebook e altri strumenti con relativi software e applicativi (di seguito anche "Strumenti").

Il dipendente/collaboratore è consapevole che gli Strumenti forniti sono di proprietà di A & T 2000 S.p.A. e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa.
Ciascun dipendente /collaboratore si deve attenere alle seguenti regole di utilizzo degli Strumenti.
a) Gli Strumenti affidati all'incaricato sono uno strumento di lavoro di proprietà della Società. Ogni utilizzo degli stessi non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza.
b) Il Personal Computer, notebook, tablet ed ogni altro hardware deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente al personale dei Servizi Informativi ogni malfunzionamento e/o danneggiamento.
c) Il Personal Computer deve essere spento al termine della giornata lavorativa oppure se ci si assenta dall'ufficio per un periodo di tempo prolungato. Negli altri casi di inutilizzo, anche se per brevi periodi, è comunque necessario disconnetterlo dalla rete premendo il tasto di accensione.
d) Non devono essere lasciati lavori incompiuti sullo schermo. È buona norma non lasciare documenti aperti e visibili sullo schermo del PC quando vi allontanate dalla postazione di lavoro anche solo temporaneamente o quando si riceve il pubblico, clienti/fornitori o colleghi.
e) È vietato l'utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli strumenti Aziendali, salvo che il supporto utilizzato sia stato fornito dai Servizi Informativi. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.
f) Gli Strumenti sono accessibili esclusivamente attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 5 del presente Regolamento.
g) Non deve essere permesso l'uso del proprio Strumento (fatta eccezione esclusivamente per i computer desktop in uso presso la sede aziendale e previa comunicazione al Servizio IT) e/o account ad altri colleghi d'ufficio o a soggetti terzi.
h) Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale dei Servizi Informativi, 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 Società a responsabilità civili e penali; si sottolinea che le violazioni della normativa a tutela dei diritti d'autore sul software impone la presenza nel sistema di software regolarmente licenziato. Comportamenti diversi sono sanzionati anche penalmente.
i) È obbligatorio rispettare le leggi in materia di sicurezza informatica. È vietato installare/utilizzare senza autorizzazione software che possa creare problemi di sicurezza o danneggiare la rete, come port scanner, security scanner, network monitor, network flooder, fabbriche di virus o di worm.
j) Salvo preventiva espressa autorizzazione del personale dei Servizi Informativi, 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 chiavette Internet, masterizzatori, modem, ecc.
k) I Notebook o Tablet in dotazione devono essere custoditi con diligenza, anche in relazione al rischio di furti. In particolare è vietato lasciare tali strumenti incustoditi ed in vista all'interno di veicoli, della Società o personali. È fatto obbligo configurare un codice o segno di sblocco e una tempistica di blocco automatico dello schermo. Fatte salve eccezioni autorizzate dai Servizi Informativi, è fatto divieto di disabilitare il controllo del PIN. L'utilizzo di dispositivo con più SIM deve essere preventivamente autorizzato dai Servizi Informativi.

I log relativi all'utilizzo di Strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui Server o sui router aziendali, nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso i Servizi Informativi aziendali, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.
I controlli possono avvenire secondo le disposizioni previste al successivo punto 5 del presente Regolamento.
Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

3.2. Uso del File System aziendale e della Rete Intranet

Il dipendente/collaboratore è consapevole che le risorse del File System (server, cartelle condivise, stampanti condivise, ecc.) e della rete Intranet della Società sono necessari per rendere la prestazione lavorativa.
Ciascun dipendente / collaboratore si deve attenere alle seguenti regole di utilizzo del File System e della Rete Intranet.

a) Per garantire la sicurezza informatica e per motivi di organizzazione della produzione, l'Utente deve salvare ogni dato ed informazione sul Server aziendale, astenendosi dal salvataggio in locale (su desktop, sulla cartella "documenti" del proprio Strumento, ecc.), salvo espressa autorizzazione da parte dei SI.

b) È vietato il salvataggio sui server della Società, ovvero sugli Strumenti, di documenti non inerenti l'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film e quant'altro. Ogni materiale personale rilevato dall'Amministratore di Sistema o dai Servizi Informativi a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche su Strumenti viene rimosso secondo le regole previste nel successivo punto 5 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare.

c) Senza il consenso del Titolare, è vietato trasferire documenti elettronici dai sistemi informativi e Strumenti della Società a device esterni (hard disk, chiavette, CD, DVD e altri supporti).

d) Senza il consenso dei Servizi Informativi è vietato salvare documenti elettronici della Società (ad esempio pervenuti via mail o salvati sul Server o sullo Strumento in dotazione) su repository esterne (quali ad esempio Dropbox, GoogleDrive, OneDrive, ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi.

e) Con regolare periodicità (almeno una volta al mese), ciascun utente provvede 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.

f) È vietato accedere alla rete aziendale con Strumenti personali, salvo l'utilizzo di reti o infrastrutture a ciò dedicate.

g) È vietato accedere alla rete Intranet 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.

h) I Sistemi Operativi degli Strumenti (IOS, Android ecc.) e gli altri Account necessari per il funzionamento degli Strumenti o degli applicativi (Microsoft ecc.) sono attivati dai Servizi Informativi con Account aziendali, che vengono gestiti dall'Ente e concessi in uso temporaneo all'Utente. E' vietato utilizzare gli Account ed i Servizi disponibili nel contesto degli Account (Repository, Cloud, Agenda, mail, Calendario, Note ecc.) per finalità personali.

I log relativi all'uso del File System e della intranet aziendale, nonché i file salvati o trattati su Server o Strumenti, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso i Servizi Informativi aziendali, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.
Si informa che gli Strumenti dell'Ente e/o i relativi Sistemi Operativi (IOS, Android ecc.) nonché gli altri Account necessari per il funzionamento degli Strumenti o degli applicativi (Microsoft ecc.) sono attivati dai Servizi Informativi con Account aziendali e vengono gestiti dall'Ente e concessi in uso temporaneo all'Utente. I log e i file contenuti negli Strumenti dell'Ente e/o i relativi Sistemi Operativi (IOS, Android ecc.) nonché gli altri Account necessari per il funzionamento degli Strumenti o degli applicativi (Microsoft ecc.) non sono oggetto di controllo sistematico da parte dell'Azienda, ma potrebbero essere oggetto di accesso per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.
I dati contenuti negli Account Aziendali verranno resettati alla riconsegna degli Strumenti ovvero alla cessazione dell'utilizzo del Servizio da parte dell'Utente.
I controlli possono avvenire secondo le disposizioni previste al successivo punto 5 del presente Regolamento.
Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

3.3. Uso dell'indirizzo di Posta elettronica

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.
Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo dell'indirizzo di Posta elettronica.
a) La casella di posta elettronica assegnata all'utente è di proprietà della Società, ancorché sia strutturata riportando i dati anagrafici del dipendente/collaboratore. Essa è domicilio informatico della Società ed è concessa esclusivamente quale strumento di lavoro.
b) È vietato utilizzare indirizzi di posta elettronica personali per finalità lavorative.
c) È vietato utilizzare le caselle di posta elettronica **con dominio @aet2000.it** per motivi diversi da quelli strettamente legati all'attività lavorativa, in particolare per l'invio e la ricezione di messaggi che non abbiano contenuto e rilevanza giuridica e commerciale. A titolo puramente esemplificativo, all'utente è vietato utilizzare la posta elettronica per:
- l'invio e/o il ricevimento di allegati contenenti contenuti multimediali (immagini, foto, filmati o brani musicali) non correlati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali, legati alla famiglia, amicizie, associazioni, acquisti di beni o servizi online, partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche o di Sant'Antonio. Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale dei Servizi Informativi. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

d) È vietato utilizzare la casella di posta elettronica aziendale quale username / nome utente (ovvero come indirizzo mail di riferimento) per Servizi non inerenti l'attività lavorativa (es. per account di social network, servizi di e-commerce, registrazione a siti web, ecc.)
e) La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili, obsoleti e soprattutto gli allegati ingombranti.
f) Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per la Società ovvero contenga documenti da considerarsi riservati in quanto

contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere autorizzata o visionata dal Responsabile di Area/Funzione.

g) È obbligatorio controllare con attenzione gli allegati di posta elettronica prima del loro utilizzo, verificando prima dell'apertura degli stessi ogni elemento che possa indurre a ritenere che si tratti di un VIRUS (es. se il mittente è sconosciuto, se il testo della mail presenti strani errori di battitura o un testo poco comprensibile ecc.). In caso di dubbio rivolgersi preventivamente ai Servizi Informativi.

h) È vietato effettuare l'apertura di file allegati alla posta elettronica che siano eseguibili (.exe), cartelle compresse (.zip, .rar, ecc.) soprattutto se provenienti da istituzioni bancarie o società di servizi (Enel, Eni, Wind, Telecom, Poste, ecc.)

i) 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 del dipendente/collaboratore (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella, o malattia) invierà messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In caso di assenze programmate la funzionalità deve essere sempre attivata dall'utente; in caso di assenza non programmata (ad es. per malattia) verrà attivata a cura dei Servizi Informativi.

j) Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato, appositamente definito dai SI di concerto con l'ufficio comunicazione, nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato della Società potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nel presente Regolamento.

Si informa che, ai sensi dell'articolo 2214 del Codice civile e dell'articolo 22 del Dpr 600/73, la Società deve conservare per dieci anni sui propri Server di Posta Elettronica tutti i messaggi di posta elettronica a contenuto e rilevanza giuridica e commerciale provenienti da e diretti a domini aziendali.
Si informa altresì che la Società, per il tramite dei Servizi Informativi, non controlla sistematicamente il flusso di comunicazioni mail né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail.
Tuttavia, in caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale ovvero per motivi di sicurezza del sistema informatico, la Società per il tramite dei Servizi Informativi può, secondo le procedure indicate successivo punto 5 del presente Regolamento, accedere all'account di posta elettronica aziendale, prendendo visione dei messaggi, salvando o cancellando file.
Si informa che, in caso di cessazione del rapporto lavorativo, la mail aziendale affidata all'incaricato verrà sospesa per un periodo di **6 mesi** e successivamente disattivata. Nel periodo di sospensione l'account rimarrà attivo e visibile ad un soggetto incaricato dalla Società solo in ricezione, che tratterà i dati e le informazioni pervenute per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, trasmettendone il contenuto ad altri dipendenti (se il messaggio ha contenuto lavorativo) ovvero cancellandolo (se il messaggio non ha contenuto lavorativo). Il sistema in ogni caso genererà una risposta automatica al mittente, invitandolo a reinviare il messaggio ad altro indirizzo mail aziendale.
Le informazioni eventualmente raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

3.4. Uso della rete Internet e dei relativi servizi

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

Ciascun dipendente /collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.

a. Gli Strumenti assegnati al singolo utente possono essere abilitati alla navigazione in Internet. La rete Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

b. Fermo quanto sopra, a titolo puramente esemplificativo, l'utente non potrà utilizzare la rete Internet per:

- l'upload o il download di software, documenti, file multimediali (film, musica, ecc.) anche tramite software peer to peer;
- 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 dal Legale Rappresentante o eventualmente dal Responsabile di Area / Funzione o dai Servizi Informativi 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 e Social non professionali, 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 di Area / Funzione;
- l'accesso, tramite internet, a siti non inerenti l'attività lavorativa nonché servizi web di qualsiasi genere non inerenti l'attività lavorativa (quali caselle webmail di posta elettronica personale, servizi online di Google / Apple / Microsoft ecc.).

c. Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda, come a titolo esemplificativo: filmati (tratti da youtube, siti di informazione, siti di streaming ecc) o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.

d. È vietato accedere ai social network (Facebook, Twitter, Linkedin, YouTube, Whatsapp ecc) durante l'orario di lavoro. Il divieto si estende anche al caso di utilizzo di smartphone e tablet personali.

e. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, in ossequio ai principi di prevenzione illustrati nelle "Linee guida del Garante per posta elettronica e internet" pubblicato in Gazzetta Ufficiale n. 58 del 10 marzo 2007, A & T 2000 S.p.A. rende peraltro nota l'adozione di 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. Eventuali richieste di accesso a siti "bloccati" devono essere inoltrate ai Servizi Informativi, che le valuterà unitamente al responsabile del Trattamento.

Si informa che la Società, per il tramite dei Servizi Informativi, non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo Utente, né controlla con sistemi automatici i dati di navigazione dello stesso.

Si informa tuttavia che al fine di garantire il Servizio Internet e la sicurezza dei sistemi informativi, nonché per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, l'Ente registra per 60 giorni i dati di navigazione (file di log riferiti al traffico web) con modalità inizialmente volte a precludere l'immediata e diretta identificazione di Utenti, mediante opportune aggregazioni.

Solo in casi eccezionali e di comprovata urgenza rispetto alle finalità sopra descritte, l'Ente può trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente.

In tali casi i controlli avverranno nelle forme indicate al successivo punto 5 del presente Regolamento.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

3.5. Multifunzione, Fax, Fotocopiatrici, Scanner, Plotter e altri strumenti (strumenti di stampa)

Il dipendente è consapevole che gli Strumenti di stampa sono di proprietà della Società e sono affidati all'utente per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.
Ciascun dipendente /collaboratore si deve attenere alle seguenti regole di utilizzo.

a. È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di Area / Funzione.
b. È vietato l'utilizzo delle multifunzioni, fotocopiatrici, scanner, plotter aziendali e altri strumenti di stampa per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Area / Funzione.
c. È necessario prestare attenzione alle fotocopie e alle stampe di documenti: copie mal riuscite, inutilizzate, minute, appunti ecc. devono essere eliminate utilizzando la macchina distruggi-documenti, ovvero sminuzzando i fogli in modo che risultino difficilmente leggibili.

3.6 Telefonia cellulare, Smartphone, Tablet e Badge di Rilevazione Presenze

Il dipendente è consapevole che il telefono, lo smartphone, il tablet assegnati nonché ogni applicazione in essi installata (di seguito anche Strumenti) sono di proprietà di A & T 2000 S.p.A. e vengono affidati all'utente per rendere la prestazione lavorativa.

Pertanto ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa.

Ciascun dipendente /collaboratore si deve attenere alle seguenti regole di utilizzo.

a. È vietato effettuare comunicazioni nonché inviare o ricevere SMS o altre comunicazioni elettroniche a carattere personale o comunque non strettamente inerenti l'attività lavorativa.
b. L'eventuale uso promiscuo (anche per fini personali) degli Strumenti è possibile soltanto in presenza di preventivo accordo e in conformità delle istruzioni al riguardo impartite dal personale dei Servizi Informativi.
c. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di ragionevole necessità ed urgenza.
d. Salvo quanto previsto alla lettera b, è vietata l'installazione di Applicazioni non strettamente inerenti l'attività lavorativa e la sincronizzazione di qualsiasi file personale (sia proveniente da Applicazioni, che foto, filmati, contatti, chat ecc.) con l'Account aziendale con cui è stato attivato lo Strumento (vedi 3.2).
e. L'Utente è responsabile del corretto utilizzo e della custodia degli Strumenti.
f. Il dipendente è consapevole che il Badge di rilevazione delle presenze è di proprietà di A & T 2000 S.p.A. e viene concesso ad uso esclusivamente personale al fine di registrare sistematicamente su un software gestionale gli orari di entrata e uscita nonché per registrare gli accesi del personale. Il Badge deve essere conservato con cura, segnalando tempestivamente all'Ufficio del Personale eventuali danneggiamenti o lo smarrimento dello stesso. Il badge fornito impiega la tecnologia RFID (Radio Frequency Identification). Tale tecnologia si basa sullo sfruttamento delle onde radio per consentire l'identificazione del badge su cui è stata apposta un'etichetta elettronica che viene rilevata dai lettori.

Si informa che il telefono, smartphone, tablet o dispositivo portatile vengono attivati con Account aziendale (vedi art. 3.2) concessi in uso temporaneo all'Utente.

Le informazioni relative all'utilizzo degli Strumenti nonché i file con essi trattati (documenti, foto, video, messaggi ecc.) sono registrati nella memoria degli stessi ovvero possono lasciare traccia su Server e router aziendali, nelle relative bollette pervenute alla società o nelle "aree personali" dei siti dei fornitori dei servizi di telefonia, ovvero sono trattati negli account di attivazione dello Strumento (es. Microsoft, Google, Apple, etc.).

A & T 2000 S.p.A. non controlla sistematicamente tali informazioni, né sono installati software o sistemi in grado di monitore l'uso degli Strumenti. Esclusivamente per inderogabili esigenze organizzative e produttive e per la tutela del patrimonio aziendale, il personale dei Servizi Informativi può accedere a tali informazioni.

In caso di restituzione degli Strumenti, i dati saranno resettati.

I controlli possono avvenire secondo le disposizioni previste successivo punto 5 del presente Regolamento.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

4. Gestione delle credenziali di autenticazione agli strumenti e servizi aziendali

Il rilascio, la modifica o la cancellazione di credenziali di autenticazione che permettono l'accesso a Strumenti, posta elettronica, rete, Server della Società, ecc. vengono effettuati dal personale dei Servizi Informativi, previa espressa indicazione della Direzione aziendale ovvero previa formale richiesta del Responsabile di Area / Funzione nell'ambito del quale lavora l'utente.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dai Servizi Informativi, associato ad una parola chiave (password) riservata che deve essere custodita dall'incaricato con la massima diligenza.
È vietato comunicare a soggetti terzi le proprie credenziali.
Se necessario far accedere terzi ai sistemi informativi protetti da una propria password, è necessario rivolgersi preventivamente e di volta in volta ai Servizi Informativi per l'autorizzazione.
È fatto assoluto divieto di trascrivere la parola chiave nei pressi della postazione di lavoro o in luoghi o strumenti accessibili a terzi.
La parola chiave, formata da lettere (maiuscole e minuscole), numeri e caratteri speciali, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato o alle parole chiave precedentemente utilizzate.
È necessario prestare particolare attenzione a non essere osservati mentre si digita la password o qualunque codice di accesso ai sistemi informatici. Infatti, anche se molti programmi non ripetono in chiaro la password sullo schermo, l'attenta osservazione da parte altrui dei tasti digitati può condurre all'individuazione della parola chiave.
È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni tre mesi. Si informa che il sistema assegna di default un termine di validità delle password: qualora l'utente non provveda a variare la propria password in tempo, l'accesso al personal computer e/o al sistema verrà temporaneamente bloccato.
Qualora la parola chiave dovesse venir sostituita in quanto abbia perso la propria riservatezza, si procederà a sostituirla come da modalità descritta nel presente Regolamento d'intesa con il personale dei Servizi Informativi.
Le parole chiave di accesso definite dagli utenti non sono conosciute dagli Amministratori di Sistema.

5. Controlli sugli strumenti (art. 6.1 Provv. Garante, ad integrazione dell'informativa ex art. 13 D.Lgs 196/03)

5.1. Principi generali

L'uso degli Strumenti Informatici della Società può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei riquadri di cui ai punti 3.1 – 3.2. – 3.3 – 3.4 – 3.5 – 3.6 del presente Regolamento.
Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'Utente, possono essere oggetto di controlli da parte della Società, per il tramite dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.).
Gli interventi di controllo sono di due tipi (di seguito descritti al punto 5.2 e 5.3) e possono permettere alla Società di prendere indirettamente cognizione dell'attività svolta con gli strumenti.

5.2. Controlli per la tutela del patrimonio aziendale, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.).
Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni descritte ai punti 3.1 – 3.2. – 3.3 – 3.4 – 3.5 – 3.6 il Responsabile del trattamento dei dati personali per il tramite dei Servizi Informativi, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

1. Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento.
2. Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, la Società potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni descritte ai punti 3.1 – 3.2. – 3.3 – 3.4 – 3.5 – 3.6 con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.
3. Qualora il rischio di compromissione del sistema informativo aziendale sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti 1 e 2, il Responsabile del Trattamento, unitamente all'amministratore di sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

Tutti i controlli sopra descritti avvengono nel rispetto del principio di necessità e non eccedenza rispetto alle finalità descritte nel presente Regolamento. Dell'attività sopra descritta viene redatto verbale, sottoscritto dal Responsabile del Trattamento e dall'Amministratore di Sistema che ha svolto l'attività.
In caso di nuovo accesso da parte dell'utente allo Strumento informatico oggetto di controllo, lo stesso dovrà avvenire previo rilascio di nuove credenziali (salvo diverse esigenze tecniche).
Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

5.3. Controlli per esigenze produttive e di organizzazione
Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un Utente (quali file salvati, posta elettronica, chat, SMS, ecc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato.

Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni descritte ai punti 3.1 – 3.2. – 3.3 – 3.4 – 3.5 – 3.6 il Responsabile del trattamento dei dati personali, per il tramite dei Servizi Informativi, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

1. Redazione di un atto da parte del Direttore e/o Capo Area che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
2. Incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
3. Redazione di un verbale che riassuma i passaggi precedenti.
4. In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.
5. Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

6. Partecipazioni a social media

6.1. L'utilizzo a fini promozionali e commerciali di Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali (ed altri siti o social media) è gestito ed organizzato esclusivamente dalla Società attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

6.2. Fermo restando il diritto della persona alla libertà di espressione, la Società 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 è vietata la partecipazione agli stessi social media durante l'orario di lavoro.

6.3. Il presente articolo deve essere osservato dall'Utente sia che utilizzi dispositivi messi a disposizione dalla Società, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente della Società.

6.4. La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni aziendali considerate dalla Società riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici. 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 della Società. L'utente, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo della Società, 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.

6.5. L'utente deve garantire la tutela della riservatezza e dignità 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 nei 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.

6.6. Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali (es. post su prodotti, servizi, fornitori, partner, ecc.) egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con la Società, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili alla Società.

7. Sanzioni

È fatto obbligo a tutti i dipendenti/collaboratori/utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento.

Eventuali violazioni del presente Regolamento da parte dei dipendenti nonché di altre norme previste dal CCNL applicato, a seconda della gravità della infrazione, comportano l'adozione dei seguenti provvedimenti secondo le disposizioni del Codice Sanzionatorio aziendale:

- censura scritta;
- sospensione dal servizio;
- licenziamento in tronco;
- licenziamento di diritto.

Rimane comunque riservato il diritto di intraprendere azioni civili e penali nei confronti dei responsabili di qualsivoglia violazione a danno della Società.