



CONNECTION PLUS

e

Connection Plus S.R.L.



CONNECTION PLUS

CODICE ETICO E DISCIPLINARE

Casteldaccia, 1.12.2025



PREMESSA

Il presente Codice Etico e Disciplinare definisce l'insieme delle norme di comportamento, degli obblighi contrattuali e delle misure disciplinari applicabili ai dipendenti della Connection Plus S.r.l.

Integra e completa:

- il CCNL Telecomunicazioni, normativa applicabile al personale dipendente;
- il Regolamento Aziendale (Art. 1-18);
- la Policy Utilizzo Dispositivi Aziendali (HW, SW, internet, PEC)
- la Policy Trasferte e Note Spese (versione 1.3);
- la normativa vigente (L. 300/1970, D.Lgs. 81/2008, GDPR, Codice civile, normativa AGCOM/MIMIT).

Il Codice è parte integrante degli obblighi contrattuali del personale.



1. PRINCIPI ETICI GENERALI

1.1 Obbligo di fedeltà e riservatezza

Ai sensi del Regolamento aziendale (Art. 2) e del Codice Civile:

- è vietato trattare affari in concorrenza con l'azienda;
- è vietato divulgare informazioni aziendali, know-how, procedure, dati clienti, contratti, file, CRM;
- ogni dato trattato deve rispettare il GDPR.

1.2 Diligenza, correttezza e rispetto delle direttive

Il lavoratore deve utilizzare la massima diligenza nello svolgimento delle attività (Art. 3 Regolamento), rispettando:

- ordini e procedure aziendali;
- tempi, metriche, KPI e standard qualitativi previsti dal CCNL Telecomunicazioni.

1.3 Comportamento e decoro

È obbligatorio mantenere:

- rispetto verso colleghi, clienti e superiori;
- un abbigliamento decoroso e adeguato;
- un comportamento corretto e professionale.

Sono vietati:

- ✓ molestie, mobbing, discriminazioni;
- ✓ riproduzione di musica in ufficio;
- ✓ linguaggi offensivi o comportamenti conflittuali.



1.4 Sicurezza sul lavoro

Ogni lavoratore deve:

- utilizzare DPI;
- segnalare rischi e anomalie;
- rispettare regole di sicurezza aziendali e procedure interne.

Responsabile interno sicurezza: ALESSIA ALAIMO.

1.5 Rispetto orario, presenze e assenze

Il lavoratore deve:

- rispettare rigorosamente l'orario di lavoro;
- comunicare assenze entro 48 ore;
- produrre certificazione per malattia;
- richiedere ferie e permessi secondo le modalità aziendali.



2. UTILIZZO DI DISPOSITIVI, INTERNET, E-MAIL E PEC

Il presente Codice recepisce integralmente la Policy Utilizzo Dispositivi Aziendali

2.1 Accesso a internet

È vietato:

- visitare siti non pertinenti alla mansione o contrari alla legge;
- installare software non autorizzati;
- utilizzare VPN, reti parallele o creare reti WIFI non autorizzate;
- condividere o cedere credenziali di accesso;
- aggirare sistemi di sicurezza aziendale.

2.2 Posta elettronica

È vietato:

- inviare documenti aziendali verso indirizzi privati;
- inviare spam, catene o comunicazioni massive;
- scaricare allegati sospetti;
- modificare configurazioni IT.

Obbligo di correttezza, attenzione e tutela della riservatezza.

2.3 PEC

È consentito esclusivamente l'uso lavorativo.

Il responsabile deve:

- monitorare costantemente la casella;
- conservare documenti PEC;
- cambiare password in caso di rischio;
- custodire le credenziali.



2.4 Beni aziendali

Il dipendente deve:

- firmare moduli di assegnazione;
- custodire beni con diligenza (pc, tablet, telefoni, auto, badge);
- non smontare o manomettere apparecchiature;
- non lasciare PC incustoditi (auto, hotel, aree pubbliche).

Danni, smarrimenti e furti devono essere comunicati tempestivamente (Policy §8).



3. TRASFERTE E NOTE SPESE

3.1 Autorizzazione

Ogni trasferta deve essere:

- autorizzata per iscritto dal responsabile diretto;
- prenotata attraverso HR.

Voli, treni, hotel devono essere prenotati esclusivamente da HR (Policy §3.4).

3.2 Massimali

- Hotel in Italia: max 50€
- Hotel estero: max 80€
- Pranzo: 12€
- Cena: 20€
- Carburante (auto assegnata/autonoleggio): max 300€/mese
- Rimborso auto propria: max 0,20€/km

3.3 Spese NON rimborsabili

Non sono rimborsati:

- taxi;
- penali per cambi volo richiesti dal dipendente;
- happy hour, caffè, snack;
- spese non autorizzate;
- spese prive di giustificativi validi.



4. DISCIPLINA SPECIFICA DEL SETTORE TELECOMUNICAZIONI

Comportamenti vietati:

- manipolazione di report, KPI, statistiche di chiamata;
- falsificazione di contratti o procedure di attivazione;
- violazione delle regole AGCOM sulla trasparenza;
- utilizzo fraudolento di CRM, ticket o piattaforme gestionali;
- registrazione non autorizzata di conversazioni;
- qualsiasi pratica commerciale ingannevole.

5. SANZIONI DISCIPLINARI (CCNL TELECOMUNICAZIONI)

5.1 Rimprovero verbale

Per lievi irregolarità:

- primi ritardi;
- mancato rispetto formale delle procedure.

5.2 Rimprovero scritto

Per infrazioni non gravi:

- ripetuti ritardi;
- inosservanza disposizioni;
- uso improprio di strumenti.

5.3 Multa

Per comportamenti più rilevanti:

- abbandono temporaneo del posto;
- mancato rispetto norme sicurezza;



- negligenza con danno lieve.

5.4 Sospensione fino a 10 giorni

Per infrazioni gravi:

- violazione privacy non dolosa;
- condotte scorrette verso colleghi/clienti;
- alterazioni non fraudolente di dati.

5.5 Licenziamento con preavviso

Per:

- reiterazione infrazioni;
- grave insubordinazione;
- violazioni gravi con danno all'azienda.

5.6 Licenziamento per giusta causa

Per fatti che rendono impossibile il rapporto:

- furto, danneggiamento, manomissioni;
- falsificazione contratti/KPI;
- violazione dolosa privacy e data breach;
- utilizzo fraudolento accessi IT;
- aggressioni e comportamenti violenti;



6. PROCEDURA DISCIPLINARE

Ai sensi dell'art. 7 L. 300/1970:

- contestazione scritta;
- 5 giorni per difesa;
- eventuale audizione;
- valutazione;
- comunicazione della sanzione.

7. ENTRATA IN VIGORE

Il presente Codice entra in vigore alla data di consegna ai lavoratori ed è parte integrante:

- del contratto individuale di lavoro;
- del Regolamento aziendale;
- della Policy Trasferte;
- della Policy Utilizzo Dispositivi.



- devono essere predisposte misure tecniche ed organizzative di sicurezza per l'accesso ai locali, che ospitano i server e gli strumenti elettronici in dotazione alle postazioni di lavoro, favorendo possibilmente la localizzazione e l'ubicazione in unico luogo o in luoghi collegati, al fine di consentire una migliore gestione degli strumenti e della sicurezza attiva e passiva;
- ogni eventuale incidente o evento straordinario, che possa pregiudicare la sicurezza dei dati e dei sistemi, deve essere oggetto di analisi e di rapporto scritto;
- tutti i progetti per lo sviluppo di nuovi sistemi / servizi, aventi natura trasversale e che possano interessare il sistema informativo dell'azienda, devono essere comunque gestiti secondo quanto riportato nel presente manuale;
- al pari, tutte le modifiche eventualmente apportate ai processi organizzativi devono essere documentate nel presente manuale o nei documenti del sistema di qualità aziendale.

In particolare, l'analisi e la valutazione dei rischi sono mediante l'individuazione delle singole minacce e vulnerabilità, per le quali si è provveduto a determinare il peso del rischio in termini di probabilità (P) e di danno (D), valutati secondo i parametri (alto – medio – lieve) associati alle minacce.

Data di Adozione	3.12.2025
Data di Revisione	
Per accettazione ed adozione	~~Di Salvo Vincenzo~~ , n.q. GIUSEPPE BRIANONE