

Regolamento aziendale Sotacarbo SpA

REGOLAMENTO SULL'UTILIZZO DEGLI STRUMENTI INFORMATICI, TELEMATICI E DI POSTA ELETTRONICA

1. Finalità

1. Il presente regolamento definisce le procedure specifiche per l'uso dei sistemi informatici aziendali, della posta elettronica e dell'accesso a internet, anche in ottemperanza a quanto previsto dal Regolamento (UE) 2016/679, dal D.Lgs. 196/2003 e ss.mm.ii. "Codice in materia di protezione dei dati personali", dalla Deliberazione n. 13 del 01/03/2007 del Garante per la protezione dei dati personali "Linee guida per posta elettronica e internet" (con i chiarimenti e le integrazioni forniti dal Garante successivamente all'entrata in vigore del GDPR), dalla L. 81/2017 in materia di lavoro agile e dalle misure tecniche e organizzative richieste dall'art. 32 del GDPR e dalla Direttiva n. 2/09 del 26/05/2009 della Presidenza del Consiglio dei ministri "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro". In merito all'uso corretto degli strumenti informatici da parte dei lavoratori ed alle modalità di controllo da parte dei datori di lavoro.
2. Tali procedure, diffuse tra i dipendenti della Società con il seguente regolamento interno, hanno lo scopo di ridurre i rischi di natura patrimoniale, di danno d'immagine della Società nonché di incorrere in responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge. Le regole che disciplinano l'utilizzo delle risorse informatiche e telematiche si ispirano ai principi della diligenza e della correttezza. Per quanto non espressamente indicato, si rimanda alla normativa specifica in materia.

2. Destinatari

Il regolamento deve essere osservato da tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché da tutti i collaboratori della Società, a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, in stage, ecc.).

3. Utilizzo del personal computer e internet

1. Il Personal Computer affidato al dipendente è uno strumento di lavoro; pertanto, ogni utilizzo non inerente all'attività lavorativa è vietato, poiché può causare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. È assolutamente proibita la navigazione su Internet per motivi personali e per quelli diversi da quelli strettamente legati all'attività lavorativa.
2. Il personal computer deve essere custodito con cura, evitando ogni forma di danneggiamento. L'addetto alla gestione dei sistemi informatici, sotto indicazione del DPO, ha la facoltà di collegarsi, in presenza dell'utente, alle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc.
3. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dall'addetto alla gestione dei sistemi informatici per conto della Società 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.

4. Salvo autorizzazione dell'addetto alla gestione dei sistemi informatici, 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.).
5. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'addetto alla gestione dei sistemi informatici nel caso in cui siano stati rilevati virus.
6. 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, salvo disposizioni e/o richieste specifiche da parte dell'addetto ai sistemi informatici. In ogni caso i computer devono essere bloccati quando le postazioni di lavoro non sono occupate.
7. Qualora, l'utente sia dotato di un PC portatile, egli è responsabile di custodirlo con diligenza sia se l'utilizzo avviene fuori sede sia durante l'utilizzo nel luogo di lavoro.
8. I PC portatili utilizzati nelle missioni, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.
9. Tutti i supporti magnetici rimovibili (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.
10. I supporti magnetici contenenti dati relativi a persone fisiche devono essere adeguatamente custoditi dagli utenti in armadi chiusi.
11. È vietato l'utilizzo di supporti rimovibili personali.
12. Per motivi di sicurezza del sistema informatico, per motivi tecnici e/o manutentivi e per finalità di controllo e programmazione dei costi aziendali, il legale rappresentante può richiedere all'addetto alla gestione dei sistemi informatici l'accesso agli strumenti informatici aziendali e ai documenti ivi contenuti, comunque estraneo a qualsiasi finalità di controllo dell'attività lavorativa. Tale accesso avviene nel rispetto dell'art. 4 della L. 300/1970 e previa adeguata informativa ai lavoratori nelle forme previste dall'art. 4, comma 3, L. 300/1970. I controlli c.d. 'difensivi' in senso stretto, diretti ad accertare specifiche condotte illecite di singoli dipendenti sulla base di concreti indizi, avvengono nel rispetto delle medesime garanzie. L'azienda, inoltre, informa i dipendenti che gli strumenti informatici assegnati (PC, posta elettronica, accessi di rete, badge) possono generare dati e log registrati dai sistemi. Tali dati potranno essere utilizzati, in conformità all'art. 4, co. 3, L. 300/1970, per tutti i fini connessi al rapporto di lavoro. L'installazione di strumenti dai quali derivi anche la possibilità di controllo a distanza avverrà previo accordo con le RSU/RSA o, in mancanza, previa autorizzazione dell'Ispettorato Nazionale del Lavoro, ai sensi dell'art. 4, co. 1, St. Lav.
13. La prestazione lavorativa in modalità smart working (lavoro agile) dev'essere svolta possibilmente attraverso dispositivi portatili aziendali, laddove questo non sia possibile, il dipendente svolgerà tali attività utilizzando un proprio dispositivo, loggandosi però con le proprie credenziali di accesso al portale Microsoft 365. Nel caso di utilizzo di dispositivi personali, il dipendente è tenuto a rispettare tutte le misure di sicurezza previste dal presente regolamento ai sensi della L. 81/2017 e dell'art. 12 del D.Lgs. 82/2005 come modificato dal D.L. 76/2020. Al dipendente verrà inoltre consegnata l'apposita informativa sindacale.

14. L'utilizzo di sistemi di Intelligenza Artificiale Generativa su dispositivi aziendali o tramite credenziali aziendali è disciplinato dal 'Regolamento per l'utilizzo aziendale dell'Intelligenza Artificiale Generativa', adottato contestualmente al presente regolamento e da intendersi quale parte integrante dello stesso. È fatto divieto assoluto di accedere, tramite dispositivi aziendali o credenziali aziendali, a strumenti di IA classificati in Categoria Rossa (Vietati) ai sensi del predetto regolamento.

15. RegISTRAZIONI di sistema e conservazione dei log: il sistema in cloud utilizzato “Microsoft 365 Business” registra l’attività relativa all’utilizzo dei singoli applicativi in modo anonimo mediante pseudonimizzazione. I dati raccolti riguardano la percentuale di utilizzo delle singole applicazioni, al fine di ottimizzarne l’uso, e vengono conservati per un massimo di 180 giorni. Tali dati possono essere consultati esclusivamente dagli amministratori del sistema 365. Non vengono registrati log di navigazione, di accesso alla rete e metadati delle mail.

4. Gestione delle credenziali di accesso

1. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dall’addetto alla gestione dei sistemi informatici, previa formale richiesta del responsabile d'area, nell'ambito del quale verrà inserito e opererà il nuovo utente, e non possono essere cedute ad altri soggetti.
2. Nel caso di tirocinanti, stagisti e collaboratori esterni, la preventiva richiesta, se necessaria, verrà inoltrata direttamente dal responsabile dell'unità operativa con il quale il collaboratore si coordina nell'espletamento del proprio incarico.
3. Le credenziali di autenticazione per il personal computer consistono in un codice per l'identificazione dell'utente (user id) associato ad una password riservata che dovrà venir custodita dall'autorizzato con la massima diligenza e non divulgata. Le password dovranno avere una lunghezza minima di 8 caratteri, dovrà essere composta da almeno un numero, una lettera maiuscola, una minuscola e dove possibile un carattere speciale (per esempio: £, \$, %, @, &, ecc.), dovranno essere cambiate ogni 6 mesi e conservate in luogo sicuro
4. Le credenziali di autenticazione per il sistema ZUCCHETTI consistono in una user id e una password.
5. Le password non possono essere lasciate su note adesive attaccate sopra o sotto un computer, né possono essere lasciate per iscritto su una postazione accessibile.
6. Le credenziali di accesso alla rete Wi-Fi aziendale sono riservate ai soli dipendenti (tempo determinato e indeterminato) della Società e non possono essere cedute a terzi.
7. Verrà consegnato a ciascun utente il personale badge di accesso al centro ricerche da parte del responsabile della gestione del centro, che dovrà essere conservata con cura e non diffusa a persone terze.

5. Uso della posta elettronica

1. La casella di posta elettronica assegnata all'utente è uno strumento di lavoro finalizzato allo scambio di informazioni nell’ambito dell’attività lavorativa.
2. Le caselle aziendali associate al dominio “sotacarbo.it” sono di proprietà della Società, che ne concede l’uso ai dipendenti secondo le norme indicate nel presente Regolamento; i dipendenti assegnatari sono responsabili del loro uso conforme e corretto.

3. Le comunicazioni via posta elettronica devono avere un contenuto espresso in modo professionale e corretto, nel rispetto della normativa vigente.
4. Le comunicazioni in uscita devono essere 'firmate' inserendo in calce al documento la firma assegnata a ciascun utente.
5. I messaggi di posta elettronica devono contenere il seguente avvertimento ai destinatari *"The SOTACARBO. The company shareholders, directors and management accept no responsibility and accordingly shall have no liability to any party whatsoever with respect to the contents of this message. This message (including any attachments) is intended only for the use of the addressee(s) named above. It may contain information that is PRIVILEGED and CONFIDENTIAL and should not be read, copied or otherwise used by any other person. If you are not the intended recipient, you are hereby notified that any use, retention, disclosure, copying, printing, forwarding or dissemination of this communication is strictly prohibited. If you have received this communication in error, please erase all copies of the message and its attachments and notify us immediately."*
6. Ogni assegnatario deve consultare la propria casella con frequenza giornaliera, salvo casi di assenza dal lavoro; tale casella può, comunque, essere consultata dal dipendente titolare della stessa tramite accesso pubblico al di fuori della rete aziendale.
7. Nel caso di assenza dal lavoro prolungata e programmata, il dipendente deve attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti, indicando nel messaggio di accompagnamento ogni riferimento utile per contattare la struttura organizzativa competente.
8. Nei casi di assenza non programmata o di impossibilità, temporanea o protratta nel tempo, se non è possibile attivare la procedura sopra citata, per garantire l'ordinaria operatività aziendale, il dipendente deve delegare ad un collega a sua scelta ("fiduciario") il compito di verificare il contenuto dei messaggi e di inoltrare al Responsabile del gruppo di lavoro in cui opera quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. In questo caso, il Responsabile del gruppo di lavoro deve informare il dipendente appena possibile, fornendo un'adeguata spiegazione e riportando l'evento in apposito verbale.
9. Nel caso in cui si debba inviare un documento all'esterno della Società, è preferibile utilizzare un formato protetto dalla scrittura (ad esempio, il formato Acrobat *.pdf).
10. Nel caso di invio di allegati "pesanti", utilizzare i formati compressi (*.zip, *.7z, *.rar). Laddove sia invece necessario inviare un documento contenente dati personali, è obbligatoria la creazione di un file protetto da password (nel caso di più documenti, creare una cartella compressa, anch'essa protetta da password). La password deve essere comunicata con un altro idoneo strumento (per es. Sms, ulteriore e-mail etc.). Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus informatici, occorrerà cancellare i messaggi senza aprirli. Analogamente, messaggi provenienti da mittenti conosciuti che contengono allegati sospetti (file con estensione .exe, .scr, .pif, .bat, e .cmd) non devono essere aperti. Va evitata la diffusione incontrollata di sistemi per propagare messaggi a diffusione capillare e moltiplicata che inducono il destinatario a produrne molteplici copie da spedire, a propria volta, a nuovi destinatari, in quanto limitano l'efficienza del sistema di posta. L'iscrizione alle mailing list esterne è concessa solo per motivi professionali. Prima di iscriversi occorre verificare in anticipo se il sito è affidabile.
11. È vietato l'utilizzo dell'indirizzo mail aziendale per l'iscrizione a qualsiasi servizio on line (social network, gruppi di discussione, servizi telefonici, bancari, assicurativi di tipo personale etc.) che non sia strettamente correlato alla propria attività istituzionale.
12. La casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili e, soprattutto, allegati ingombranti, o salvandoli in un'apposita cartella di servizio creata sul

proprio PC: il dipendente ha il dovere di verificare periodicamente lo spazio a disposizione nella propria casella di posta, evitando così di non ricevere messaggi per mancanza di spazio disponibile. Per la trasmissione di file tramite posta elettronica, bisogna prestare attenzione alle dimensioni degli allegati, che non devono superare i 20 MB.

Sulla base delle indicazioni sin qui riportate, gli utilizzatori di una casella pubblica di posta sul dominio sotacarbo.it devono attenersi alle seguenti regole:

- non utilizzare l'indirizzo mail aziendale per comunicazioni personali;
- utilizzare sempre un linguaggio appropriato e rispettoso;
- rispondere all'eventuale richiesta del mittente di conferma di lettura del messaggio;
- non inviare messaggi che possano danneggiare la reputazione e l'immagine della Società;
- non inviare comunicazioni che siano diffamatorie, oscene, pornografiche, offensive, tali da recare danno o che possano essere considerate da altre fonti di molestie o discriminazione religiosa, sessuale, razziale, politica o sindacale;
- non utilizzare il campo cc e ccn a "cascata" per mettere in copia destinatari non strettamente attinenti all'oggetto della comunicazione;
- in caso di comunicazioni con operatori economici preliminari a una richiesta d'acquisto, cosiddette indagini preliminari di mercato, riportare in oggetto "Indagine esplorativa informale" e nel testo la premessa "si informa che la presente non costituisce in alcun modo una richiesta d'offerta, ma una richiesta di collaborazione ad una mera indagine esplorativa informale, volta a ..." così come stabilito dal Regolamento acquisti.

13. Le caselle di posta elettronica in uso ai dipendenti vengono disattivate al momento della cessazione del rapporto di lavoro, come previsto dalla normativa vigente.

14. I libri, le scritture e la documentazione obbligatoria tenuta con strumenti informatici sono soggetti alle disposizioni dell'art. 2215-bis c.c. I documenti destinati a produrre effetti giuridici verso l'esterno devono essere sottoscritti con firma digitale qualificata o con altra firma elettronica avanzata, secondo le disposizioni del Codice dell'Amministrazione Digitale (D.Lgs. 82/2005).

6. Non osservanza della normativa societaria

La mancata adozione, da parte dei dipendenti, delle misure indicate in questo regolamento li espone a provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, nonché, laddove ricorrano gli estremi, alla segnalazione alle autorità competenti per tutte le azioni civili e penali consentite.

7. Coordinamento con gli altri regolamenti

Il presente regolamento si intende da applicarsi coordinatamente con il *Regolamento per l'utilizzo aziendale dell'intelligenza artificiale generativa (GenAI)* in merito alla disciplina di utilizzo dei sistemi IA di cui al punto 14 dell'articolo 3 del presente regolamento.

8. Aggiornamento

Il presente regolamento verrà aggiornato laddove dovessero subentrare aggiornamenti di carattere normativo o tecnologico, o che comportino modifiche sostanziali alle procedure e alle misure in esso indicate. Tale aggiornamento sarà a cura del DPO in coordinamento con quanti altri possano essere coinvolti.

9. Entrata in vigore

Il presente regolamento entra in vigore con la pubblicazione sul sito web aziendale.

Carbonia, 31/07/2026

Ing. Mario Porcu
Amministratore Unico Sotacarbo SpA