REGOLAMENTO PER L'UTILIZZO DELLE RISORSE INFORMATICHE AZIENDALI

Alstom Ferroviaria S.p.A.
Alstom Services Italia S.p.A.

Ultimo aggiornamento al 19/12/2019

Premesse e termini utilizzati

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai personal computer, espone **Alstom Ferroviaria S.p.A.** P.I. 02791070044 ed **Alstom Services Italia S.p.A.** P.I. 03430220040 (d'ora in avanti, congiuntamente, l'"Azienda") ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Azienda stessa.

L'Azienda mette a disposizione del proprio personale, per il corretto svolgimento dell'attività lavorativa, le necessarie risorse informatiche, telematiche, elettroniche e telefoniche quali personal computer, smartphone, tablet (con possibilità di navigazione in internet, utilizzo della posta elettronica, ecc.), stampanti e altro.

Al fine di eliminare o quantomeno ridurre i rischi derivanti da un uso poco corretto o poco consapevole delle risorse messe a disposizione, dando per acquisito che l'utilizzo di qualsiasi strumento di lavoro deve sempre ispirarsi ai principi di diligenza e correttezza impliciti nell'ambito del rapporto di lavoro, vengono impartite a tutti gli utenti che utilizzano dette risorse (siano essi dipendenti, amministratori, collaboratori, consulenti, dipendenti di enti o aziende esterne legate da contratti di fornitura di servizi o altri individui a cui ne è concesso l'uso) le modalità e condizioni di utilizzo.

Oltre che per mitigare i rischi di un uso insicuro degli strumenti, questo documento si propone anche di chiarire alcuni aspetti fondamentali relativi alle modalità e alle condizioni di utilizzo delle risorse, al fine di migliorarne l'efficienza d'uso, evitare utilizzi non conformi alla destinazione delle risorse stesse e garantire tempestività nell'attività di assistenza tecnica.

È utile definire in questa premessa i termini maggiormente ricorrenti nel documento o quelle definizioni tecniche che potrebbero essere difficilmente comprensibili:

- *Risorse informatiche*: qualsiasi combinazione di apparati tecnologici, hardware o software aziendali utilizzati per le comunicazioni elettroniche e l'elaborazione dei dati.
- *Mobile Device*: cellulare, smartphone, tablet e simili.
- *Situazione d'emergenza*: circostanza in cui la tempestività d'azione è di fondamentale importanza al fine di evitare danni significativi a cose o persone, perdita di informazioni o di prove di rilievo per l'Azienda, danni economici e di immagine o l'interruzione della continuità operativa aziendale.
- *Servizi IT*: la struttura che si occupa della gestione operativa delle risorse informatiche.
- *Trattamento*: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione, mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- *Dato personale*: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- *Categorie Particolari di Dati Personali*: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo

univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

- *Dati giudiziari*: i dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.
- *Titolare del trattamento*: Alstom Ferroviaria S.p.A. ed Alstom Services Italia S.p.A.
- *Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;*
- *Autorizzato* ogni persona fisica (a titolo esemplificativo si citano: dipendenti, collaboratori, lavoratori somministrati, stagisti o tirocinanti) autorizzata a compiere operazioni di trattamento dal Titolare. Tale figura potrà anche venir indicata quale "Utente", quando le operazioni eseguite da questi comportano il trattamento dei dati personali sotto l'autorità del Titolare.
- *Utente*: ciascuna persona che acceda alle Risorse informatiche.

1. Entrata in vigore del regolamento, pubblicità e campo di applicazione

1.1 Questo regolamento è in vigore a partire dalla data di approvazione indicata nella prima pagina e copia dello stesso verrà messa a disposizione di ciascun Autorizzato, anche per gli effetti delle seguenti normative:

- Tutela dei Dati Personali: Reg. UE 679/2016 (di seguito "**GDPR**" o "**Regolamento**"), D.lgs. 196/2003 (con ciò intendendosi lo stesso decreto modificato a seguito dell'entrata in vigore del Regolamento - o il decreto sostitutivo dello stesso d.lgs. 196/2003 ai fini del Regolamento, di seguito "**Decreto**") e provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali; successivamente all'entrata in vigore dello strumento legislativo di armonizzazione della normativa italiana con il Regolamento ("**Decreto di Armonizzazione**"), i rinvii alle disposizioni del Codice abrogate dal Decreto di Armonizzazione, contenuti in norme di legge e nel presente regolamento, si intendono riferiti alle corrispondenti disposizioni del GDPR e a quelle introdotte o modificate dal Decreto di Armonizzazione, in quanto compatibili.
- Lavoro: le linee guida del Garante per posta elettronica e internet. Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- Art. 4, 3° comma, legge 20 maggio 1970, n. 300, come modificato dall'art. 23 del decreto legislativo 14 settembre 2015, n. 151.

1.2 Le norme contenute in questo regolamento si applicano, in quanto compatibili, a tutti gli utenti che utilizzano le risorse informatiche aziendali (a titolo di esempio si citano i dipendenti di enti o aziende esterne legate da contratti di fornitura di servizi) anche se non designati "incaricati".

1.3 Il regolamento, oltre ad essere affisso nella bacheca aziendale, verrà pubblicato nella intranet aziendale.

2. Utilizzo delle risorse informatiche aziendali

2.1 L'utilizzo delle risorse informatiche aziendali è riservato ai dipendenti e agli altri soggetti espressamente autorizzati dall'Azienda.

2.2 Tutti i computer e i server di rete sono protetti da credenziali di autenticazione (nome utente e password) assegnate a ciascun utente. L'abilitazione all'accesso alla rete, a specifiche cartelle di memorizzazione sui server o a specifiche applicazioni necessarie per ciascun utente, vanno richieste al proprio Responsabile di ufficio/area.

2.3 Tutti i responsabili di ufficio/area sono invitati a comunicare prontamente ai Servizi IT qualsiasi modifica relativa all'organico o all'assegnazione di compiti e mansioni operative che richieda l'attivazione o la sospensione di servizi informatici o autorizzazioni all'accesso a risorse o banche dati.

2.4 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 (personal computer, periferiche, stampanti locali, mobile devices, alimentatori, cavi, ecc.). Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di 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 denunciati alle autorità competenti e prontamente segnalati al proprio Responsabile di ufficio/area. Copia della denuncia deve essere prontamente consegnata all'ufficio personale.

3. Utilizzo della rete

3.1 Hanno diritto ad accedere alla rete aziendale tutti gli utenti autorizzati dall'Azienda. L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature. I Servizi IT possono limitare l'accesso alla rete di determinate categorie di utenti, quando ciò sia richiesto da ragioni tecniche oppure per esigenze lavorative.

3.2 L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare le indicazioni presenti in questo documento e le eventuali altre norme disciplinanti le attività e i servizi che si svolgono via rete e si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi. L'utente che ottiene l'accesso alla rete e agli applicativi si assume inoltre la totale responsabilità delle attività che svolge tramite la rete.

3.3 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.

3.4 Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Nelle unità di rete adibite a scambio files (Dischi di rete ed FTP), i file memorizzati per lo scambio con altri utenti devono essere tempestivamente eliminati a scambio avvenuto.

3.5 Le password d'accesso alla rete ed ai programmi sono personali e vanno gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

3.6 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.

3.7 I Servizi IT possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericoloso per la sicurezza della rete aziendale.

4. Utilizzo di personal computer

4.1 L'accesso all'elaboratore è protetto da password che deve essere custodita dall'utente con la massima diligenza e non divulgata.

4.2 Non è consentito all'utente modificare la configurazione impostata sul proprio PC, salvo previa autorizzazione esplicita dei Servizi IT.

4.3 Durante la prestazione dell'attività lavorativa in azienda, il personal computer deve essere assicurato tramite cavo di sicurezza alla postazione di lavoro. Il personal computer non deve essere lasciato incustodito e con la sessione di lavoro attiva. In caso di allontanamento dalla postazione di lavoro l'utente deve attivare lo screen saver con la relativa password di protezione. Il PC deve essere spento ogni sera prima di lasciare gli uffici e in caso di assenze prolungate dall'ufficio.

4.4 L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete. I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.

4.5 È consentito l'uso e l'installazione dei programmi distribuiti e autorizzati ufficialmente dai Servizi IT. Qualora, per imprescindibili esigenze professionali, si renda necessario installare nuovi applicativi sulle postazioni di lavoro non in gestione dei Servizi IT, questi ultimi dovranno essere debitamente provvisti di licenza e provenienti da fonti autorizzate. Si rammenta che, in ogni caso, si dovrà contattare i Servizi IT che provvederanno a verificarne la compatibilità nonché a fornire le corrette istruzioni per l'installazione e/o a procedere direttamente all'installazione.

L'inosservanza della presente disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (L. 633/41 e successive modifiche; D.Lgs. 518/92 sulla tutela giuridica del software; L. 248/2000, nuove norme di tutela del diritto d'autore; L. 128/2004 e successive modifiche) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore. Si evidenzia, inoltre, che tali comportamenti possono anche far sorgere una responsabilità amministrativa a carico dell'Azienda, come disposta dal D.Lgs. 231/2001, con applicazione di sanzioni pecuniarie ed interdittive.

4.6 Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, hd usb, chiavette USB per accesso a reti esterne a quella aziendale, ecc.), se non con espressa autorizzazione aziendale. Per le modalità di attivazione della procedura autorizzativa, si prega di contattare i Servizi IT

4.7 È vietato connettere o configurare punti di accesso wireless parassiti connessi all'infrastruttura di rete aziendale in quanto causa di possibili problemi di intrusione dall'esterno, a meno di autorizzazione dei Servizi IT.

5. Gestione delle credenziali di autenticazione

5.1 Le credenziali di autenticazione per l'accesso al PC, alla rete e ai programmi vengono assegnate dal personale dei Servizi IT, previa formale richiesta del Responsabile dell'ufficio/area interessata.

5.2 È necessario procedere alla modifica della password a cura dell'Autorizzato del trattamento al primo utilizzo e, successivamente, almeno ogni 90 giorni. Il sistema avvertirà l'utente della necessità di procedere a tale modifica.

5.3 Le password devono essere formate da lettere (maiuscole o minuscole) e numeri, ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'Autorizzato.

5.4 La password è personale e come tale deve essere conosciuta solamente dall'Autorizzato.

5.5 La password deve essere immediatamente sostituita nel caso si sospetti che la stessa abbia perso la segretezza.

5.6 Qualora l'utente dimentichi la password o venga a conoscenza di quella di altro utente, è tenuto a darne immediata notizia ai Servizi IT, che procederanno alla invalidazione della stessa.

5.7 Le password non devono mai esser salvate sul PC o in rete in file di testo (o simili) non protetti. La stessa parola chiave non deve essere utilizzata per sistemi di autenticazione interni alla rete aziendale e per sistemi di autenticazione esterni, come ad esempio l'accesso al proprio conto corrente bancario o alla propria Web Mail, specie se non legati direttamente all'attività lavorativa.

6. Accesso ai file su PC, mobile device e cartelle di rete

6.1 L'accesso ai file contenuti nei PC desktop e portatili, nei mobile device e nelle cartelle di rete presenti sui server è regolato da disposizioni e sistemi di autorizzazione studiati in base alle specifiche esigenze aziendali. La richiesta di abilitazione alle cartelle di rete va rivolta al proprio Responsabile di ufficio/area.

6.2 In caso di assenze prolungate o in situazioni di emergenza, alla persona che sostituisce nella funzione il dipendente assente possono essere assegnati diritti di autorizzazione tali da potere accedere a tutti i file necessari allo svolgimento della propria mansione, sia quelli presenti sulle cartelle di rete, sia quelli archiviati su PC desktop e portatili, sia su eventuali mobile device. In assenza di un sostituto specifico nella funzione del dipendente assente,

tali abilitazioni possono essere assegnate a un collega esplicitamente delegato o al Responsabile di ufficio/area.

6.3 In caso di cessazione del rapporto di lavoro, alla persona che sostituisce nella funzione il dipendente cessato, vengono assegnati diritti di autorizzazione tali da potere accedere a tutti i file necessari allo svolgimento della propria mansione, sia quelli presenti sulle cartelle di rete, sia quelli archiviati su PC desktop e portatili, sia su eventuali mobile device. In assenza di un sostituto specifico nella funzione del dipendente assente, tali abilitazioni possono essere assegnate a un collega esplicitamente delegato o al Responsabile di ufficio/area. Al personale che si appresta a concludere il rapporto di lavoro non è permesso cancellare file di interesse aziendale memorizzati su PC, su mobile device o sulle unità di rete.

7. Assistenza tecnica e protezione da virus

7.1 In caso di guasti e problemi relativi all'utilizzo delle postazioni di lavoro e/o delle funzionalità offerte dai sistemi di rete, il personale dovrà rivolgersi ai Servizi IT. In tal senso, gli utenti della rete non devono salvare sulla stazione di lavoro locale i propri documenti elettronici, ma conservarli nelle aree del server previste, poiché in caso di malfunzionamenti gravi delle postazioni di lavoro, potrebbe essere necessario procedere alla formattazione degli Hard Disk interessati ed alla rigenerazione completa dell'ambiente di lavoro.

7.2 Per facilitare le operazioni di aggiornamento del software e per garantire la sicurezza dei dispositivi, delle applicazioni e dei dati, i Servizi IT possono 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 previa autorizzazione dell'utilizzatore e di norma in presenza dell'utilizzatore stesso. In caso di malfunzionamenti straordinari e in situazioni di emergenza, gli amministratori di sistema hanno comunque facoltà di accedere in qualunque momento ai sistemi informatici per l'espletamento delle proprie funzioni.

7.3 Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o altro software malefico. In particolare, l'utente deve:

- limitare allo stretto necessario lo scambio fra computer di file con estensione: exe, dll, zip, com, bat, chm, cmd, cpl, hlp, hta, inf, lnk, ocx, pif, reg, scr, url, vbs, rar;
- non aprire gli allegati di posta se non si è certi della loro provenienza;
- non cliccare mai un link presente in un messaggio di posta elettronica di provenienza sconosciuta;
- non cliccare mai, durante la navigazione Internet, su banner o link pubblicitari non necessari per l'attività lavorativa.

7.4 Ogni anomalia o problematica relativa a virus ed antivirus dovrà essere prontamente segnalata ai Servizi IT. Nel caso il software antivirus rilevi la presenza di un file infetto non bonificato, l'utente dovrà immediatamente sospendere ogni elaborazione in corso - senza spegnere il PC - e segnalare l'accaduto.

8. Uso della posta elettronica

8.1 La casella di posta assegnata dall'Azienda all'utente è uno strumento di lavoro. 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 aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list per motivi non attinenti allo svolgimento delle mansioni assegnate salvo diversa ed esplicita autorizzazione della Direzione dell'Azienda. In ragione della possibile connessione con l'Azienda, l'utente dovrà

precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Azienda. Resta comunque inteso che le comunicazioni all-user Italia saranno veicolate esclusivamente dall'Azienda attraverso i canali istituzionali.

8.3 Considerata la finalità e la funzione dei sistemi di comunicazione aziendale e la stretta correlazione tra il contenuto dei messaggi di posta inviati e ricevuti con mail aziendale (anche del tipo nome.cognome@nomeazienda.it) e l'attività aziendale, la natura e il contenuto di tali messaggi di posta non può essere considerato confidenziale o riservato/personale. In casi eccezionali, la Direzione dell'Azienda potrà effettuare controlli, negli stretti limiti consentiti dal presente regolamento, dal GDPR, dalla normativa nazionale in materia di diritto del lavoro e di tutela dei dati personali e dai provvedimenti del Garante per la Tutela dei Dati Personali, per verificare il rispetto del regolamento e della legge, in caso di anomalie e di episodi che rivelino la potenziale – o attuale – commissione di illeciti, concordemente a quanto previsto nel seguito e dalla normativa applicabile.

8.4 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

8.5 L'azienda 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.

8.6 È fatto espresso divieto di sincronizzare o combinare l'account aziendale con il proprio eventuale account privato ovvero effettuare il back up della posta elettronica aziendale su dispositivi o per usi diversi da quelli aziendali.

9. Gestione della posta elettronica del personale assente o cessato

9.1 La casella di posta elettronica è uno strumento che può contenere informazioni utili per l'attività aziendale, pertanto in caso di assenze prolungate o per urgenti necessità, il dipendente deve predisporre una o più delle seguenti azioni:

9.1.1 Impostazione di un messaggio automatico di "out of office", in modo da segnalare a coloro che inviano messaggi alla casella l'assenza della persona che normalmente la riceve. Ove possibile, nel messaggio sarà segnalato anche il periodo dell'assenza e, se necessario, un indirizzo di posta alternativa a cui inviare il messaggio.

9.1.2 Re-inoltro di copia dei messaggi inviati alla casella del dipendente assente alla persona che la sostituisce nella funzione. In mancanza di un sostituto specifico, i messaggi possono essere inoltrati a un collega esplicitamente delegato o al Responsabile di ufficio/area.

9.1.3 Assegnazione dei diritti di accesso alla casella alla persona che sostituisce nella funzione il dipendente assente, in modo che questi possa accedere anche al contenuto dei messaggi precedenti al periodo di assenza. In mancanza di un sostituto specifico nella funzione del dipendente assente, tali abilitazioni possono essere assegnate, se necessario, a un collega esplicitamente delegato o al Responsabile di ufficio/area.

9.2 In caso di cessazione del rapporto di lavoro, la casella di posta elettronica assegnata al dipendente verrà disattivata e rimossa.

9.3 Al personale che si appresta a concludere il rapporto di lavoro è richiesto di:
- trasferire tutti i dati e le informazioni di interesse aziendale su OneDrive, coordinandosi con il proprio manager;
- eliminare tutte le informazioni e i dati di carattere personale presenti all'interno del personal computer o della propria casella di posta elettronica.
Al personale che si appresta a concludere il rapporto di lavoro non è permesso cancellare i messaggi di interesse aziendale presenti nella casella di posta elettronica.

10. Uso della rete internet e dei relativi servizi

10.1 Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.

10.2 È fatto divieto all'utente lo scarico (download) di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dai Servizi IT. Non è consentito lo scaricamento né l'esecuzione online di file musicali, video o multimediali; è da evitare la connessione a siti musicali o l'ascolto in linea di musica, notizie, radio o altro o il download di brani musicali: tali pratiche sono causa di sovraccarico della rete e ne limitano l'utilizzo per fini lavorativi; analogo problema comporta l'accesso a filmati e webcam, salvo naturalmente i casi direttamente attinenti all'attività lavorativa.

10.3 È da evitare ogni forma di registrazione con account aziendale a siti, social media, forum, chat non attinenti all'attività lavorativa. È vietata la partecipazione a Forum non professionali, 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 di ufficio/area.

10.4 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.

10.5 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 potrebbero, attraverso elaborazioni ed associazioni, permettere 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. Nelle normali procedure di elaborazione tali file di log non sono conservati. In presenza di gravi anomalie o problemi tecnici dovuti al comportamento degli utenti, si procederà alla loro conservazione 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 a controlli su base individuale.

10.6 Non è ammesso utilizzare Internet per esigenze private, salvo nei periodi di pausa consentiti dal regolamento aziendale. Anche in questo ultimo caso devono essere rispettate le leggi vigenti e comunque non devono essere pregiudicati gli interessi aziendali né devono essere perseguiti intenti di lucro o immorali. In particolare:

(i) non è consentito l'accesso a determinate categorie di siti web quali ad esempio i siti di pornografia, pedopornografia, violenza, malware, etc.;

(ii) non è consentito l'upload o il download di software gratuiti (freeware e shareware) prelevati da siti Internet, 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 preventivamente contattata la Direzione Aziendale), se non previa espressa autorizzazione dell'Azienda;

(iii) è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;

(iv) non sono permesse, per motivi non professionali, la partecipazione a forum, l'utilizzo di chat line o di bacheche elettroniche e le registrazioni in guest book, anche utilizzando pseudonimi (o nickname);

(v) non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

(vi) tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo antivirus;

(vii) non è consentito scaricare e/o memorizzare file di grandi dimensioni salvo che per necessità lavorative e, in tale ultimo caso, previo loro inoltro alla Direzione Aziendale;

(viii) non è consentito, salvo preventiva esplicita autorizzazione dell'Azienda, lo scambio (ad esempio Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, etc., protetto da copyright;

(ix) non è consentito sfruttare i loghi o materiale di proprietà dell'Azienda in una qualsiasi pagina web o pubblicarli su Internet, a meno che tale azione non sia stata anticipatamente approvata da un'unità operativa o dai responsabili aziendali;

(x) non è consentito l'accesso a siti di giochi e scommesse online, nonché - salvo preventiva autorizzazione dell'Azienda - di home banking;

(xi) non è consentito tentare di ottenere illegalmente accesso, ovvero causare danno o nocumento, a sistemi remoti accessibili via Internet;

(xii) è vietata, se non per motivi professionali, la partecipazione a forum, newsgroup, discussion groups, o bacheche elettroniche;

(xiii) è altresì proibito rigorosamente qualsiasi uso del web che possa essere associato all'Azienda e ne trasmetta un'immagine negativa o possa essere nocivo alla stessa. Pertanto, non sono consentite attività (di trasmissione, download, salvataggio e/o connessione) che possono essere considerate illegali, fraudolente, spiacevoli, di disturbo, offensive, discriminatorie, diffamatorie;

(xiv) non è consentito creare pagine web o siti Internet per conto dell'Azienda, fingere di agire per conto della stessa o diffondere in alcun modo dati e informazioni riguardanti l'Azienda;

(xv) pubblicare materiale informatico dell'Azienda su computer accessibili via Internet che si avvalgano di servizi di FTP anonimo o simili, senza il preventivo espresso consenso espresso dell'Azienda.

11. Utilizzo di telefoni, mobile device, fax e fotocopiatrici aziendali

11.1 Il telefono aziendale affidato all'utente è uno strumento di lavoro.

11.2 Qualora venisse assegnato un mobile device aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al mobile device si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale e, in quanto compatibili, per l'uso dei PC.

11.3 I controlli sul corretto utilizzo dei telefoni aziendali verranno effettuati dal Responsabile di ufficio/area, o altra persona da lui incaricata, in presenza di evidenti anomalie, mediante *screening* generale dei tabulati telefonici. A seguito dei controlli effettuati, ove emergano comportamenti in violazione del presente regolamento, o comunque "anomali", si procederà con un avviso circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. Se a seguito di tali provvedimenti le anomalie dovessero ripetersi, si procederà con controlli su base individuale, secondo criteri di gradualità e conformità alla normativa in materia di tutela dei dati personali, così come indicato al punto 16.

11.4 I fax sono strumenti aziendali e il loro utilizzo per fini personali deve essere occasionale.

11.5 Le fotocopiatrici, le stampanti e gli scanner aziendali sono strumenti aziendali e il loro utilizzo per fini personali deve essere occasionale.

12. Custodia dei documenti cartacei contenenti dati personali

12.1 L'Azienda ha messo a disposizione appositi locali ed archivi ad accesso selezionato (di seguito "luogo sicuro"), ove sono di norma custoditi i documenti contenenti dati personali; come regola generale, tali documenti non devono essere asportati da tale luogo sicuro e, ove ciò avvenga, la asportazione deve essere ridotta al minimo tempo necessario per effettuare le operazioni di trattamento.

12.2 Dal luogo sicuro devono essere asportati solo i documenti strettamente necessari per le operazioni di trattamento e non intere pratiche, se ciò non è necessario. Al termine delle operazioni di trattamento, i documenti devono essere riposti nel luogo sicuro.

12.3 Per tutto il periodo in cui i documenti sono all'esterno del luogo sicuro, l'Autorizzato non deve mai perderli di vista, adempiendo ad un preciso obbligo di custodia dei documenti stessi.

12.4 I documenti di cui sopra non devono essere mai lasciati incustoditi sul tavolo durante il giorno. In particolare, ci si deve assicurare che un visitatore o terzo (ad esempio: addetto alla manutenzione, addetto alle pulizie o collega non autorizzato) non possa venire a conoscenza dei contenuti dei documenti.

12.5 E' cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria. Si deve porre particolare attenzione nell'utilizzo delle stampanti di rete, in particolare quando queste sono poste in luoghi il cui accesso non è controllato, recuperando immediatamente i documenti stampati quando questi contengono dati personali o informazioni aziendali riservate.

12.6 Devono essere ridotte allo stretto necessario le fotocopie di documenti che abbiano ad oggetto dati sensibili, giudiziari o comunque riservati.

12.7 Eventuali fotocopie/stampe non riuscite bene debbono essere distrutte in un apposito distruggitore, se disponibile, oppure devono essere distrutte in modo tale da non consentire la ricostruzione del contenuto. È tassativamente proibito utilizzare le fotocopie/stampe non riuscite, contenenti dati personali, come carta per appunti. È parimenti tassativamente proibito trasportare all'esterno del posto di lavoro fotocopie non riuscite, da utilizzare altrove come carta per appunti.

12.8 L'utente dovrà altresì attenersi alle misure di sicurezza relative agli archivi cartacei previsti dal Datore di Lavoro a tutela dei dati personali.

13. Custodia dei supporti rimovibili

13.1 In linea generale non è consentita la copia su cd, dvd, nastri, hd usb o simili (di seguito "supporti rimovibili") di dati personali, sensibili, giudiziari o informazioni costituenti il Know-How aziendale, per ridurre al minimo il rischio di perdita o distruzione anche accidentale dei dati stessi. Ciò premesso, ove nello svolgimento della normale attività assegnata all'Autorizzato, nell'ambito del suo profilo di autorizzazione, sia indispensabile effettuare una copia di tali dati su supporti rimovibili, occorre attenersi alle seguenti cautele:

13.1.1 Tutti i supporti rimovibili 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;

13.1.2 In caso di spedizione ad altro Autorizzato, occorre accertarsi che il destinatario abbia lo stesso profilo di autorizzazione del mittente e che il supporto rimovibile venga spedito in una busta sigillata, intestata personalmente all'Autorizzato. Non si deve spedire un supporto rimovibile, senza aver prima concordato con il destinatario stesso le modalità e tempi di consegna ed aver stabilito la procedura che permette di confermare l'avvenuta consegna al destinatario del supporto stesso;

13.1.4 L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti. Si faccia sempre attenzione a non dimenticare il supporto rimovibile all'interno del computer quando, al termine della copia, si spegne il computer e ci si allontana. Il supporto rimovibile non deve mai essere lasciato abbandonato sul tavolo, ma deve essere immediatamente posto all'interno di una custodia sicura, quando non utilizzato; in funzione della criticità dei dati archiviati, si può andare da un cassetto della scrivania chiuso a chiave sino ad una cassaforte.

14. Social Media Policy

14.1 L'utilizzo da parte dell'Azienda dei canali di social media – quali Facebook™, Twitter™, Linkedin™, Instagram™, You tube e in generale blog o forum, anche professionali – viene gestito ed organizzato attraverso figure professionali che all'interno dell'azienda si occupano della gestione dei social media (social media specialist e ufficio comunicazione) che parlano a nome dell'azienda, rimanendo escluse iniziative individuali, quali la creazione di account aziendali non ufficiali sui social media, da parte dei singoli/gruppi di utenti.

14.2 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. La policy qui dettata deve essere 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.

14.3 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni aziendali considerate dall'Azienda riservate e in genere, a titolo esemplificativo e non esaustivo, sulle informazioni finanziarie ed economiche, commerciali, sui piani industriali, sui clienti, sui fornitori e 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 fotografie e video od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione dell'Azienda.

14.4 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 della Direzione.

14.5 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.

14.6 Infine, in via generale ed ove non autorizzato in senso diverso dalla Direzione dell'Azienda, 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.

15. Osservanza delle disposizioni in materia di protezione dati personali e della normativa applicabile all'uso degli strumenti informatici

15.1 E' obbligatorio attenersi alle disposizioni contenute nel Reg. UE 679/2016 ("GDPR" o "Regolamento"), D.lgs. 196/2003 (con ciò intendendosi lo stesso decreto modificato a seguito dell'entrata in vigore del Regolamento - o il decreto sostitutivo dello stesso d.lgs. 196/2003 ai fini del Regolamento, di seguito "Decreto") e provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali; successivamente all'entrata in vigore dello strumento legislativo di armonizzazione della normativa italiana con il Regolamento ("Decreto di Armonizzazione"), i rinvii alle disposizioni del Codice abrogate dal Decreto di Armonizzazione, contenuti in norme di legge e nel presente regolamento, si intendono riferiti alle corrispondenti disposizioni del GDPR e a quelle introdotte o modificate dal Decreto di Armonizzazione, in quanto compatibili. Ciascun utente deve altresì attenersi alle disposizioni aziendali in materia di dati personali, in particolare alla Guida al Regolamento (UE) 2016/679 – GDPR e alle procedure in materia di misure di sicurezza.

Si informano gli Utenti che l'esercizio dei propri diritti in qualità di "Interessati" - così come previsti dall'art. 7, D.lgs. n. 196/2003 e dagli artt. 13, 15, 16, 17, 18, 20 e 21 del Regolamento Europeo n. 679/2016 potrà avvenire contattando il Datore di Lavoro secondo quanto indicato nell'informativa consegnata a ciascun utente nell'ambito del proprio rapporto di lavoro.

15.2 E' altresì obbligatorio attenersi alle disposizioni in materia di sicurezza sul lavoro (art. 2087 cod. civ., D. Lgs. n. 81/08 e ss.mm.ii., etc.), lotta alla pornografia e pedofilia (artt. 600-ter e 600-quater cod. pen., Legge 269/1998 e ss.mm.ii., Legge 38/06 e ss.mm.ii., etc.), tutela del diritto d'autore (Legge 633/1941 e ss.mm.ii., etc.) e contrasto ai reati informatici (artt. 615-ter, 615-quater, 615-quinquies, 635-bis e 640-ter cod. pen., Legge n. 547/1993 e ss.mm.ii., Legge n. 12/2012 e ss.mm.ii., etc.). Ciascun Utente, pertanto, è direttamente e personalmente responsabile delle proprie azioni nell'utilizzo del Sistema Informatico e, in genere, degli strumenti aziendali affidatigli per espletare i propri compiti e mansioni.

In caso di violazione del presente regolamento, l'Azienda potrà applicare, nel pieno rispetto di quanto previsto dall'art. 7 della Legge n. 300 del 1970, le sanzioni disciplinari previste dalla legge e dal CCNL applicabile, fatti salvi i rimedi, anche risarcitori, e le altre misure sanzionatorie previste dalle disposizioni della legge civile e/o penale.

Inoltre, il datore di lavoro informerà immediatamente – senza necessità di preventive contestazioni e/o addebiti formali – le autorità competenti nel caso di commissione di reato, sia essa effettiva o anche solo probabile o sospetta, tramite l'utilizzo illecito o non conforme dei sistemi informatici.

15.3 Gli strumenti informatici/tecnologici considerati nel presente Regolamento 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; conseguentemente le informazioni raccolte sulla base di quanto qui indicato, anche conformemente al successivo art. 16, 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, fermo restando il rispetto della normativa in materia di protezione dei dati personali.

16. Controlli graduali e accesso ai dati trattati dall'utente

16.1 Il Datore di Lavoro non effettua attività di controllo sistematico, quali, ad esempio:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- l'analisi sistematica delle pagine web visualizzate dal lavoratore;

- la lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- l'analisi occulta di computer portatili affidati in uso.

16.1 Il Datore di lavoro, inoltre, preso atto del divieto di utilizzo di strumenti informatici/tecnologici per il controllo dell'attività lavorativa del dipendente, assicura che i predetti strumenti saranno installati esclusivamente per esigenze di carattere organizzativo, produttivo, della sicurezza del lavoro e per la tutela del patrimonio aziendale.

Ferme restando le modalità di controllo specificate negli articoli precedenti, in caso di anomalie il personale incaricato dei Servizi IT, nel rispetto della normativa sulla protezione dei dati personali, potrà effettuare controlli su tutti gli strumenti informatici/tecnologici forniti dall'Azienda e sui documenti ivi contenuti, secondo un principio di gradualità e necessità, conformemente alle prescrizioni del GDPR.

16.2 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. Qualora si dovessero riscontrare reiterate violazioni del presente regolamento, indizi di commissione di gravi abusi, di illeciti o di attività contrarie ai doveri gravanti sull'Utente in virtù del rapporto di lavoro/collaborazione in essere, o l'anomalia inizialmente rilevata dovesse persistere, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale. In particolare, potranno essere effettuati controlli per le seguenti finalità:

- tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;
- 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 l'Azienda si riserva di avvalersi di soggetti esterni.

16.3 In presenza di seri indizi, il personale incaricato, anche previo l'ausilio di legali o consulenti tecnici appositamente nominati, 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.

In ogni caso, le modalità di effettuazione dei controlli sono state determinate dalla Datore di Lavoro sulla base di una valutazione, condotta alla luce delle attuali conoscenze tecnologiche e dei dispositivi concretamente utilizzati, volta a determinare i concreti rischi per la sicurezza dei dati personali dagli stessi derivanti e ad individuare le misure di sicurezza e i meccanismi necessari a ridurre al minimo tali rischi.

17. Non osservanza della normativa aziendale

17.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Fermi restando gli eventuali profili di responsabilità civile e penale, 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 e, nei confronti dei collaboratori, consulenti e fornitori esterni di cui al suddetto art. 1.2, verificata la gravità della violazione contestata, con la risoluzione o il recesso dal contratto ad essi relativo.

18. Aggiornamento e revisione

18.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione e dai Servizi IT.