



**OCS Officine Costruzioni Speciali S.p.A.**

**REGOLAMENTO PER L'UTILIZZO  
DEI SISTEMI E STRUMENTI INFORMATICI**

## **Premessa**

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet da Personal Computer, tablet e smartphone, espone *OCS* e gli utenti del sistema informativo aziendale (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.

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, *OCS* ha adottato un Regolamento interno diretto ad evitare che comportamenti anche inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e quindi del proprio sistema informatico. Il Regolamento 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 generale n. 679/2016 contenenti anche le misure di sicurezza, nonché integrano le informazioni già fornite agli interessati ai sensi dell'art. 13 del Regolamento generale n. 679/2016, 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 *OCS*, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo messo a disposizione dei propri collaboratori che ne necessitano per il tipo di funzioni svolte, **computer**, telefoni, telefoni cellulari, computer portatili, tablet, smartphone, ecc., sono state inserite nel Regolamento alcune clausole relative alle modalità ed ai doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

## 1. Entrata in vigore del Regolamento e pubblicità

- 1.1 Il nuovo Regolamento entrerà in vigore il 15/11/2021. Con l'entrata in vigore del presente Regolamento 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 del Regolamento, oltre ad essere affisso nella bacheca aziendale anche per quanto prevede l'art.7 della Legge n. 300/1970, verrà consegnato a ciascun dipendente, anche ai fini dell'art. 13 del Regolamento generale n. 679/2016 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. Pertanto, il presente regolamento entra a far parte, per quanto occorra, del Codice disciplinare aziendale.

## 2. Campo di applicazione del Regolamento

- 2.1 Il nuovo Regolamento si applica a tutti i dipendenti, collaboratori e consulenti dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto 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 del presente Regolamento nel contratto concluso con quest'ultimi.
- 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 o Notebook.

- 3.1 Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. 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 OCS solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto 4 del presente Regolamento.
- 3.3 OCS rende noto che il personale incaricato che opera presso il servizio Information and Communication Technology (nel seguito per brevità "Servizio ICT") della stessa OCS 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 *OCS* 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 *OCS* a 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 *OCS*.
- 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, ecc.).
- 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 del presente Regolamento 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.

#### **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.
- 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 essere **custodita dall'incaricato con la massima diligenza e non divulgata**.
- 4.3 La parola chiave, formata da lettere maiuscole, minuscole, numeri e caratteri speciali (es. punteggiatura, &, %, ecc.), deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

- 4.4 Il sistema assegna di default un termine di validità delle password **pari a sei mesi**. Qualora l'utente non provveda a variare la propria password in tempo, l'accesso al personal computer e/o alla rete aziendale verrà temporaneamente bloccato.
- 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 d'intesa con il personale del Servizio ICT.
- 4.6 Soggetto preposto alla custodia delle credenziali di autenticazione degli **utenti di amministrazione** dei sistemi informativi (sia software che apparati di rete) è il personale incaricato del Servizio ICT di *OCS*

## 5. Utilizzo della rete di *OCS*

- 5.1 Per l'accesso alla rete di *OCS* ciascun utente deve utilizzare la propria credenziale di autenticazione.
- 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 aree di memorizzazione dati utenti (cartelle o similari) presenti nei server di *OCS* 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. (Si ricorda che tutti i dischi o altre unità di memorizzazione locali - es. disco C: interno PC - non sono soggette a salvataggio da parte del personale incaricato del Servizio ICT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente).
- 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 tre 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.

## **6. Utilizzo di altri dispositivi elettronici**

- 6.1 Tutti i dispositivi elettronici dati in dotazione al personale di OCS 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 in questione vanno annoverati i telefoni aziendali, PC portatili, tablet, telefoni cellulari, smartphone, ecc., indipendentemente dal fatto che l'utente abbia o meno la possibilità di accedere alla rete di OCS 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. Dove possibile, è obbligatorio inserire un PIN per proteggere l'accesso allo strumento, della massima lunghezza consentita. In caso di smarrimento o furto di dispositivi l'utente dovrà immediatamente avvisare l'Azienda per consentire al servizio ICT la tempestiva cancellazione da remoto dei dati.
- 6.3 Con riferimento ai telefoni aziendali e telefoni cellulari aziendali, 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 o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, viene consentita solo nel caso di comprovata necessità ed urgenza. Inoltre, l'eventuale 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.
- 6.4 Si precisa, peraltro, che le disposizioni previste nel presente Regolamento ai punti 3, 7, 8, 9, 10 e 11 dello stesso trovano applicazione anche nell'uso dei dispositivi elettronici qui considerati.

## **7. Utilizzo e conservazione dei supporti rimovibili**

- 7.1 Tutti i supporti 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 severamente vietato l'utilizzo di supporti rimovibili personali.
- 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.

## 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 sui server di gestione del servizio 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 **con dominio aziendale** 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, **se non per fini di sviluppo o marketing, previa autorizzazione;**

Se si dovessero peraltro ricevere messaggi di tale tipo, si deve 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 i messaggi ivi contenuti, sottoposti, a cura dell'utente della casella, alle procedure di protocollazione ed archiviazione attivate dall'Azienda avendo di conseguenza presuntivamente natura 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), 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 all'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 *OCS* ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analogo 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 allegati 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 (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le coordinate di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere attivata e disattivata dall'utente.
- 8.8 In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere tempestivamente attivata dal lavoratore avvalendosi del servizio webmail - 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 8.8; assenza non programmata ed impossibilità di attendere i due giorni di cui al punto 8.9) 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.
- 8.11 OCS 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.
- 8.12 La casella di posta elettronica, unitamente alle credenziali di autenticazione per l'accesso alla rete, viene disattivata al momento della conclusione del rapporto di lavoro che ne giustificava l'assegnazione. Contestualmente alla disattivazione:
- verrà in automatico generata una mail ai mittenti 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.
- 8.13 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 apposito Regolamento aziendale a ciò dedicato e che va comunque a completare ed integrare il presente Regolamento.

## 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. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.
- 9.2 In questo senso, a titolo puramente esemplificativo, **l'utente non potrà 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.

- 9.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, *OCS* rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevenivano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una "black list".
- 9.4 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 30 giorni, 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 reparto 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 *OCS* 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.

## 11. Partecipazioni a social media

- 11.1 L'utilizzo a fini promozionali e commerciali dei social media – quali Facebook™, Twitter™, LinkedIn™, 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 di sicurezza, come indicato nella lettera di designazione ad incaricato al trattamento dei dati ai sensi del Regolamento generale n. 679/2016 e del presente Regolamento aziendale.
- 12.2 Gli strumenti 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 indicato nel Regolamento, 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, OCS provvederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n.300/1970, dandone anche opportuna informazione agli utenti stessi.

## **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, ecc.), 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. Sistemi di controlli gradualità**

- 14.1 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 compiuti solo in caso di successive ulteriori anomalie.
- 14.2 In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

## 15. Rilevazione incidenti

15.1 Al rilevamento di una violazione dei dati personali (data breach), ogni utente è tenuto ad informare tempestivamente il titolare del trattamento senza indebiti ritardi.

## 16. Sanzioni

16.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. 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 Metalmeccanici Industria, 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.

## 17. Aggiornamento e revisione

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

17.2 Il presente Regolamento è soggetto periodicamente a revisione.

Albignasego (PD), 15/11/2021

La Direzione

