RONCHI

RONCHI
PACKAGING MACHINERY

CODICE ETICO INFORMATICO

INDICE

1. Premessa

La progressiva diffusione di nuove tecnologie informatiche potrebbero esporre le società del gruppo Ronchi Mario S.p.A a rischi di coinvolgimento sia patrimoniale che penale, creando al contempo problemi d'immagine e sicurezza, qualora gli strumenti informatici in dotazione vengano utilizzati in maniera scorretta o per finalità illecite.

L'accresciuta importanza delle informazioni riservate all'interno del patrimonio aziendale e il legittimo vantaggio concorrenziale che da esse deriva per l'azienda impongono a quest'ultima di dotarsi di adeguati strumenti di tutela volti a prevenire la diffusione dei dati riservati dalla quale potrebbero derivare responsabilità civili e penali per colui che viola il segreto aziendale.

A conferma di ciò, adeguandosi ai principi europei in materia, il legislatore italiano è intervenuto sull'art. 99 del Codice della Proprietà Industriale, imponendo all'azienda che intenda tutelare le proprie informazioni segrete di dotarsi di misure positive (ad esempio misure di sicurezza) atte a proteggere la segretezza delle informazioni.

In particolare, con riferimento alle misure di sicurezza imposte dal Decreto Legislativo 30 giugno 2003, n. 196, per il trattamento dei dati personali, Ronchi Mario Sp.A ha provveduto a dare idonee indicazioni ed istruzioni a tutti quegli "utenti aziendali" che, operando con strumenti informatici, sono interessati dalle predette misure. Il decreto legislativo 30 giugno 2003, n. 196 è stato successivamente integrato con le modifiche introdotte dalla L. 27 dicembre 2019 n. 160, dal D. L. 14 giugno 2019 n. 53, dal D. M. 15 marzo 2019 e dal Decreto Legislativo 10 agosto 2018,n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle Disposizioni del Reg. UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati".

Inoltre, in ottemperanza al Decreto Legislativo 8 giugno 2001, n. 231, Ronchi Mario S.p.A ha elaborato il proprio Modello di Organizzazione, Gestione e Controllo, al fine di prevenire, per quanto possibile, la commissione di illeciti da parte di amministratori, dipendenti e soggetti terzi in genere.

Considerato che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o

comportamento posto in essere nell'ambito del rapporto di lavoro, si ritiene utile adottare ulteriori regole interne di comportamento in ambito informatico, dirette ad evitare comportamenti inconsapevoli e/o scorretti.

2. Definizioni

Nel presente Codice Etico informatico determinati termini assumono un significato preciso, che per chiarezza riportiamo di seguito:

- SOCIETÀ O AZIENDA: le società del gruppo Ronchi Mario S.p.A.;
- ORGANISMO DI VIGILANZA: l'organismo di controllo di cui all'art.6, lett. B del D. Lgs. 8 giugno 2001, n.231;
- APPARECCHIATURA INFORMATICA: qualsiasi strumento utilizzato da ogni utente aziendale per l'espletamento delle proprie funzioni, a titolo esemplificativo e non esaustivo, PC, smartphone, telefoni, stampanti, ecc.;
- SISTEMA INFORMATICO: insieme di risorse, dati, applicazioni e programmi presenti su apparecchiature e supporti informatici;
- UTENTE AZIENDALE: ogni soggetto anche non dipendente della società al quale siano state assegnate una o più apparecchiature informatiche e/o sia stato abilitato all'accesso e all'utilizzo del sistema informatico aziendale.

3. Sistemi informatici aziendali

Tutte le apparecchiature informatiche, i relativi programmi e/o applicazioni, affidate agli utenti aziendali sono considerati, ai sensi dell'art. 1 -"Rapporti con l'azienda"- del CCNL Industria metalmeccanica e della installazione di impianti, strumenti di lavoro. Pertanto:

- tali strumenti vanno custoditi in modo appropriato;
- tali strumenti possono essere utilizzati solo per fini professionali (ovviamente in relazione alle mansioni assegnate) e non anche per scopi personali, tanto meno per scopi illeciti;

- non è consentito prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile dei Sistemi Informativi;
- non è consentito rimuovere i contrassegni identificativi presenti sulle apparecchiature informatiche;
- devono essere prontamente segnalati al Responsabile dei Sistemi Informativi, alla Direzione Risorse Umane ed alla propria Direzione il furto, il danneggiamento o lo smarrimento di tali strumenti. Inoltre, qualora si verifichi un furto o si smarrisca un'apparecchiatura informatica di qualsiasi tipo, l'interessato, o chi ne ha avuto consegna, entro 24 ore dal fatto, dovrà far pervenire alla Direzione Sistemi informativi l'originale della denuncia all'Autorità di Pubblica Sicurezza;
- è fatto assoluto divieto di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, con qualsiasi strumento informatico, hardware e cartaceo, documentazione e/o materiale informatico di proprietà di terzi, aventi o meno natura riservata, senza l'espresso consenso del titolare. Resta inteso che, in caso di violazione, troveranno applicazione la personale responsabilità civile e penale del dipendente, nonché le sanzioni disciplinari da parte dell'Azienda;
- è fatto assoluto divieto di trasferire all'esterno dell'Azienda e/o trasmettere file, documenti, disegni, progetti o qualsiasi altra documentazione riservata o, comunque, di proprietà della società, mediante qualsiasi strumento informatico, hardware e cartaceo, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
- è fatto assoluto divieto di mettere in condivisione su aree comuni (quali a titolo esemplificativo e non esaustivo Workspace/ cartelle di rete, ecc.) o comunque far circolare internamente, mediante qualsiasi strumento informatico, hardware e cartaceo, documenti e informazioni non pertinenti con le mansioni / attività professionali sia del destinatario che del mittente;
- non è consentita la memorizzazione sul sistema informatico aziendale di documenti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

- non è consentita la memorizzazione di documenti aziendali su supporti non autorizzati (quali a titolo esemplificativo e non esaustivo memorie mobili, chiavette USB, ecc.);
- in caso di cessazione del rapporto di lavoro per qualsiasi causa gli utenti aziendali devono riconsegnare alla Direzione Risorse Umane tutte le apparecchiature informatiche e gli strumenti di lavoro a loro assegnati nelle condizioni di utilizzo. La cancellazione dei dati registrati sulle apparecchiature informatiche e su strumenti di lavoro dovrà avvenire in presenza del Responsabile dei Sistemi Informativi ;
- in ogni momento la società si riserva la facoltà di disporre diversamente delle apparecchiature informatiche assegnate agli utenti aziendali, di chiederne la restituzione immediata e/o di eseguire controlli sugli stessi al fine di accertarne il corretto utilizzo.

4. Utilizzo delle apparecchiature informatiche

Ai fini sopra esposti, sono quindi da evitare atti o comportamenti contrastanti con le predette indicazioni come, ad esempio, quelli di seguito richiamati a titolo indicativo:

- onde evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal Responsabile dei Sistemi Informativi;
- non sono consentiti l'installazione e l'uso di programmi non autorizzati dal Responsabile dei Sistemi Informativi che valuterà il rispetto degli obblighi imposti dalla legge 22 aprile 1941, n. 633 e successive modifiche, sulla tutela giuridica del software e del diritto d'autore;
- non è consentito modificare le configurazioni impostate sulle apparecchiature informatiche senza la preventiva autorizzazione del Responsabile dei Sistemi Informativi;
- non è consentita l'installazione e/o il collegamento alle apparecchiature informatiche di periferiche aggiuntive non autorizzate dal Responsabile dei Sistemi Informativi;
- sui PC dotati di scheda audio e/o lettori CD/DVD non è consentito l'ascolto di file audio o musicali, né la visualizzazione di video e film se non a fini prettamente lavorativi. Non ne è consentito, tanto meno, il loro salvataggio sulle periferiche aziendali;

- non è consentito lasciare incustodite e/o accessibili ad altri le apparecchiature informatiche assegnate. Durante le assenze prolungate deve essere attivata la funzione di Blocco PC/apparecchiatura;
- non è consentito lasciare incustodita e/o accessibile ad altri qualsiasi apparecchiatura informatica mobile (PC portatili, PDA – smartphone, videoproiettori, telefoni mobili, ecc.) durante gli spostamenti (esempio aree di sosta, parcheggi, ecc.), trasferte (esempio: aeroporti, stazioni, etc), ovvero, durante l'assenza dall'azienda (ferie, fine settimana, notte).

5. Password

Le password che consentono l'accesso alla Rete Societaria devono essere, con riferimento alle Misure di Sicurezza imposte dal Decreto Legislativo 196 del 30 giugno 2003, riservate; ognuno ha pertanto il dovere di tutelare la loro segretezza.

Le password non devono essere comunicate ad altri, né devono essere esposti sul PC etichette e/o adesivi riportanti user-id e/o password. Le password devono essere lunghe almeno otto caratteri, non devono contenere riferimenti agevolmente riconducibili all'utente, devono essere modificate al primo accesso e cambiate almeno ogni tre mesi.

Non è in alcun modo consentito l'utilizzo di password di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto degli stessi, salvo espressa autorizzazione del Responsabile dell'utente aziendale e del Titolare della Privacy.

6. Utilizzo della rete aziendale

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi. La società si riserva la facoltà di modificare le autorizzazioni di accesso alla rete aziendale e alle relative applicazioni qualora possa essere messa in pericolo, anche solo potenzialmente, l'integrità del patrimonio informatico / informativo aziendale. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, sul sistema informatico aziendale e sulle apparecchiature

informatiche.L'accesso di ciascun dipendente a qualsiasi risorsa del sistema informatico aziendale (cartelle presenti nella rete aziendale, aree condivise, ecc.) deve essere autorizzato dal relativo Responsabile in ragione delle mansioni attribuite a ciascun dipendente; ciascun utente aziendale deve pertanto utilizzare la rete aziendale per fini strettamente riconducibili allo svolgimento della propria mansione, in conformità al contenuto dell'autorizzazione.

Ogni utente aziendale è tenuto a salvaguardare la riservatezza dei dati da lui trattati prestando particolare attenzione ai dati condivisi e alle eventuali copie cartacee dei dati elettronici, rimuovendo immediatamente i dati una volta cessata la necessità operativa; in particolare è fortemente consigliato proteggere con password qualsiasi documento memorizzato temporaneamente nelle aree di transito accessibili a tutti gli utenti aziendali. In ogni momento la società si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà pericolosi per la sicurezza del sistema, ovvero che siano stati acquisiti e/o installati in violazione del presente Codice Etico Informatico; in particolare la società si riserva la facoltà di cancellare i dati salvati nelle aree di transito comuni a tutti gli utenti aziendali entro le 24 ore successive al salvataggio.

Non è consentito installare ed utilizzare strumenti software e/o hardware atti ad intercettare conversazioni (in qualsiasi forma, telefonica, sms, e-mail, ecc.) e falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici aziendali.

Non è consentito collegare alla rete aziendale PC o altre apparecchiature informatiche non di proprietà della società, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi.

7. Utilizzo della rete internet e dei relativi servizi

La società fornisce, limitatamente agli utenti aziendali che ne hanno necessità, l'accesso alla Rete Internet tramite le postazioni di lavoro di propria competenza. La connessione ad Internet deve essere mantenuta per il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento. Pertanto:

- non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;

- non sono consentiti il download e la memorizzazione di documenti non autorizzati e comunque di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- non è consentita l'effettuazione di ogni genere di transazione finanziaria, comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi previsti dalle procedure di acquisto aziendali;
- non è consentito il download di qualsiasi tipo di software prelevato da siti Internet, se non espressamente autorizzato dal Responsabile dei Sistemi Informativi;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa; non è permesso l'utilizzo e la consultazione, per motivi non professionali, di servizi quali forum, social network, chat-line, newsgroup, bacheche elettroniche o simili e le registrazioni in guest book, neanche utilizzando pseudonimi (nickname);
- non è permesso iscriversi a forum, chat-line, blog, newsletter o siti internet legati all'attività di lavoro, con indirizzo e-mail aziendale, salvo specifica e preventiva autorizzazione del proprio Responsabile.

Ognuno è, in ogni caso, direttamente responsabile del corretto e lecito utilizzo dell'e-mail aziendale, nonché del contenuto delle dichiarazione e informazioni trasmesse; l'unico tipo di connessione Internet consentita è quella tramite rete aziendale; non sono quindi autorizzate in azienda connessioni diverse quali ad esempio quelle che utilizzano le linee telefoniche in dotazione; in ogni momento la società si riserva la facoltà di attivare dei filtri alla navigazione Internet, impedendo l'accesso a siti non pertinenti all'attività lavorativa, ritenuti pericolosi o che potenzialmente potrebbero determinare una violazione del Modello di Organizzazione Gestione e Controllo ("Modello 231") adottato dalla società.

8. Utilizzo della posta elettronica

La società fornisce, limitatamente agli utenti aziendali identificati per mansione e ruolo, una Casella di Posta Elettronica nominale ed univocamente assegnata. Anche la Posta Elettronica è uno strumento di lavoro messo a disposizione per svolgere le attività legate alle mansioni assegnate,

pertanto l'indirizzo attribuito agli utenti aziendali è personale ma non privato. Ognuno è direttamente responsabile, disciplinarmente e giuridicamente, del contenuto della propria Casella di Posta e dei messaggi inviati.

Si ritiene utile segnalare che:

- non è consentito utilizzare la Posta Elettronica, interna ed esterna, per motivi non attinenti allo svolgimento delle mansioni assegnate;
- non è consentito inviare o memorizzare messaggi, interni ed esterni, di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- ogni comunicazione esterna, inviata o ricevuta, potrebbe essere condivisa e visionata all'interno dell'azienda;
- non è consentito l'utilizzo della Posta Elettronica di altri utenti aziendali per l'invio di comunicazioni a proprio nome o in nome di questi, salvo espressa autorizzazione dei medesimi; in caso di assenza l'utente aziendale ha l'obbligo di attivare, dall'ufficio o da remoto, un messaggio di risposta automatica di "fuori sede" con indicata la persona di riferimento da contattare in caso di urgenza e le sue coordinate elettroniche e/o telefoniche. Il messaggio di "Fuori Sede" deve essere attivato sia per i mittenti interni che per quelli esterni all'azienda;
- il personale dell'ufficio Sistemi Informativi, in qualità di "fiduciario", potrà accedere alla casella di posta elettronica degli utenti aziendali assenti e visionare i messaggi necessari nel rispetto delle garanzie previste dalla normativa in materia di tutela della Privacy e secondo le circostanze descritte nella procedura di dettaglio;
- le caselle di posta elettronica individuali vengono create e assegnate senza configurazione di alcuna condivisione e/o regola. Ogni utente aziendale è pertanto responsabile di ogni eventuale condivisione e/o regola applicate alla sua casella di Posta Elettronica;
- non è consentito creare, consultare, utilizzare caselle di Posta Elettronica private;
- la società ha comunque reso disponibili alcuni indirizzi condivisi da più utenti aziendali rendendo chiara la natura non privata della corrispondenza. Tali indirizzi corrispondono generalmente a caselle di Direzione o caselle di Servizio. Tutte le comunicazioni esterne, inviate o ricevute tramite questi indirizzi, potranno essere archiviate.

9. Controlli

La società si riserva la facoltà di procedere periodicamente, secondo le garanzie previste dalla normativa in materia di tutela della Privacy e di diritto del lavoro, a controlli sulle apparecchiature informatiche aziendali assegnate (compresi i telefoni mobili), sull'utilizzo delle stesse e dei relativi programmi e/o applicazioni, allo scopo di rilevare la presenza di virus informatici e di garantire l'integrità e la sicurezza del sistema, nonché il loro corretto utilizzo, oltre a contrastare eventuali comportamenti che potrebbero mettere a rischio l'integrità del patrimonio aziendale.

La società si riserva la facoltà di disporre, secondo le garanzie previste dalla normativa in materia di tutela della Privacy e di diritto del lavoro, controlli specifici, non sistematici, sull'utilizzo della Posta Elettronica e di Internet, attraverso analisi di dati aggregati, allo scopo di verificare il corretto utilizzo dei servizi e contrastare eventuali comportamenti che potrebbero mettere a rischio l'integrità del patrimonio aziendale. Qualora un dipendente sia stato abilitato ad accedere a determinate informazioni del sistema informatico aziendale, detta autorizzazione deve intendersi strettamente limitata all'esercizio delle proprie mansioni coerentemente con quanto indicato nei moduli autorizzativi preventivamente rilasciati. La società potrà effettuare controlli periodici, ma non sistematici, sui profili degli utenti aziendali, al fine di verificare le modalità di accesso e di gestione dei dati aziendali, nonché la coerenza tra le mansioni attribuite, il profilo assegnato e le autorizzazioni, individuando eventuali comportamenti che potrebbero mettere a rischio l'integrità del patrimonio aziendale. I dati analizzati durante tali controlli non vengono automaticamente né sistematicamente associati a utenti aziendali identificati, ma per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con altri dati, permettere di identificare gli utenti aziendali.

Qualora siano accertate violazioni dei profili autorizzativi di accesso ai dati aziendali, la società sarà legittimata ad adottare gli opportuni provvedimenti a propria tutela, costituendo dette violazioni grave inadempimento della legge e del contratto di lavoro.I dati Internet vengono utilizzati al solo fine di ricavare informazioni statistiche sull'uso dei siti nonché per controllarne periodicamente il corretto utilizzo e vengono conservati per un periodo di tempo limitato. Tutti i dati in questione potrebbero essere utilizzati per l'accertamento di responsabilità in caso di eventuali reati informatici ai danni della società, nonché in caso di contenziosi legali.

Vi invitiamo a segnalare eventuali violazioni al suddetto Codice Etico Informatico di cui venite a conoscenza. Le vostre segnalazioni potranno essere inviate :

- tramite mail all'indirizzo e-mail:odv@ronchi.it;
- tramite posta all'attenzione dell'Odv di Ronchi Mario S.p.A, via Italia 43, Gessate (MI).

10. Inosservanza delle disposizioni e delle sanzioni

Il mancato rispetto delle disposizioni contenute nel presente Codice Etico Informatico potrà costituire oggetto di valutazione sotto l'aspetto disciplinare con l'applicazione di provvedimenti quali richiami, multe, ammonizioni scritte, sospensione dal lavoro fino a tre giorni e licenziamento, nonché sotto l'aspetto giudiziario. La società potrà rivalendosi sui responsabili degli eventuali danni derivanti da un uso non diligente o non conforme alle norme contenute nel presente Codice Etico Informatico.Ai sensi del Codice civile e del CCNL Industria Metalmeccanica e della installazione di impianti, gli utenti aziendali potranno essere chiamati a rispondere, anche sotto l'aspetto disciplinare, del furto, dello smarrimento e degli eventuali danni alle apparecchiature informatiche imputabili ad un uso non diligente delle stesse; il relativo ammontare dei danni potrà inoltre essere addebitato tramite cedolino paga.

Rev.	Descrizione revisione	Preparazione	Verifica	Approvazione
00	Prima emissione 24/11/2021	Sistemi Informativi	HR	A.D.
		Diego Tressoldi	Giuseppina Pennisi	Gianmario Ronchi