REGOLAMENTO SULLA SICUREZZA DEI DATI E L'UTILIZZO DEGLI STRUMENTI INFORMATICI

PREMESSA

Come previsto dal Codice Etico di NoiGroup, nell'esercizio delle proprie attività la società disconosce l'uso fraudolento di dati informazioni e permessi e identità digitali di Terzi che possano procurarle beneficio e/o vantaggio. Il presente Regolamento, invece, disciplina tutta la parte di prevenzione agli accessi che possono comportare la sottrazione e la perdita dei dati trattati da NoiGroup anche nel ruolo di Titolare del Trattamento.

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, peraltro necessari allo sviluppo delle attività, espone NoiGroup ai rischi di sottrazione, perdita e/o accesso fraudolento alle proprie informazioni che possono comportare un coinvolgimento dell'azienda sia patrimoniale che penale, e di reputazione creando problemi alla sicurezza informatica e all'immagine della stessa.
Premesso quindi che l'utilizzo delle risorse informatiche e telematiche della nostra azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, NoiGroup adotta un Regolamento interno diretto ad evitare che comportamenti scorretti e/o inconsapevoli possano innescare problemi o minacce alla Sicurezza Informatica e al trattamento dei dati.
Il presente Regolamento deve essere rispettato da tutti i dipendenti di NoiGroup nonché dai collaboratori esterni per quanto compatibile. Con riferimento specifico ai collaboratori, considerata l'autonomia nelle modalità di svolgimento dell'incarico di consulenza, l'autonomia propria del collaboratore e la circostanza che il collaboratore usa strumenti di lavoro propri, il presente Regolamento di comportamento si applica quale integrazione degli obblighi di riservatezza propri dell'incarico professionale.

Il presente Regolamento tratta tutte le informazioni e/ o dati, sia in formato cartaceo che digitale. Le regole di comportamento a seguito indicate fanno riferimento ad una serie di situazioni astrattamente configurabili e indicate a titolo esemplificativo e non esaustivo. Conseguentemente, i destinatari del presente Regolamento dovranno adottare in generale un comportamento ispirato ai principi di riservatezza e tutela della sicurezza dei dati e delle informazioni, anche nelle situazioni non espressamente contemplate dal presente Regolamento che si dovessero verificare.

1. GESTIONE DEI DATI FISICI E CARTACEI

In merito alla gestione dei dati fisici cartacei il Dipendente/Collaboratore deve seguire le regole a seguito specificate.

1.1 Riporre la documentazione cartacea negli armadi lasciando a fine giornata la scrivania o la postazione in dotazione priva di documentazione relativa a clienti, fornitori, terzi e attività e/o progetti in corso.

1.2 Non lasciare incustodita eventuale documentazione cartacea e, in ogni caso qualora non più necessaria, preoccuparsi di distruggerla oppure di riporla negli appositi armadi chiusi.

1.3 In caso di svolgimento dell'attività lavorativa al di fuori della sede aziendale, scegliere luoghi che assicurino l'opportuna riservatezza e in caso di conversazioni telefoniche aventi ad oggetto i progetti e le attività in corso, e i dati che alle stesse si riferiscono, evitare che persone estranee all'Azienda possano volontariamente o involontariamente ascoltare la conversazione, ponendo particolare attenzione all'utilizzo del telefono in ambienti pubblici.

1.4 Evitare di scambiarsi informazioni riservate in luoghi o mezzi pubblici o con modalità che ne possano compromettere la riservatezza.

1.5 Non divulgare, senza specifica autorizzazione, informazioni aziendali al di fuori dell'ambiente di lavoro e in generale non discutere di aspetti riservati del proprio lavoro con persone estranee all'Azienda oppure con colleghi e/o collaboratori estranei alle attività in corso.

1.6 Durante le conversazioni telefoniche, avvisare l'interlocutore e rendere note le persone presenti qualora si attivi la modalità "viva voce".

1.7 Nell'organizzare una chiamata tramite sistema telefonico collettivo ("conference call") o video-conferenza, assicurarsi che tutti i partecipanti siano informati del livello di riservatezza della comunicazione.

1.8 Non cedere a terzi, a qualsiasi titolo, l'uso del cellulare aziendale in dotazione.

2. UTILIZZO DEI DISPOSITIVI PER IL TRATTAMENTO DEI DATI DIGITALI

A seconda delle loro Mansioni, i dipendenti e i collaboratori sono dotati di uno o più dispositivi per il trattamento dei dati digitali (es. PC, Laptop, Tablet, Smartphone).

2.1 Il dispositivo affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

2.2 L'accesso al dispositivo è sempre protetto da una password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. L'attivazione della password di accesso è consentita solo previa autorizzazione da parte dell'Amministratore di Sistema e/o dal Responsabile interno al trattamento.

2.3 L'Amministratore di Sistema, per l'espletamento delle sue funzioni, ha la facoltà, in qualunque momento, di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica.

2.4 Non è consentito installare autonomamente programmi e/o applicazioni di qualsiasi provenienza se non con l'autorizzazione esplicita del Responsabile Sicurezza Informatica e dell'Amministratore di Sistema.

2.5 Non è consentito memorizzare qualsiasi tipo di file non legato all'attività lavorativa.

2.6 I PC e i Laptop devono essere spenti ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio (fatto salvo i casi in cui ci si debba collegare ai dispositivi da remoto).

2.7 In ogni caso, lasciare incustodito un dispositivo attivo e 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.

2.8 Non è consentita l'installazione o il collegamento, anche temporaneo, sul proprio dispositivo di nessun dispositivo di memorizzazione, comunicazione o altro, se non con l'autorizzazione esplicita del Responsabile Sicurezza Informatica.

2.9 Ogni utente dovrà comunque prestare la massima attenzione ai dati digitali importati da origine esterna, avvertendo il Responsabile Sicurezza Informatica nel caso in cui vengano rilevati virus.

2.10 Non è consentito collegarsi alla rete interna con dispositivi che non siano di proprietà dell'azienda o autorizzati dal Responsabile Sicurezza Informatica e dell'Amministratore di Sistema.

2.11 Quando i dispositivi sono portati ed utilizzati all'esterno dell'Azienda, devono essere custoditi diligentemente.

2.12 La condivisione delle partizioni del/dei Server viene svolta esclusivamente dall'Amministratore di Sistema.

2.13 Le aree di condivisione devono contenere 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 in queste unità.

2.14 Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

2.15 È cura dell'operatore non salvare files in posti diversi dal/dai Server aziendale/i altrimenti non saranno sottoposti ai salvataggi periodici.

3. UTILIZZO DELLA RETE FISICA E DEI DISPOSITIVI WIFI

La rete di acceso ai dati e formata da uno o più Server e dai dispositivi ad esso connessi. Attraverso la rete è possibile accedere ai Server e al Web. La rete si suddivide in rete fisica e WI-FI.

3.1 Sia per l'accesso alla rete fisica che ai Router WI-FI è necessario disporre delle autorizzazioni agli accessi.

3.2 Sono state predisposte due reti WI-FI. La prima è dedicata a dispositivi aziendali mentre la seconda è specifica per gli ospiti e prevede il solo accesso ad Internet. Ad entrambe le reti si accede tramite password.

3.3 Le password d'accesso ai Dispositivi, ai Server ai programmi e ai siti WEB sono segrete e vanno comunicate e gestite secondo le procedure impartite.

3.4 È assolutamente proibito l'utilizzo di "nomi utente" e "password" non attribuiti al dipendente o collaboratore.(Utilizzo di credenziali non personali)

3.5 L'Amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza Informatica, sia sui Dispositivi degli incaricati che sui Server.

3.6 È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.

4. GESTIONE DELLE USER NAME E PASSWORD

4.1 La username e la password di accesso ai dispositivi, alla rete ai programmi e ai portali Web, ha la funzione di salvaguardare la sicurezza dei dati digitali e pertanto è cura dell'operatore mantenerla segreta.

4.2 Le password possono essere formate da lettere (minimo una maiuscola e minimo una minuscola) e numeri, ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno 8 caratteri. Nel caso in cui lo strumento elettronico non lo permetta, devono essere composte da un numero di caratteri pari al massimo consentito e non devono contenere riferimenti agevolmente riconducibili all'incaricato.

4.3 Nel caso si sospetti che la password abbia perso la segretezza, deve essere sostituita immediatamente.

5. USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata da NoiGroup all'Utente, è uno strumento di lavoro affidato al dipendente. La "personalizzazione" dell'indirizzo, infatti, risponde unicamente a esigenze operative e di servizio, ma non vale a connotare la casella di posta assegnata come "privata". L'eventuale utilizzo, da parte del Dipendente/Collaboratore della casella di posta elettronica aziendale per finalità personali (ricezione, invio e archiviazione di corrispondenza elettronica di carattere extra-professionale), anche ove fosse tollerato, non varrà in ogni caso a mutare la destinazione d'uso e la finalità dello strumento "casella di posta", che resterà esclusivamente destinata a finalità di carattere lavorativo.

5.1. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
5.2. È fatto divieto di utilizzare le caselle di posta assegnate dall'azienda per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso l'utente non potrà utilizzare la posta elettronica per:

- scaricare dal Web o dall'esterno file e dati non inerenti alle proprie attività lavorative, in modo da evitare la propagazione di virus informatici e in generale potenziali attacchi ai sistemi di sicurezza informatica;
- 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;
- indirizzare e/o destinare (direttamente o per conoscenza) informazioni e/o dati a chi, per ruolo e responsabilità, non sia effettivamente coinvolto dal contenuto del messaggio stesso;

5.3. Qualora si dovessero ricevere messaggi SPAM, non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi e nei casi sospetti sarà necessario comunicarlo immediatamente al Responsabile Sicurezza Informatica.
5.4. È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non scaricare file eseguibili o documenti di ogni genere da siti Web o Ftp non conosciuti.
5.5. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
5.6. È necessario limitare al massimo la diffusione in rete dell'indirizzo assegnato in uso, al fine di limitare lo spamming.
5.7. Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Azienda ovvero contenga documenti da considerarsi riservati, deve essere visionata od autorizzata dal Responsabile di riferimento.
5.8. Le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, …), devono essere autorizzate e firmate dal Presidente, e/o dalla Direzione, a seconda del loro contenuto e dei destinatari delle stesse. Sono state attivate delle caselle di posta certificata (PEC) dalle quali è possibile trasmettere e ricevere documenti ufficiali in sostituzione della posta cartacea.
5.9. Non è consentita la lettura delle caselle di posta private/personali attraverso i dispositivi aziendali.
5.10. Le mail indirizzate a info@coopnoi.it vengono ricevute e smistate dalla Segreteria che ha libero accesso a contenuti garantendo la massima riservatezza, soprattutto nel caso in cui si tratti di dati sensibili o giudiziari.
5.11. In caso di assenze programmate, il Dipendente è tenuto ad attivare un servizio di risposta automatica tramite la Web Mail che informi il mittente della sua assenza e assicurare comunque che le comunicazioni importanti vengano comunque prese in carico direttamente dal dipendente e/o figura incaricata.
5.12. In caso di assenza non programmata (ad es. per lunga malattia) la procedura sopra indicata potrà essere attivata a cura dell'Azienda attraverso l'Amministratore di Sistema.
5.13. Per la casella/caselle in uso ai Dipendenti/Collaboratori si segnala che la stessa/stesse legate alle attività aziendali in corso sono costantemente accessibili all'Amministratore di Sistema.
5.14. In ogni caso, qualora per esigenze aziendali sia necessario prendere visione dei messaggi e dei documenti contenuti nella casella di posta elettronica e/o nelle partizioni dei server del Dipendente assente, l'Azienda potrà provvedere al recupero dei documenti richiesti.
5.15. Alla cessazione del rapporto di lavoro e al completamento delle attività di progetto legate ai rapporti di consulenza/collaborazione in corso, la casella di posta elettronica verrà chiusa provvedendo eventualmente a reindirizzare su altra casella di posta elettronica aziendale la posta in arrivo.
5.16. Noi Group rende noto che, al fine di verificare la funzionalità, la sicurezza del sistema e il suo corretto utilizzo, le apparecchiature di rete preposte alla gestione delle caselle di posta elettronica e al collegamento verso *Web* possono tenere traccia dei *file* di *log* contenenti i dati riguardanti le *e-mail* e i dati di navigazione degli utenti.
5.17. Per motivi di sicurezza del sistema informatico, per motivi tecnici e/o manutentivi l'Azienda, inoltre, si riserva la facoltà di intraprendere eventuali controlli difensivi, atti a garantire la tutela del patrimonio aziendale e l'individuazione di eventuali illeciti o reati perpetrati attraverso gli strumenti informatici aziendali.

5.18. L'Azienda rende noto che gli Amministratori di Sistema sono stati autorizzati 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.).

6. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

6.1. Il Dispositivo 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.

6.2. L'utente non potrà utilizzare internet:

- Per l'upload o il download di software gratuiti (freeware) e shareware, e l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa.
- Per l'effettuazione di ogni genere di transazione finanziaria, comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione Generale e comunque nel rispetto delle normali procedure di acquisto.
- Per ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa.
- Per 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) se non espressamente autorizzati dal Responsabile d'ufficio

7. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY.

7.1. È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nei paragrafi precedenti e nei punti seguenti in riferimento al regolamento (UE) 2016/679 del parlamento europeo e del consiglio del 27 aprile 2016 e D.Lgs. 101/2018.

7.2. Occorre procedere alla raccolta dei dati dell'interessato (clienti, fornitori, dipendenti) con la massima cura verificando l'esattezza dei dati stessi e quindi l'attendibilità e genuinità della fonte e procedere all'aggiornamento dei dati, ove necessario.

7.3. È possibile accedere ai soli dati personali, oggetto di trattamento, la cui conoscenza sia strettamente necessaria per lo svolgimento dei compiti affidati.

7.4. In fase di utilizzo dei documenti cartacei contenenti qualsiasi tipo di dato (personale, sensibile o giudiziario), medesimi

7.5. atti e documenti sono controllati e custoditi dall'operatore fino alla restituzione in modo che ad essi non accedano persone non autorizzate, e al termine dello svolgimento delle operazioni devono essere nuovamente archiviati.

7.6. L'accesso agli archivi cartacei contenenti dati particolari (sensibili o giudiziari) deve essere autorizzato.

7.7. Occorre conservare i documenti o atti che contengono dati sensibili o giudiziari in archivi (ad esempio stanze, armadi, schedari, contenitori in genere) chiusi a chiave.

7.8. I documenti cartacei, non più utilizzati, devono essere distrutti o comunque resi illeggibili, prima di essere eliminati o cestinati.

7.9. Non è possibile fornire dati e informazioni relative a clienti, fornitori o dipendenti per telefono, qualora non si abbia la certezza assoluta sull'identità del destinatario.

7.10. Qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia ci si deve accertare dell'identità del chiamante, per esempio provvedendo a richiamare per avere la certezza sull'identità del richiedente.

7.11. Le porte esterne di accesso devono essere tenute chiuse; l'accesso di terzi deve essere consentito solo dopo identificazione delle persone. Qualora la situazione di confidenzialità e riservatezza del trattamento dell'informazione lo richiedano, anche le porte interne di accesso agli uffici dovranno rimanere chiuse limitatamente a tali necessità.

7.12. Le informazioni Aziendali apprese, anche accidentalmente, in ragione della propria attività lavorativa devono rimanere riservate e non devono essere rivelate a terzi.

3. I dati personali raccolti per il loro trattamento non possono essere consegnati a terzi non facenti parte degli incaricati esterni al trattamento, se non con l'Autorizzazione del Titolare al trattamento e del Responsabile interno al trattamento.

8. NON OSSERVANZA DELLA NORMATIVA AZIENDALE E SANZIONI

8.1. In riferimento al presente Regolamento periodicamente il Titolare si riserva di organizzare l'effettuazione delle verifiche controllando che le norme sopra citate vengano rispettate.

8.2. Il mancato rispetto o la violazione delle regole sopra indicate darà luogo all'applicazione dei provvedimenti disciplinari previsti dal vigente CCNL applicato al singolo contratto di lavoro, nonché all'applicazione delle altre disposizioni previste dal sistema sanzionatorio definito dal modello organizzativo 231.

9. AGGIORNAMENTO E REVISIONE

9.1. Il presente regolamento è oggetto di revisione periodica, in base alle evoluzioni normative in materia di Privacy, alle necessità aziendali e per il necessario adeguamento all'evoluzione dei sistemi ICT (Information Communication Technology) aziendali.

Il Presidente del C.d.A.