Protocollo per l'utilizzo delle risorse informatiche (regolamento informatico)

Approvato dal Consiglio di Amministrazione di SO.RI il 29.03.2024

Allegato **C** al Modello di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 Giugno 2001 n° 231

In vigore dal:
29.03.2024
Precedenti versioni:
Rev. 1 - Delibera del C.D.A del 19/07/2012

Sommario

1) PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer e l'accesso a banche dati esterne, può esporre l' azienda ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'azienda stessa.

L'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo di SO.RI Spa è ispirato al principio della diligenza e correttezza, comportamenti che il dipendente è sempre tenuto ad adottare nell'ambito del rapporto di lavoro e conseguentemente ogni utilizzo delle apparecchiature, degli elaboratori, delle reti e dei dati diversi dalle finalità strettamente professionali è espressamente vietato.

Con l'entrata in vigore, dal 25 maggio 2018, del Regolamento Europeo n.679/2016 (c.d. GDPR) in materia di trattamento dei dati personali ed ai nuovi principi in materia di Privacy, SO.RI assume la veste di titolare del trattamento (ossia di tutte quelle operazioni che saranno eseguite sui dati personali a partire dalla raccolta del dato sino alla cessazione) di dati personali rispetto ai quali la stessa è tenuta ad effettuare un uso ispirato ai vigenti principi di liceità, correttezza e trasparenza, a cui si aggiungono quelli di pertinenza, completezza e non eccedenza.

In adempimento alle disposizioni di cui al GDPR l'Azienda si è dotata del DPIA (Data Protection Impact Assisment) ossia del documento di valutazione dei rischi insiti nel trattamento in concreto realizzato da SO.RI e delle conseguenti misure adottate allo scopo di abbattere o elidere drasticamente il rischio qualificato di perdita accidentale e/o intrusione da parte di terzi e/o indebita diffusione e/o modifica, perdita del dato personale (c.d. Data Breach).

Poiché anche nella normale attività lavorativa alcuni comportamenti possono mettere a rischio la sicurezza dei dati trattati e l'immagine dell'Azienda, di seguito vengono richiamate semplici regole comportamentali finalizzate non tanto a censurare comportamenti consapevolmente scorretti, già di per sé proibiti, ma soprattutto per evitare condotte che inconsapevolmente possano causare rischi alla sicurezza ed alla integrità dei sistemi informativi aziendali.

Si rammenta che le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito fra i sistemi della rete locale, anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

L'Azienda, pertanto, predispone regolari momenti formativi ed informativi per garantire a tutti i dipendenti il massimo aggiornamento in merito ai rischi, alle procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati.

In particolare si ricorda a tutti i dipendenti che il D.Lgs 231/2001 prevede specifici reati:

- in materia informatica che fanno capo all'art. 24-bis del D.Lgs 231/2001 "Delitti informatici e trattamento illecito di dati";
- in materia di diritto d'autore che fanno capo all'art. 25 novies "Reati in materia di violazione del diritto di autore";
- in materia di pornografia che fanno capo all'art. 25 quinquies "Delitti contro la personalità individuale".

Le categorie di reati sopra indicate contemplano singole fattispecie che connesse alla criminalità informatica.

Il presente documento recepisce e si integra con le disposizioni di cui agli artt. 14 "Utilizzo delle tecnologie informatiche" e 15 "Utilizzo dei mezzi d'informazione e dei social media" di cui al Codice di Comportamento, adeguato alle modifiche introdotte dal D.P.R. 13/06/2023 n. 81.

2) AMBITO DI APPLICAZIONE

Il presente protocollo si applica a tutti gli utenti interni che sono autorizzati ad accedere alle risorse informatiche aziendali di SO.RI.

Per utenti interni si intendono gli amministratori, i soggetti apicali, i dipendenti a tempo indeterminato e determinato, i collaboratori coordinati e continuativi e il personale con altre forme di rapporto di lavoro.

3) UTILIZZO DEL PERSONAL COMPUTER E DELLA RETE AZIENDALE

Il personal computer, fornito in dotazione all'utente, è uno strumento di lavoro e il suo utilizzo deve essere finalizzato esclusivamente allo svolgimento delle attività professionali e aziendali.

Ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e tali da ridurre i rischi per la sicurezza del sistema informatico.

In particolare è fatto divieto di installare sulla strumentazione in uso hardware fisso o removibile (quali supporti esterni, modem…).

Qualora si rendessero necessarie modifiche alle configurazioni impostate sul pc in uso, occorre darne comunicazione all'Amministratore di Sistema (in SO.RI tale ruolo è rivestito dal CED del Comune di Prato).

Sul pc in uso non devono essere installati programmi che non siano ufficialmente forniti dalla società.

E' tassativamente proibito installare programmi provenienti dall'esterno, scaricati da internet (anche in versione freeware) o installati tramite chiavi USB esterne o in qualsivoglia altro formato, se non con l'autorizzazione esplicita dell'Amministratore del Sistema (in quanto l'utilizzo di software non regolarmente acquistato dall'Azienda può configurare un reato), anche in considerazione del grave pericolo di contrarre virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

E' tassativamente proibito utilizzare cloud esterni diversi tra cui (es. Dropbox, Google drive, ecc.)

La società peraltro ricorda all'utilizzatore che l'illecita duplicazione o riproduzione di software costituisce illecito ed è punita ai sensi della legge 633/1941 come novellata.

Costituisce buona regola utilizzare nel proprio lavoro solo archivi di rete su percorsi condivisi, limitando l'uso dei dischi locali solo ai documenti strettamente necessari; le unità di rete sono aree di condivisione d'informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità sono svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore del Sistema.

In qualunque momento l'Amministratore di Sistema può disporre di procedere alla rimozione di ogni file o applicazione che riterrà pericolosi per la sicurezza o non inerenti all'attività lavorativa sia sui computer degli incaricati sia sulle unità di rete.

Inoltre costituisce buona regola la periodica pulizia degli archivi locali, tramite eliminazione dei file non più utili o duplicati, previo eventuale salvataggio dei documenti archiviati secondo le indicazioni fornite dalla società con gli strumenti resi noti e poi rimessi all'amministratore di sistema.

E' assolutamente da evitare un'archiviazione ridondante che non consenta in modo chiaro ed inequivocabile l'identificazione dello stato di revisione di un documento.

L'elaboratore deve essere spento ogni sera prima di lasciare gli uffici (salvo diverse disposizioni o in caso di particolare necessità). Durante la pausa pranzo ed ogni volta che ci si allontana per lunghi periodi dalla propria postazione, è consigliato il salvataggio e la chiusura di tutti i file aperti, per non ostacolare eventuali attività dell'Amministratore di sistema, nonché l'attivazione dello screen saver protetta da password; è evidente che 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. Non sono ammesse condotte atte ad aggirare tale misura di sicurezza. Tutti i supporti magnetici riutilizzabili (CD-Rom, DVD, cassette) contenenti dati sensibili devono essere trattati con particolare cautela. Una persona esperta potrebbe recuperare i dati memorizzati anche dopo la loro cancellazione. Per questo motivo il supporto, al termine dell'utilizzo, deve essere distrutto fisicamente salvo che il suo riutilizzo non si ritenga assolutamente sicuro.

È fatto divieto di fare copia dei dati presenti sul sistema informativo aziendale e di utilizzare dati al di fuori dei locali aziendali.

Tutti i dipendenti avranno cura di eseguire la stampa dei dati solo se strettamente necessaria e di ritirarla immediatamente dai vassoi delle stampanti comuni.

I fornitori esterni, addetti alla manutenzione di hardware, software e reti, operano in conformità alle presenti istruzioni, sotto la sorveglianza dell'Amministratore del Sistema.

Ogni malfunzionamento o danneggiamento del personal computer deve essere tempestivamente comunicato al responsabile del servizio informatico aziendale-CED.

4) GESTIONE DELLE PASSWORD

Ad ogni dipendente è fornito un badge personale che consente l'accesso ai locali aziendali, la registrazione delle entrate e delle uscite dal lavoro e l'accesso al personal computer.

Per l'accesso al personal computer tramite badge personale è prevista una user-id ed una password inizialmente fornita dall'amministratore di sistema e quindi modificabile dall'utente.

Il badge è strettamente personale ed eventuali smarrimenti devono essere denunciati immediatamente agli organi competenti.

In base alle autorizzazioni fornite dalla Direzione di SO.RI, responsabile del trattamento dei dati, ciascun dipendente accede alle procedure assegnate sempre tramite chiave di autenticazione (user ID/password) fornita inizialmente dall'amministratore di sistema.

La parola chiave o password, deve essere custodita dall'incaricato con la massima diligenza, non deve essere divulgata, non deve contenere riferimenti facilmente riconducibili all'utilizzatore. La stessa deve essere cambiata al suo primo utilizzo e, successivamente dopo 90 gg. (computer inattivo) o 180 gg (computer attivo), come previsto dalla normativa privacy, sarà disabilitata automaticamente dal sistema. Qualora l'intestatario della password ritenga che un soggetto non autorizzato possa essere venuto a conoscenza della propria password, dovrà provvedere immediatamente a comunicarlo al titolare.

I requisiti minimi di complessità della password sulla base della vigente normativa privacy sono:

- Redazione con caratteri maiuscoli e/o minuscoli;
- Composizione con inclusione di numeri e lettere;
- Caratteri non inferiori ad 8 (ad eccezione dei sistemi operativi che non supportano tali requisiti);
- Password non agevolmente riconducibile all'identità del soggetto che la gestisce.

In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo che informatico.

5) UTILIZZO DELLA POSTA ELETTRONICA

L'utilizzo della posta elettronica interna contribuisce fortemente a rendere la comunicazione tempestiva, efficace ed economica. Il rispetto di alcune semplici regole può aiutare a migliorare ulteriormente l'utilizzo dello strumento.

Le caselle di posta elettronica date in uso al dipendente sono destinate esclusivamente ad un utilizzo di tipo aziendale.

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Si rappresenta che:

- è fatto divieto di utilizzare le caselle di posta elettronica aziendale nome.cognome@so-ri.it per l'invio di messaggi personali o per la partecipazione a dibattiti, forum, newsletter o mail list non attinenti l'attività lavorativa;
- 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, o che costituiscano comunque condotta illecita;
- la casella di posta personale deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti;
- è buona norma compilare sempre il soggetto mittente ed evitare messaggi estranei al rapporto di lavoro;
- è possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario;
- per le comunicazioni ufficiali verso tutti gli interlocutori aziendali (utenti, sindacati, comuni, ecc.) è comunque obbligatorio avvalersi degli strumenti tradizionali quali posta e fax utilizzando il protocollo aziendale in uscita;
- in caso di assenza programmata è onere dell'utente richiedere reindirizzamento a collega;
- è fatto divieto di divulgare notizie, dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto cui sono tenuti gli utenti in ottemperanza agli obblighi di fedeltà e correttezza.

Tutte le caselle di posta aziendale assegnate al personale sono caselle di posta certificata PEC e quindi autorizzate ad inviare comunicazioni ufficiali destinate ad altre caselle di posta certificata.

Sarà responsabile del mittente, in base alla natura della comunicazione e del destinatario, quando sprovvisto di indirizzo PEC, valutare la necessità di protocollare la comunicazione inviata a mezzo email.

Le disposizioni di questo paragrafo si integrano con le disposizioni previste dal Codice di Comportamento all'art. 14 "Utilizzo delle tecnologie informatiche".

6) UTILIZZO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

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

L'utilizzo degli strumenti per la navigazione su Internet è sottoposto ad un sistema attivo di controllo.

Quindi:

- è vietata la navigazione in siti internet non direttamente attinenti l'attività professionale ed in particolare con contenuti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita;
- è fatto divieto l'acquisizione (download) di programmi software, anche gratuiti, che non abbiano avuto esplicita autorizzazione dell'Amministratore di Sistema;
- è tassativamente proibita l'effettuazione di ogni genere di transazione finanziaria, acquisti on-line e simili, salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure aziendali;
- è vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e la registrazione in guest books anche utilizzando pseudonimi (o nicknames) e, più in generale, qualunque utilizzo di servizi Internet, attuali o futuri, non connessi all'attività istituzionale dell'Azienda, salvo che questi siano preventivamente autorizzati dalla Direzione;
- è fatto divieto all'Utente cedere il controllo del pc a server esterni (a titolo esemplificativo e non esaustivo: e-mule, peer to peer, skype, ecc.).

  Le disposizioni di questo paragrafo si integrano con le disposizioni previste dal Codice di Comportamento all'art. 15 "Utilizzo dei mezzi d'informazione e dei social media".

  Eventuali attivazioni di controlli specifici saranno preventivamente comunicati; resta inteso che in caso di anomalie, l'Azienda potrà effettuare verifiche dirette a fini di monitoraggio e controllo delle risorse informatiche, che potranno incidentalmente consentire la conoscibilità dei log di connessione relativi anche ad una sola postazione.

7) LINEE GUIDA PER LA PREVENZIONE DEI VIRUS

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi.

Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Come prevenire i virus:

- **INSTALLANDO SOLTANTO PROGRAMMI AUTORIZZATI DALL'AMMINISTRATORE DI SISTEMA**
- **ESEGUIRE LA SCANSIONE ANTIVIRUS DEI FILE DI PROVENIENZA ESTERNA PRIMA DEL LORO UTILIZZO,** nel caso siano rilevati dei virus occorre fare intervenire immediatamente l'amministratore di sistema.
- **CONTROLLANDO CHE IL SOFTWARE ANTIVIRUS SIA COSTANTEMENTE AGGIORNATO**

- Tutti i computer sono dotati di software Antivirus con update automatico. È fatto obbligo a tutti i dipendenti di non interrompere i programmi di aggiornamento periodico dei file e di effettuare la scansione del proprio computer almeno una volta al mese.
- **NON DIFFONDENDO MESSAGGI DI PROVENIENZA DUBBIA**
- Messaggi che avvisano di un nuovo virus pericolosissimo devono essere ignorati.
- Non aprire file in formato .exe allegati a comunicazioni email.
- Non cliccando su link esterni contenuti in email provenienti da mittenti non conosciuti.

8) TRATTAMENTO DATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Tutti i documenti cartacei contenenti dati personali devono essere conservati in armadi chiusi.

Gli incaricati possono prelevare i documenti utili per il trattamento, per il tempo necessario a tale operazione, dopo di che hanno il compito di riporli nel sopraccitato luogo preposto alla loro conservazione. E' compito dell'incaricato, che preleva i documenti, garantire che questi ultimi siano rinchiusi in un cassetto della propria scrivania nel periodo di temporanea assenza dal posto di lavoro.

L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate tramite il sistema di registrazione degli accessi.

9) ACCESSO AI DATI DA PARTE DELL'AMMINISTRATORE DI SISTEMA

In conformità a quanto previsto dall'atto di nomina dell'Amministratore di Sistema, nei casi in cui si verificano una delle seguenti condizioni:

- prolungata assenza o impedimento dell'incaricato;
- intervento è indispensabile e indifferibile;
- concrete necessità di operatività e di sicurezza del sistema.

L'Amministratore di Sistema può accedere al computer per acquisire i dati necessari al proseguimento dell'attività lavorativa, registrando in apposito verbale le operazioni eseguite.

L'Amministratore di sistema, su propria iniziativa o su richiesta dell'Organismo di Vigilanza, potrà effettuare controlli a campione circa il rispetto di quanto contenuto nel presente regolamento e nel Codice Etico e nel Codice di Comportamento che ciascun dipendente è tenuto a seguire.

10) SANZIONI PER INOSSERVANZA DELLE NORME.

Le presenti istruzioni sono impartite ai sensi delle normative vigenti in materia di privacy ed in conformità al Modello di organizzazione, gestione e controllo redatto ai sensi del D.Lgs 231/2001.

Inoltre si fa presente che l'inosservanza del presente regolamento potrebbe configurare violazione del Codice Etico e del Codice di Comportamento e, di conseguenza, essere passibile di sanzioni ai sensi del Codice disciplinare stesso.

11) GESTIONE, CONSERVAZIONE E CONTROLLO DEI DATI INFORMATICI

È fatto divieto applicare sistemi di crittografia, codificazione e simili ai dati se non espressamente richiesto dall'Azienda secondo la tipologia di dato o documento.

12) SEGRETO

Al dipendente/collaboratore è fatto divieto di divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in toto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni per le quali è stato assunto dalla Società, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi. Nella valutazione delle informazioni, il dipendente/collaboratore si impegna a prendere ogni misura perché le stesse rimangano segrete, essendo inteso che, in caso di divulgazione non autorizzata dalla Società, sarà a carico del dipendente/collaboratore l'onere di provare di avere adottato tutta la diligente richiesta per evitare il danno conseguente.

Il dipendente/collaboratore rimane responsabile dei danni eventualmente subiti dalla Società in caso di violazione degli obblighi di cui alla presente clausola.

Gli obblighi del dipendente/collaboratore previsti in questo capo non si esauriranno con la cessazione del rapporto di lavoro/collaborazione.

13) RISERVATEZZA DEI DATI

Premesso che per «Informazioni Riservate» si intendono tutte le informazioni di qualsivoglia natura riferite o apprese in occasione dello svolgimento di mansioni per le quali il soggetto è stato assunto dalla Società, il dipendente/collaboratore si impegna a considerare le Informazioni Riservate come strettamente private e riservate e ad adottare tutte le misure necessarie per non pregiudicare la riservatezza di tali informazioni.

Il dipendente/collaboratore si impegna ad utilizzare le Informazioni Riservate unicamente allo scopo di svolgere l'attività cui è preposto e di conseguenza a non usare tali informazioni in modo da arrecare danno alla Società, né per alcun altro scopo di qualsiasi natura.

Gli impegni di cui al presente capo non proibiscono di comunicare Informazioni Riservate:

a) ad amministratori e dipendenti, membri dell'Organismo di Vigilanza o soggetti terzi di cui si avvale la società mediante accordi consolidati, ai quali è necessario comunicare tali Informazioni al fine dell'espletamento di attività funzionali all'ente;

b) a soggetti diversi da quelli specificati alla precedente lettera a), qualora ciò sia stato autorizzato dalla Società;

L'obbligo di riservatezza non opera in caso di informazioni:

a) che al momento in cui vengono rese note siano di pubblico dominio;

b) che diventino di pubblico dominio dopo essere state rese note per causa non imputabile al dipendente/collaboratore;

L'impegno di riservatezza di cui al presente capo si protrarrà anche dopo la cessazione del rapporto di lavoro e sino a quando le informazioni in oggetto non saranno rese di pubblico dominio.

14) APPLICAZIONE ED INTERPRETAZIONE DEL PRESENTE REGOLAMENTO

Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, il dipendente/collaboratore può rivolgersi al suo referente.

15) DISCIPLINA DEROGHE E MODIFICHE DEL PRESENTE REGOLAMENTO

Qualora al presente regolamento la Società intenda apporre modifiche, queste saranno applicate dandone conoscenza immediata al dipendente/collaboratore.

Deroghe o modifiche di una o più clausole del presente regolamento non comportano la sua integrale modifica o quelle non direttamente emendate, salva l'ipotesi di evidente incompatibilità.

16) RESPONSABILITA'

La violazione di una qualsiasi delle clausole di cui al presente regolamento, dà diritto alla Società di procedere disciplinarmente nei confronti del dipendente/collaboratore infedele.

Qualora la Società venga a conoscenza di una violazione del presente regolamento che costituisca illecito civile o penale, provvederà immediatamente a darne avviso alla competente Autorità.