DIMEDP CONSULTING SRL

Codice Etico, Codice di Condotta Anti-Corruzione e Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001

Società	DIMEDP CONSULTING SRL
Sede e contatti	Strada Casale Valenza 4 L, 15033 Casale Monferrato (AL) Tel. +39 0142 230539 info@dimedpconsulting.it | PEC dimedpconsulting@registerpec.it
Dati societari	P. IVA / C.F. 02380070066 Capitale interamente versato €34.000,00 REA AL 250702
Stato documento	Documento aziendale di riferimento in materia di etica, prevenzione della corruzione e presidi ex D.Lgs. 231/2001, coordinato con la documentazione organizzativa e gli aggiornamenti periodici applicabili.

Indice contenuti

1. Codice Etico

1.1 Premessa

Il presente Codice Etico definisce i principi, i valori e le regole di comportamento cui si ispira DIMEDP CONSULTING SRL nello svolgimento delle proprie attività di consulenza organizzativa e ICT, implementazione e supporto software, soluzioni ERP, business continuity, cyber security e servizi connessi. Il Codice orienta i comportamenti interni ed esterni della società, ne tutela la reputazione e contribuisce alla prevenzione di condotte illecite o non coerenti con i principi aziendali.

1.2 Destinatari

Il Codice Etico si applica agli amministratori, ai dirigenti, ai dipendenti, ai collaboratori, ai consulenti, ai partner commerciali, ai fornitori e, più in generale, a tutti i soggetti che operano in nome o per conto della società o che intrattengono con essa rapporti professionali o commerciali, nei limiti di compatibilità con il rispettivo ruolo.

1.3 Principi generali

La società opera secondo i principi di legalità, correttezza, integrità, trasparenza, responsabilità, professionalità, tracciabilità delle decisioni, tutela della persona, riservatezza delle informazioni, sicurezza, continuità operativa e affidabilità verso clienti, partner e mercato.

1.4 Impegni della società

- agire nel pieno rispetto delle leggi, dei regolamenti, delle procedure interne e degli obblighi contrattuali assunti;
- promuovere un ambiente di lavoro rispettoso, professionale, sicuro e orientato al merito;
- adottare comportamenti trasparenti nei rapporti con clienti, fornitori, partner, consulenti e Pubblica Amministrazione;
- assicurare la corretta gestione di documenti, dati, credenziali, sistemi informatici e informazioni aziendali;
- prevenire conflitti di interesse, discriminazioni, abusi, indebite pressioni e utilizzi impropri delle risorse aziendali.

1.5 Rapporti con il personale

La società valorizza competenze, formazione e responsabilità individuale. Non sono ammessi comportamenti discriminatori, intimidatori, lesivi della dignità o contrari alla normativa su salute e sicurezza sul lavoro. Ogni destinatario è tenuto a mantenere un comportamento corretto, collaborativo e rispettoso.

1.6 Rapporti con clienti, partner e fornitori

Ogni rapporto commerciale deve basarsi su criteri oggettivi, trasparenti e documentabili. La selezione di partner e fornitori deve essere coerente con l'interesse aziendale, la qualità del servizio richiesto e adeguati presidi di affidabilità, reputazione e conformità normativa.

1.7 Rapporti con la Pubblica Amministrazione

Nei rapporti con enti pubblici, pubblici ufficiali o incaricati di pubblico servizio è vietata qualsiasi promessa, offerta o dazione indebita di denaro, utilità, vantaggi o favori finalizzati a ottenere trattamenti di favore, autorizzazioni, contributi, provvedimenti o omissioni non dovuti.

1.8 Riservatezza, dati e strumenti aziendali

- i dati e le informazioni acquisiti nello svolgimento dell'attività devono essere trattati secondo necessità, pertinenza, riservatezza e minimizzazione;
- l'utilizzo di sistemi, credenziali, software, device, accessi remoti e ambienti cliente deve avvenire solo per finalità legittime e autorizzate;
- ogni destinatario è tenuto a rispettare le policy interne su sicurezza informatica, protezione dei dati, backup, continuità operativa e gestione degli accessi.

1.9 Conflitto di interessi

Ogni destinatario deve evitare situazioni in cui interessi personali, familiari o di terzi possano interferire con l'imparzialità delle decisioni assunte per conto della società. Eventuali situazioni di conflitto, anche solo potenziale, devono essere comunicate tempestivamente secondo le procedure interne.

1.10 Segnalazioni e violazioni

Le violazioni del Codice Etico devono essere segnalate tramite i canali interni adottati dalla società, ivi incluso il canale whistleblowing gestito mediante piattaforma WithSecure. È garantita la gestione riservata della segnalazione e la tutela del segnalante nei limiti di legge e delle procedure aziendali applicabili.

2. Codice di Condotta Anti-Corruzione

2.1 Finalità

Il presente Codice di Condotta Anti-Corruzione integra il Codice Etico e definisce le regole specifiche adottate dalla società per prevenire fenomeni corruttivi, promesse indebite, pressioni improprie, vantaggi illeciti o pratiche opache nei rapporti con soggetti pubblici e privati.

2.2 Principio di tolleranza zero

DIMEDP CONSULTING SRL adotta un principio di tolleranza zero verso ogni forma di corruzione, attiva o passiva, diretta o indiretta, pubblica o privata. È vietato offrire, promettere, richiedere o accettare denaro, beni, servizi, omaggi, utilità o altre forme di vantaggio indebito.

2.3 Ambito soggettivo

Le presenti regole si applicano ad amministratori, management, dipendenti, collaboratori, consulenti, partner commerciali, rivenditori, intermediari e fornitori, nei limiti di compatibilità con il rapporto in essere.

2.4 Divieti specifici

- corrispondere o accettare somme non dovute, anche tramite soggetti terzi o prestanome;
- riconoscere compensi non giustificati o sproporzionati rispetto alla prestazione effettiva;
- omettere controlli o alterare documentazione per facilitare vantaggi indebiti;
- utilizzare contanti o flussi non tracciabili oltre i limiti consentiti e fuori procedura;
- creare fondi occulti o registrazioni contabili false, incomplete o ingannevoli.

2.5 Regali, omaggi, ospitalità e spese di rappresentanza

Sono ammessi solo omaggi e forme di ospitalità di modico valore, occasionali, leciti, coerenti con la normale cortesia commerciale e mai idonei a influenzare l'indipendenza del destinatario o a generare l'apparenza di un vantaggio indebito. La società potrà integrare la presente regola con soglie economiche e flussi autorizzativi interni.

2.6 Rapporti con la Pubblica Amministrazione

- ogni contatto con soggetti pubblici deve essere gestito da persone autorizzate e, ove opportuno, tracciato;
- è vietato ottenere o tentare di ottenere contributi, agevolazioni, licenze o autorizzazioni tramite informazioni non veritiere o omissioni rilevanti;
- in caso di bandi, finanziamenti o verifiche ispettive, la documentazione trasmessa deve essere completa, veritiera e controllabile.

2.7 Consulenti, intermediari, partner e fornitori

Prima dell'avvio del rapporto e durante la sua esecuzione devono essere valutati affidabilità, reputazione, coerenza del compenso, titolarità effettiva del rapporto, eventuali conflitti di interesse e presenza di clausole contrattuali di conformità normativa e 231/anticorruzione.

2.8 Registrazioni contabili e controlli

Ogni operazione deve risultare supportata da documentazione idonea e da una registrazione completa, corretta, tempestiva e verificabile. Nessuna operazione può essere occultata, artificiosamente frazionata o rappresentata in modo non fedele.

2.9 Segnalazioni

Ogni richiesta indebita, anomalia, pressione impropria o sospetto di condotta corruttiva deve essere segnalata con tempestività attraverso i canali interni adottati dalla società, ivi incluso il canale whistleblowing gestito mediante piattaforma WithSecure, secondo quanto previsto dalla procedura aziendale vigente.

2.10 Misure conseguenti

Le violazioni del presente Codice costituiscono inadempimento rilevante e possono comportare sanzioni disciplinari, risoluzione del rapporto contrattuale, attivazione di audit interni, segnalazioni agli organi societari e, ove necessario, alle autorità competenti.

3. Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 - Parte Generale

3.1 Premessa

DIMEDP CONSULTING SRL adotta il presente Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 8 giugno 2001, n. 231, con l'obiettivo di prevenire la commissione dei reati-presupposto rilevanti per la società e di rafforzare un sistema di gestione improntato a legalità, controllo, tracciabilità e responsabilità.

3.2 Obiettivi del Modello

Il Modello mira a individuare i processi sensibili, definire protocolli di prevenzione, attribuire responsabilità chiare, disciplinare i flussi informativi e rendere effettivo il sistema di controllo interno e di vigilanza.

3.3 Destinatari del Modello

Il Modello si applica a organi sociali, dipendenti, dirigenti, collaboratori, consulenti, partner, fornitori e terzi che operano in nome o per conto della società, nei limiti di compatibilità con la natura del rapporto.

3.4 Assetto aziendale

Campo / tema	Contenuto
Attività societaria	DIMEDP CONSULTING SRL opera nell'ambito della consulenza ICT, della system integration, dei software gestionali ed ERP, della business continuity, della cyber security e dei servizi tecnico-specialistici collegati alla gestione applicativa, sistemistica e database.
Organizzazione	Presidente: Otello Volpato. Amministratore Delegato: Dott. Claudio Guarracino. Responsabile IT area Cyber Security & Sistemi: Enrico Pivetta. DBA Oracle: Stefano Cappa. Responsabile Progetti ERP: Dott. Claudio Guarracino. L'assetto organizzativo è improntato a una struttura snella con presidio diretto delle aree direzionali, progettuali, sistemistiche, di sicurezza informatica e di gestione database.
Sistemi e processi	I processi rilevanti comprendono, in via esemplificativa, gestione offerte e ordini, pianificazione e delivery di progetto, assistenza tecnica e accesso remoto ai sistemi cliente, gestione credenziali e ambienti applicativi, presidio

Campo / tema	Contenuto
	infrastrutturale e sicurezza informatica, amministrazione dei database Oracle, whistleblowing tramite piattaforma WithSecure e gestione documentale/compliance, inclusi i presidi privacy/GDPR tramite portale TeamSystem Digital.
Rapporti esterni	La Società intrattiene rapporti con clienti privati, partner tecnologici, fornitori ICT, vendor software, consulenti e soggetti terzi coinvolti nella delivery dei servizi. I rapporti con controparti pubbliche o assimilabili, ove presenti, devono essere gestiti secondo criteri di tracciabilità, autorizzazione e rispetto delle regole interne richiamate dal presente Modello.

3.5 Metodologia di predisposizione e aggiornamento

La predisposizione del Modello si fonda su analisi organizzativa, mappatura delle attività sensibili, individuazione dei possibili reati-presupposto, verifica dei controlli esistenti e definizione o formalizzazione di procedure e protocolli. Il Modello deve essere aggiornato in caso di modifiche normative, variazioni organizzative, introduzione di nuovi servizi o emersione di criticità rilevanti.

3.6 Principi generali di controllo

La società adotta e mantiene, in misura proporzionata alla propria struttura e complessità, i seguenti principi di controllo:

- separazione dei compiti e chiara attribuzione delle responsabilità;
- sistema autorizzativo coerente con ruoli, poteri e procure;
- tracciabilità delle decisioni, delle attività e dei flussi approvativi più rilevanti;
- controlli preventivi, successivi e campionari sulle operazioni sensibili;
- archiviazione ordinata e reperibile della documentazione;
- flussi informativi verso gli organi societari e verso l'Organismo di Vigilanza.

3.7 Organismo di Vigilanza

La società prevede un presidio di vigilanza sul funzionamento e sull'osservanza del Modello, improntato ai principi di autonomia, indipendenza, professionalità e continuità d'azione, con il compito di monitorarne l'efficacia, promuoverne l'aggiornamento, ricevere i flussi informativi rilevanti e riferire periodicamente agli organi societari secondo l'assetto organizzativo adottato dalla Società.

3.8 Flussi informativi verso l'OdV

Devono essere gestiti con tempestività, secondo modalità organizzative coerenti con l'assetto della Società, almeno i seguenti flussi informativi rilevanti: violazioni o sospette violazioni del Modello, del Codice Etico o del Codice Anti-Corruzione; contenziosi, ispezioni, accertamenti o richieste dell'autorità; anomalie gestionali, incidenti di sicurezza, procedimenti disciplinari rilevanti; modifiche organizzative o operative significative; rapporti con soggetti pubblici o assimilabili di particolare rilievo; eventi che possano incidere

sull'efficacia dei presidi di controllo. Il canale whistleblowing e gli ulteriori flussi documentali rilevanti costituiscono parte integrante del presente Modello.

3.9 Sistema disciplinare

La società adotta un sistema disciplinare coerente con il proprio assetto e con i contratti applicabili, idoneo a sanzionare il mancato rispetto del Modello, del Codice Etico, del Codice Anti-Corruzione e dei presidi operativi richiamati dal presente documento, da parte di dipendenti, dirigenti, amministratori, consulenti, partner e fornitori.

In particolare:

• per i dipendenti, le violazioni sono sanzionate secondo la normativa applicabile, il contratto di lavoro, il CCNL di riferimento e le regole disciplinari interne della Società;

• per i dirigenti e gli altri soggetti apicali, la violazione del Modello può comportare misure organizzative e contrattuali proporzionate, ivi inclusa la revisione o revoca di deleghe, poteri o incarichi;

• per gli amministratori, la violazione è valutata dall'organo competente ai fini dell'adozione dei provvedimenti consentiti dall'ordinamento societario e dall'eventuale azione di responsabilità;

• per consulenti, collaboratori, partner e fornitori, il mancato rispetto dei presidi richiamati dal presente Modello costituisce inadempimento contrattuale e può comportare diffida, sospensione, risoluzione del rapporto, esclusione da ulteriori affidamenti e richiesta di risarcimento del danno, nei limiti di legge e del contratto applicabile.

3.9.1 Presidi operativi minimi

In assenza di procedure formalizzate autonome su tutti i processi sensibili, il presente Modello stabilisce quali presidi operativi minimi immediatamente applicabili e vincolanti per i destinatari:

• tracciabilità nella selezione e nell'affidamento a fornitori, consulenti, partner e subfornitori, con adeguata evidenza delle verifiche svolte e delle autorizzazioni interne;

• autorizzazione, assegnazione, utilizzo e revoca degli accessi ai sistemi, alle credenziali e agli ambienti cliente secondo criteri di necessità, profilazione e tracciabilità;

• presidio della sicurezza informatica, della gestione degli incidenti, dei backup, dei log e della continuità operativa in coerenza con i ruoli tecnici interni e con gli strumenti adottati dalla Società;

• corretta gestione dei dati personali e della documentazione GDPR tramite i presidi organizzativi e documentali gestiti sul portale TeamSystem Digital;

• tracciabilità di spese, omaggi, utilità, note spese, sponsorizzazioni o altre liberalità, che devono essere coerenti con finalità lecite, autorizzate e documentabili;

• gestione tracciata dei rapporti con la Pubblica Amministrazione o con soggetti assimilabili, ove presenti, con divieto di offerte o utilità indebite e con adeguata autorizzazione interna;

• tracciabilità delle attività progettuali ERP, delle attività di assistenza tecnica, degli accessi remoti, degli interventi sui sistemi cliente e delle attività DBA su ambienti Oracle, nei limiti degli strumenti e delle modalità operative adottate dalla Società.

3.10 Formazione, informazione e diffusione

Il Modello deve essere diffuso internamente ed esternamente in misura coerente con i soggetti interessati. La Società assicura adeguate attività di informazione, sensibilizzazione e aggiornamento documentale, in forma proporzionata ai ruoli, alle responsabilità e ai processi sensibili interessati.

3.11 Sistema di segnalazione interna (Whistleblowing) e presidi GDPR

La Società ha attivato un canale interno di segnalazione conforme al D.Lgs. 24/2023, finalizzato a consentire la segnalazione di violazioni normative e di condotte illecite rilevanti anche ai fini del presente Modello, nel rispetto dei principi di riservatezza, protezione del segnalante e divieto di ritorsione.

Il canale interno è gestito mediante piattaforma WithSecure, adottata dalla Società quale strumento tecnico per la ricezione e la gestione delle segnalazioni. La gestione delle segnalazioni è disciplinata da apposita procedura aziendale, che definisce i soggetti legittimati a segnalare, le modalità di invio, ricezione e istruttoria, i tempi di riscontro, le tutele di riservatezza e le misure di conservazione della documentazione.

La Società assicura che il sistema whistleblowing sia coerente con la normativa vigente e con i principi richiamati nel presente Modello. Per gli aspetti operativi di dettaglio si rinvia alla procedura whistleblowing aziendale vigente tempo per tempo adottata.

Con riferimento ai presidi in materia di protezione dei dati personali, la Società gestisce gli adempimenti e la documentazione GDPR tramite il portale TeamSystem Digital, quale ambiente di supporto organizzativo e documentale per l'aggiornamento delle informative, dei registri, delle procedure e degli altri presidi privacy applicabili.

4. Parti Speciali del Modello 231

Le seguenti Parti Speciali essenziali individuano, in forma sintetica ma operativa, le principali famiglie di reato rilevanti per la Società, le attività sensibili maggiormente esposte e i presidi minimi di comportamento e controllo da applicare.

Parte Speciale essenziale	Attività / processi sensibili	Presidi minimi previsti
Reati contro la Pubblica Amministrazione	Partecipazione a bandi, agevolazioni, richieste autorizzative, rapporti con enti, verifiche ispettive e interlocuzioni con pubblici ufficiali o incaricati di pubblico servizio	Autorizzazione preventiva, tracciabilità dei contatti e dei documenti trasmessi, divieto di utilità indebite, conservazione delle evidenze e informativa all'OdV per eventi rilevanti
Reati informatici e trattamento illecito di dati	Accessi remoti a sistemi cliente, gestione credenziali, supporto applicativo, sicurezza, log, dati, ambienti IT e attività DBA su database Oracle	Profilazione e tracciamento accessi, uso autorizzato delle credenziali, logging, gestione incidenti, backup, protezione dei dati e rispetto dei presidi GDPR

Parte Speciale essenziale	Attività / processi sensibili	Presidi minimi previsti
Corruzione tra privati	Relazioni commerciali, rete partner, intermediari, vendor, regalie, spese di rappresentanza, negoziazioni e affidamenti	Documentazione delle trattative, controllo su omaggi e spese, verifica reputazionale delle controparti, approvazione interna delle condizioni economiche e divieto di vantaggi indebiti
Reati societari	Flussi amministrativi, rappresentazione contabile, deleghe, poteri, reporting e documentazione societaria	Corretta tenuta delle evidenze, segregazione dei ruoli, coerenza con deleghe e procure, verificabilità delle registrazioni e conservazione della documentazione rilevante
Riciclaggio e autoriciclaggio	Incassi e pagamenti, selezione consulenti e fornitori, tracciabilità dei flussi, verifica controparte	Pagamenti tracciabili, verifica della controparte, coerenza economica dei contratti, divieto di operazioni anomale e segnalazione interna di criticità rilevanti
Reati tributari	Gestione documentale, fatturazione, note spese, supporto amministrativo e conservazione evidenze	Completezza e veridicità della documentazione, autorizzazione dei rimborsi, archiviazione ordinata, collaborazione con i consulenti competenti e divieto di condotte elusive o fraudolente
Salute e sicurezza sul lavoro	Attività presso sedi cliente, trasferte, gestione interferenze e adempimenti D.Lgs. 81/2008	Cooperazione con il cliente, rispetto delle prescrizioni di sicurezza, gestione dei rischi interferenziali e tracciabilità delle comunicazioni e delle autorizzazioni rilevanti
Diritti d’autore e proprietà intellettuale	Software, licenze, codice, documentazione tecnica, materiale di terzi, repository e ambienti di sviluppo	Utilizzo legittimo di software e materiali, rispetto di licenze e diritti di terzi, controllo sui repository e tutela della documentazione tecnica e dei contenuti proprietari

5. Presidi e documenti organizzativi richiamati dal Modello

Il presente Modello richiama i seguenti presidi e documenti organizzativi, da mantenere coerenti con l'assetto della Società e aggiornati nel tempo in quanto adottati e applicabili.

Presidio / documento	Modalità di richiamo nel Modello
Sistema disciplinare	Disciplina richiamata al paragrafo 3.9 del presente Modello, applicabile a dipendenti, soggetti apicali, amministratori e terzi in funzione della natura del rapporto.
Presidio di vigilanza	Presidio di vigilanza richiamato al paragrafo 3.7, da organizzare secondo l'assetto adottato dalla Società e coerente con i principi di autonomia, indipendenza, professionalità e continuità d'azione.
Whistleblowing	Canale interno attivo mediante piattaforma WithSecure, disciplinato dalla procedura aziendale vigente e coordinato con i flussi informativi e i presidi di controllo interni.
Presidi operativi minimi	Regole immediatamente applicabili richiamate nel presente Modello per fornitori e partner, accessi ai sistemi, sicurezza informatica, gestione dati, spese e rapporti con la Pubblica Amministrazione.
Deleghe e procure	Sistema autorizzativo e dei poteri, ove formalizzato, da mantenere coerente con l'assetto organizzativo, con la documentazione societaria e con le responsabilità effettivamente attribuite.
Presidi GDPR	Presidi privacy e documentazione GDPR gestiti tramite portale TeamSystem Digital, da coordinare con ruoli, responsabilità e misure organizzative applicabili.
Documentazione organizzativa	Ulteriore documentazione interna utile a dare attuazione al presente Modello, in quanto adottata e applicabile, da mantenere coerente con l'assetto e i processi della Società.
Aggiornamento periodico	Il Modello e i relativi presidi sono soggetti a riesame e aggiornamento in relazione a modifiche normative, organizzative o operative rilevanti.

Il presente documento costituisce il riferimento organizzativo e comportamentale della Società in materia di etica, prevenzione della corruzione e presidi ex D.Lgs. 231/2001, da coordinare con la documentazione organizzativa e gli aggiornamenti periodici applicabili.