Premessa

L'utilizzo delle risorse informatiche e degli strumenti aziendali deve ispirarsi ai principi di diligenza, correttezza e responsabilità, che costituiscono elementi fondamentali del rapporto di lavoro.
NEWCERT S.r.l. ha adottato il presente Regolamento al fine di contribuire alla diffusione della cultura della sicurezza informatica e della protezione dei dati e di prevenire comportamenti, anche inconsapevoli, che possano determinare disservizi, perdite di dati, violazioni della sicurezza o altre minacce per l'Azienda.
Il presente Regolamento disciplina le condizioni per il corretto utilizzo degli strumenti informatici e delle risorse aziendali da parte del personale dipendente, collaboratori e di altri soggetti autorizzati ad accedervi.
Le risorse aziendali devono essere utilizzate esclusivamente per finalità lavorative, nel rispetto delle disposizioni aziendali, delle procedure interne e della normativa vigente.

1. Utilizzo del Personal Computer - PC

Il Personal Computer affidato al personale dipendente costituisce uno strumento di lavoro. Ogni utente è responsabile dell'utilizzo diligente e corretto delle dotazioni informatiche ricevute in assegnazione.
Non è consentito modificare le caratteristiche hardware o software del PC, installare programmi, applicazioni, componenti o periferiche non autorizzati.
Il PC deve essere spento, al termine della giornata lavorativa o quando richiesto da esigenze manutentive e comunque non deve essere lasciato accessibile a soggetti non autorizzati;
pertanto durante le assenze, anche temporanee, l'utente deve provvedere al blocco della sessione mediante le funzionalità messe a disposizione dal sistema operativo.
È buona regola effettuare periodicamente una verifica dei file presenti nelle aree locali del PC, eliminando quelli obsoleti o non più necessari. L'archiviazione dei dati aziendali deve essere effettuata, ove previsto, negli spazi e nei sistemi aziendali centralizzati.
La memorizzazione locale di dati aziendali deve essere limitata allo stretto necessario, privilegiando le modalità di archiviazione centralizzata predisposte dall'Azienda.

2. Utilizzo della rete aziendale e di Internet

L'accesso alla rete e ai sistemi aziendali è protetto da credenziali personali. Ogni utente deve utilizzare esclusivamente il proprio profilo e non può consentire ad altre persone di utilizzare le proprie credenziali.
È assolutamente vietato utilizzare la rete aziendale per finalità illecite, fraudolente o comunque non autorizzate, nonché per attività che possano compromettere la sicurezza, la disponibilità o le prestazioni dei sistemi aziendali.
È vietata la creazione o la condivisione di cartelle, archivi o risorse accessibili in rete al di fuori delle modalità e degli strumenti autorizzati.

Non è consentito effettuare attività di monitoraggio, intercettazione, scansione o analisi del traffico di rete o dei sistemi informatici aziendali, salvo che tali attività siano espressamente autorizzate e rientrino nelle mansioni o nelle responsabilità assegnate (es. penetration test per verifica della vulnerabilità della rete).

3. Gestione delle password e delle credenziali

L'utente è tenuto a mantenere la massima riservatezza sulle proprie password, credenziali di accesso, codici e su qualsiasi altra informazione utilizzata per l'autenticazione ai sistemi aziendali.
Le credenziali sono personali e non devono essere comunicate, cedute o rese disponibili ad altre persone.
Le password devono essere scelte e gestite secondo le regole di sicurezza definite (dagli applicativi o dall'azienda stessa) e non devono essere annotate in luoghi accessibili a terzi.
Qualora l'utente sospetti (o riceva comunicazioni) che le proprie credenziali siano state compromesse, divulgate o utilizzate da soggetti non autorizzati, deve provvedere, non appena possibile, alla loro immediata modifica e informare tempestivamente il responsabile IT aziendale .

4. Utilizzo dei PC portatili e dispositivi mobili

L'utente è responsabile del PC portatile e degli eventuali dispositivi mobili assegnatigli dall'Azienda e deve custodirli con particolare diligenza sia durante gli spostamenti sia durante l'utilizzo presso la sede aziendale o presso luoghi esterni.
Ai PC portatili si applicano tutte le disposizioni previste dal presente Regolamento per i Personal Computer (paragrafo 1).
Durante gli spostamenti e in caso di temporaneo allontanamento, il dispositivo non deve essere lasciato incustodito o esposto a rischi di furto, smarrimento o accesso da parte di soggetti non autorizzati.
Quando utilizzato in luoghi pubblici, l'utente deve adottare ogni ragionevole precauzione per impedire che terzi possano visualizzare dati, documenti, comunicazioni o credenziali aziendali.

5. Utilizzo dei telefoni cellulari aziendali

Il telefono cellulare aziendale e la relativa SIM costituiscono strumenti di lavoro messi a disposizione dell'utente per lo svolgimento delle proprie mansioni.
L'utente è responsabile della custodia e del corretto utilizzo del dispositivo e deve adottare tutte le necessarie precauzioni per impedirne il furto, lo smarrimento, il danneggiamento o l'accesso da parte di soggetti non autorizzati.
Il telefono aziendale deve essere utilizzato per finalità lavorative; eventuali utilizzi personali devono essere occasionali, ragionevoli e non devono comportare costi ingiustificati, interferire con l'attività lavorativa o compromettere la sicurezza dell'Azienda.

È vietato installare applicazioni, software o servizi non autorizzati, nonché modificare le impostazioni di sicurezza del dispositivo o disabilitare sistemi di protezione, aggiornamento, cifratura o gestione aziendale eventualmente presenti.
Il dispositivo deve essere protetto mediante codice, PIN, password, sistema biometrico o altra modalità di autenticazione resa disponibile.
L'utente non deve utilizzare il telefono aziendale per memorizzare o trasferire dati aziendali attraverso applicazioni o servizi personali non autorizzati.
È assolutamente vietato utilizzare il dispositivo aziendale per attività illecite, per contenuti contrari alla legge o comunque incompatibili con i principi di correttezza e professionalità propri del rapporto di lavoro.
In caso di furto, smarrimento, perdita della SIM, sospetto accesso non autorizzato o altra situazione che possa compromettere la sicurezza dei dati o delle comunicazioni aziendali, l'utente deve informare immediatamente l'Azienda, affinché possano essere adottate le necessarie misure di protezione.

6. Utilizzo della posta elettronica

La casella di posta elettronica assegnata dall'Azienda costituisce uno strumento di lavoro. L'utente è responsabile del suo corretto e diligente utilizzo.
L'utente deve prestare particolare attenzione ai messaggi provenienti da mittenti sconosciuti, alle richieste anomale, ai collegamenti contenuti nelle e-mail e agli allegati inattesi (phishing); pertanto In presenza di messaggi sospetti non devono essere aperti gli allegati, selezionati collegamenti o fornite credenziali, dati personali, informazioni aziendali o dati bancari.
Anche nel caso di messaggi apparentemente provenienti da mittenti conosciuti, qualora il contenuto o la richiesta risultino anomali, l'utente deve verificarne l'autenticità attraverso un canale alternativo prima di procedere.
Quando un documento deve essere inviato all'esterno dell'Azienda, deve essere utilizzato, ove opportuno, un formato idoneo a impedirne modifiche non autorizzate, come il formato PDF, e devono essere adottate le eventuali misure di protezione previste dalle procedure aziendali.
È vietato installare o scaricare software gratuito, shareware o altri programmi da Internet se non espressamente autorizzati.

7. Utilizzo degli strumenti di Intelligenza Artificiale (AI)

Gli strumenti di Intelligenza Artificiale, inclusi chatbot, sistemi di generazione e analisi di testi, immagini, codice, documenti o altri contenuti, possono essere utilizzati esclusivamente per finalità lavorative e nel rispetto delle disposizioni aziendali, della normativa vigente in materia di protezione dei dati personali e del Regolamento (UE) 2024/1689 – Artificial Intelligence Act (AI Act).

L'utilizzo degli strumenti di AI deve avvenire in modo responsabile, consapevole e verificabile. L'utente rimane responsabile dei contenuti, delle informazioni e dei risultati prodotti o utilizzati nell'ambito della propria attività lavorativa.
È vietato inserire in strumenti di AI non espressamente autorizzati dall'Azienda dati personali, informazioni riservate o confidenziali, credenziali, password, documenti aziendali, informazioni relative a clienti e fornitori, codice sorgente, know-how o altri dati soggetti a obblighi di riservatezza.
I contenuti generati dall'AI non devono essere considerati automaticamente corretti, completi o attendibili. L'utente è pertanto tenuto a verificarne l'accuratezza e l'idoneità prima del loro utilizzo, soprattutto quando gli stessi siano destinati a clienti, fornitori, dipendenti o terzi, oppure possano incidere su decisioni aziendali.

8. Protezione dei dati personali

NEWCERT S.r.l. tratta i dati personali nel rispetto del Regolamento (UE) 2016/679 (GDPR), del D.Lgs. 196/2003 e successive modifiche e integrazioni, nonché delle ulteriori disposizioni applicabili in materia di protezione dei dati personali.
Tutti gli utenti autorizzati al trattamento dei dati personali devono operare nel rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione (accountability).
I dati personali devono essere trattati esclusivamente per finalità determinate, esplicite e legittime e nei limiti delle autorizzazioni ricevute.
È vietato raccogliere, consultare, utilizzare, modificare, copiare, comunicare o diffondere dati personali per finalità diverse da quelle connesse alle proprie mansioni o comunque non autorizzate.
Gli utenti devono trattare esclusivamente i dati personali necessari allo svolgimento dell'attività lavorativa, evitando la raccolta o la conservazione di informazioni eccedenti rispetto alle finalità perseguite.

9. Restituzione delle dotazioni aziendali

Tutte le apparecchiature, i dispositivi, gli accessori, le SIM, le credenziali e le altre risorse aziendali affidate all'utente rimangono di proprietà o nella disponibilità dell'Azienda.
Alla cessazione del rapporto di lavoro o di collaborazione, alla modifica delle mansioni o quando richiesto dall'Azienda, l'utente deve restituire tempestivamente le dotazioni ricevute e non deve trattenere copie di dati, documenti o informazioni aziendali, salvo diversa autorizzazione.

10. Segnalazione degli incidenti

Qualsiasi evento che possa compromettere la sicurezza delle informazioni o delle risorse aziendali deve essere segnalato tempestivamente.

A titolo esemplificativo, devono essere comunicati furti o smarrimenti di dispositivi, sospette violazioni delle credenziali, e-mail di phishing, apertura accidentale di allegati sospetti, perdita o divulgazione di dati, accessi non autorizzati e anomalie dei sistemi.
La tempestività della segnalazione è essenziale per consentire all'Azienda di limitare eventuali conseguenze e adottare le misure necessarie.

11. Mancato rispetto del Regolamento

Il mancato rispetto o la violazione delle disposizioni contenute nel presente Regolamento può comportare l'adozione dei provvedimenti previsti dalla normativa vigente, dal contratto collettivo applicabile e dalle procedure aziendali, nel rispetto delle garanzie e delle procedure previste dalla legge.
Restano ferme, ove applicabili, le responsabilità civili, amministrative e penali derivanti da comportamenti illeciti.
L'Azienda si riserva di aggiornare il presente Regolamento in relazione all'evoluzione tecnologica, alle esigenze organizzative, alle minacce informatiche e alla normativa applicabile.

La Direzione
NEWCERT S.r.l.
Via Riccardo Billi, 10
00173 - Roma
P.IVA 12017391009