VITTONE
STEEL FORGING SINCE 1906

DISCIPLINARE AZIENDALE RELATIVO ALL'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI MESSI A DISPOSIZIONE DEI DIPENDENTI E COLLABORATORI DALLA SOCIETÀ VITTONE S.R.L

Aggiornamento 1 del 07/04/2026

VITTONE
STEEL FORGING SINCE 1906

Premessa.

Negli ultimi anni l'organizzazione e lo svolgimento del lavoro sono stati sottoposti ad un sempre crescente processo di informatizzazione. In particolare, i servizi di rete, tra cui la posta elettronica ed *internet*, sono divenuti strumenti quotidiani indispensabili per l'esercizio delle attività lavorative.

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete *internet* dai *personal computer*, tuttavia, può esporre le aziende e gli utenti delle stesse (dipendenti e collaboratori) a rischi di natura patrimoniale, oltre a responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge.

L'uso di tali strumenti in modo non corretto, anche a seguito di comportamenti inconsapevoli, inoltre, può essere causa di gravi minacce e problemi per la sicurezza del sistema e delle informazioni in esso contenute.

Al fine di evitare che comportamenti, anche inconsapevoli, dei dipendenti e/o collaboratori possano determinare problemi o minacce alla sicurezza nel trattamento dei dati, la società Vittone S.r.l. ha adottato il presente Regolamento.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti i dipendenti e collaboratori mediante la diffusione del Modello di Organizzazione e di Gestione *ex* d. l.vo 8 giugno 2001, n. 231 e, in particolare, della parte speciale III, "*Reati informatici*".

1. Entrata in vigore del disciplinare.

Il presente disciplinare entrerà in vigore il 1° gennaio 2026.

Copia del presente disciplinare verrà consegnato a ciascun dipendente e sarà disponibile sul sito web aziendale www.vittoneforging.com.

2. Ambito di applicazione del disciplinare.

Il presente disciplinare si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda, a prescindere dal rapporto contrattuale con la stessa intrattenuto.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente o collaboratore in possesso di specifiche credenziali di autenticazione.

3. Utilizzo del *personal computer.*

La società mette a disposizione dei propri dipendenti e/o collaboratori le strumentazioni informatiche necessarie per lo svolgimento delle attività lavorative.

Il *personal computer* affidato all'utente è uno strumento di lavoro. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa può contribuire a determinare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da *password* che deve essere custodita dall'utente con la massima diligenza e non divulgata. Le *passwords* devono essere utilizzate per l'accesso alla rete, per l'accesso a qualsiasi applicazione che le preveda, per il salvaschermo e per il collegamento ad *internet*.

Non è consentito all'utente modificare le caratteristiche *hardware* e *software* impostate sul proprio *personal computer*, salvo preventiva autorizzazione da parte dell'Amministratore Delegato della società o da personale da questi incaricato.

Il *personal computer* non deve essere lasciato incustodito, deve essere spento al termine di ogni turno di lavoro, prima di lasciare gli uffici ed in caso di assenza prolungata dal posto di lavoro (oltre 15 minuti). Ogni qualvolta l'utente si allontani dalla propria postazione di lavoro, lo stesso è tenuto a chiudere la sessione (Ctrl + Alt + Canc" quindi "Blocca computer") ovvero a rendere inaccessibile a terzi l'uso del personal computer (ad es. mediante l'utilizzo di salvaschermo dotati di *password*).

L'utente può archiviare sul *personal computer* esclusivamente le informazioni necessarie all'attività lavorativa, con tassativa esclusione di qualsiasi documento o corrispondenza ad essa estranea, nonché di natura personale.

Non è consentita l'installazione di programmi diversi da quelli autorizzati dalla società.

Non è consentito all'utente modificare le caratteristiche impostate sui *personal computer* assegnati, i punti rete di accesso e le configurazioni delle reti LAN/WAN presenti nelle sedi.

Non è consentito installare autonomamente programmi provenienti dall'esterno senza la preventiva autorizzazione scritta dell'Amministrazione aziendale. È altresì vietata la riproduzione o la duplicazione di programmi informatici ai sensi delle leggi vigenti in materia.

Non è consentita l'installazione sul proprio *personal computer* di mezzi di comunicazione propri (ad es. *modem*).

L'Amministratore Delegato, o altro soggetto da questi incaricato, può in qualunque momento procedere alla rimozione di ogni *file* o applicazione che ritenga essere pericolosi per la sicurezza dei *personal computer*, del *server* e delle unità di rete.

È vietato l'uso di dispositivi di memorizzazione removibili personali. Gli utenti che necessitino, per ragioni lavorative, di utilizzare detti supporti devono farne richiesta formale all'Amministrazione della società. È fatto divieto di registrare o archiviare *files* che non riguardano l'attività lavorativa.

Non è consentito l'ascolto di programmi, *files* audio o musicali, se non ai fini prettamente lavorativi.

Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei *files* obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati.

La società rende noto che l'Amministratore Delegato, o il personale da questi incaricato della gestione e manutenzione del servizio informatico, è 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, sussiste anche in caso di assenza prolungata o impedimento dell'utente.

L'Amministratore Delegato, o il personale da questi incaricato, ha la facoltà di collegarsi e visualizzare in remoto il *desktop* delle singole postazioni dei *personal computers* 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.

4. Utilizzo della rete telematica interna aziendale.

L'accesso alla rete aziendale è consentito mediante specifiche credenziali di autentificazione.

È vietato accedere nella rete e nei programmi con un codice autentificazione utente diverso da quello assegnato.

È fatto divieto di utilizzare la rete aziendale per fini non espressamente autorizzati e non consentiti dalla legge.

È vietato connettere in rete stazioni di lavoro (*server*, *personal computer* e stampanti) o altri apparati (*router*, *switch*, *modem*, ecc.) se non dietro esplicita e formale autorizzazione dell'Amministrazione della società.

Le cartelle utenti presenti nei *server* della società sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzati per scopi diversi. Pertanto, qualunque *file* che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.

È vietata l'installazione non autorizzata di *modem* che sfruttino il sistema di comunicazione telefonico per l'accesso a banche dati esterne o interne all'azienda, salvo previa autorizzazione da parte dell'Amministrazione della società.

L'Amministratore Delegato della società, o personale da questi incaricato, può in qualunque momento procedere alla rimozione di ogni *file* o applicazione che riterrà essere pericolosi per la sicurezza, sia quelli presenti nei *personal computer*, che quelli dislocati nelle unità di rete.

5. Gestione delle *passwords.*

Le credenziali di autenticazione per l'accesso alla rete *internet* e alla rete *intranet* aziendale sono attribuite dall'Amministrazione della società, e sono strettamente personali. La *password* è sempre modificabile dall'utente.

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

La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

L'utente è tenuto a conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione/autorizzazione.

L'utente è tenuto a scollegarsi dal sistema di rete ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (*personal computer*) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima.

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

Soggetto preposto alla custodia delle credenziali di autenticazione è il Responsabile del Trattamento Privacy della società.

6. Utilizzo dei *personal computers* portatili.

L'utente è responsabile del *personal computer* portatile assegnatogli dall'azienda e deve custodirlo con diligenza, sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro.

Ai *personal computers* portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali *files* elaborati prima della riconsegna.

I *personal computers* portatili utilizzati all'esterno (convegni, visite in azienda, etc.), in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

Il portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i *files* strettamente necessari.

7. Uso della posta elettronica.

L'abilitazione alla posta elettronica deve essere preceduta da regolare autorizzazione dalla direzione della società.

Unitamente all'indirizzo delle *e-mail* viene consegnata la relativa *password*, per la quale sono applicate le condizioni di cui al precedente punto 5.

È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste *on line*, concorsi, *forum* o *mailing list*;
- la partecipazione a catene telematiche.

È fatto altresì divieto di accedere ed utilizzare la posta elettronica personale dell'utente mediante le dotazioni informatiche messe a disposizione dall'azienda, nonché di utilizzare la medesima posta elettronica personale per inviare messaggi ed informazioni di natura aziendale.

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

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 visionata od autorizzata dal responsabile dell'ufficio.

È obbligatorio porre la massima attenzione nell'aprire i *file attachements* di posta elettronica prima del loro utilizzo (non eseguire *download* di *files* eseguibili o documenti da siti *web* o *ftp* non conosciuti).

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 dall'utente.

In caso di assenza non programmata (ad es. per malattia) la procedura, qualora non possa essere attivata dal lavoratore avvalendosi del servizio *webmail* entro due giorni, verrà attivata a cura dell'azienda.

Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dall'azienda, accedere alla casella di posta elettronica in uso all'utente in ogni ipotesi in cui si renda necessario ai fini della gestione del rapporto di lavoro (ad es.: mancata attivazione della funzionalità del sistema; assenza non programmata ed impossibilità di attendere i due giorni).

L'Amministratore Delegato, o persona da esso incaricata, in caso di impossibilità di procedere come sopra indicato e di necessità di non pregiudicare la necessaria tempestività ed

efficacia dell'intervento, potrà accedere alla casella di posta elettronica al fine di garantire la sicurezza e salvaguardia del sistema, nonché per motivi tecnici o manutentivi.

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

8. Uso della rete internet e dei relativi servizi.

L'abilitazione ad *internet* deve essere preceduta da regolare autorizzazione dalla direzione della società.

Il *personal computer* abilitato alla navigazione in *internet* costituisce uno strumento aziendale necessario all'esclusivo svolgimento della propria attività lavorativa.

È assolutamente proibita la navigazione in *internet* per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

Non possono essere utilizzati *modem* (mediante linee telefoniche) per il collegamento alla rete *internet*, né abilitazioni private.

È fatto divieto all'utente di scaricare *software* gratuito (*freeware*) e *shareware* prelevato da siti *internet*, se non espressamente autorizzati dalla direzione della società.

È vietata la partecipazione a *forum* 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*), di *social network*.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa la società rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'*upload* o l'accesso a determinati siti inseriti in una *black list*.

Tutti gli accessi ad *internet* sono cronologicamente registrati e tracciati in appositi *files* (LOG), così come prevede in generale la norma in materia e le misure minime di sicurezza del C.E.D. I *files* di LOG sono sottoposti a rigide misure di protezione, anche ai fini della tutela della *privacy*.

Gli eventuali controlli, compiuti dall'Amministratore Delegato, o da persona da esso incaricata, e finalizzati a garantire la sicurezza e salvaguardia del sistema, nonché per motivi tecnici o manutentivi, 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 *files* stessi vengono conservati unicamente per il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

9. Protezione *antivirus*.

Il sistema informatico della società 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 (ad esempio, non aprire *mail* o relativi allegati sospetti, non navigare su siti non professionali etc.).

Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del *software antivirus* aziendale.

Nel caso che il *software antivirus* rilevi la presenza di un virus che non è riuscito a rimuovere, l'utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare l'accaduto all'Amministrazione della società.

Ogni dispositivo magnetico (CD, FD) di provenienza esterna all'azienda dovrà essere verificato mediante il programma *antivirus* prima del suo utilizzo e, nel caso venga rilevato un *virus* non eliminabile dal *software*, non dovrà essere utilizzato.

10. Utilizzo dei telefoni, fax e fotocopiatrici aziendali.

Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso aziendale a disposizione.

Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere chiamate, *sms* o *mms* di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. 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 dall'Amministrazione aziendale.

È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte dell'amministrazione aziendale.

È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del responsabile dell'ufficio.

11. Accesso ai dati trattati dall'utente.

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione *hardware*, etc.) o per finalità di controllo e programmazione dei costi aziendali (adesempio, verifica costi di connessione ad *internet*, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell'Amministratore Delegato, tramite l'incaricato al servizio informatico o agli addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla *privacy*, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

12. Sistemi di controlli graduali.

In caso di anomalie, l'Amministratore Delegato o il personale incaricato del servizio informatico 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 individuale potranno essere computi solo in caso di riscontrate successive ulteriori anomalie.

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

13. Osservanza della normativa aziendale.

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento.

Ove venisse accertata la violazione, da parte dell'utente, delle disposizioni di cui al presente disciplinare, il medesimo sin da ora esonera la società, e/o i soggetti operanti per conto o nell'interesse della stessa, da ogni e qualsiasi responsabilità per i danni che gli dovessero derivare dalla presa di cognizione dei suoi dati personali, illegittimamente contenuti nel *personal computer* messogli a disposizione, ovvero nella posta elettronica aziendale, ovvero nella posta elettronica personale, allorquando l'accesso alla medesima sia avvenuto mediante le dotazioni informatiche aziendali in uso all'utente stesso.

In ogni caso, il mancato rispetto o la violazione delle regole contenute nel presente disciplinare è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

14. Aggiornamento e revisione.

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dall'Amministrazione aziendale.