DISCIPLINARE DEL TRATTAMENTO DEI DATI

a cura di

CNA Ferrara

Per l'AZIENDA: *DELTA 2000 SOC. CONS A R.L.*

Ambito generale

Politica aziendale

La nostra Azienda al fine di rispettare il Regolamento Europeo 2016/679 e le Disposizioni successive relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, ha predisposto la seguente documentazione al fine di fornire istruzioni chiare sulla corretta gestione dei dati e degli strumenti aziendali.
L'organizzazione mira a sensibilizzare i propri operatori alla salvaguardia del diritto alla riservatezza degli utenti ed orientarne le azioni al rispetto delle dovute cautele.

Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone DELTA 2000 SOC. CONS A R.L. e gli Utenti (dipendenti e collaboratori) a rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Azienda stessa.
*L'ambito lavorativo porta l'organizzazione e gli Utenti a gestire una serie di "**informazioni**", proprie e di terzi, per poter erogare i servizi che le vengono contrattualmente richiesti. **I dati di cui gli utenti vengono a conoscenza, nell'ambito della propria attività lavorativa, sono da considerarsi riservati e non devono essere comunicati o diffusi a nessuno (anche una volta cessato il rapporto lavorativo con l'organizzazione stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita dell'Azienda.** Anche tra colleghi, oppure tra dipendenti e collaboratori esterni vige la regola che impone la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi esclusivamente a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.*
Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, DELTA 2000 SOC. CONS A R.L. ha predisposto il seguente documento interno diretto ad evitare anche comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.
Chiediamo a tutti un'attenta lettura e il massimo rispetto del Disciplinare.

Operazioni volte alla protezione della postazione di lavoro

Utilizzo e protezione della postazione di lavoro

La postazione di lavoro (pc, terminale o notebook) assegnata all'utente è uno strumento di lavoro.
I dispositivi non devono essere utilizzati per finalità non inerenti l'attività lavorativa se non eccezionalmente.
L'utilizzo non autorizzato dei Device può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce.
La postazione di lavoro deve essere custodita con cura evitando ogni possibile forma di danneggiamento. È necessario che gli incaricati conservino le postazioni di lavoro nella configurazione loro assegnata; gli è quindi vietato:

- togliere/aggiungere/cambiare componenti hardware e software;
- cambiare l'ubicazione delle apparecchiature,

senza la preventiva autorizzazione di DELTA 2000 SOC. CONS A R.L..

Login e Logout

È obbligatoria l'assegnazione di credenziali di autenticazione per ogni singolo utente.
Tale obbligo viene assolto mediante l'operazione iniziale di "Login"[1] con la quale l'Incaricato si connette al sistema

[1] procedura di accesso a un sistema informatico riservato mediante l'inserimento di un codice identificativo e di una parola d'ordine da parte dell'utente.

aziendale o a una parte di esso, dichiarando il proprio Username e Password (ossia l'Account) e aprendo una sessione di lavoro. L'incaricato, finita la sessione di lavoro è tenuto a effettuare il "Logout"[2] dall'Account di sua appartenenza. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.

Obblighi in capo all'Utente

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.

L'incaricato deve quindi eseguire le operazioni seguenti:

- In caso di allontanamento dalla postazione di lavoro è necessario utilizzare la funzione "blocco del computer" con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla. Tale operazione permette di mettere in protezione il Device affinché persone non autorizzate non abbiano accesso ai dati protetti;
- Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente nel caso in cui siano rilevati virus;
- Chiudere la sessione (Logout) a fine giornata;
- Spegnere il PC dopo il Logout;
- Controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del dispositivo.

Password

Assegnazione e gestione di credenziali di autenticazione

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (User id), assegnato associato a una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e dell'ente nel suo complesso.

L'incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni tre mesi dovrà procedere alla modifica della Password. Il sistema avvertirà l'utente della scadenza della password e della necessità di modifica della stessa.

Altra buona regola è quella di evitare di memorizzare la password su supporti facilmente accessibili da altre persone. La miglior soluzione è conservare la propria password nella propria memoria.

L'organizzazione si riserva la facoltà di revocare l'incaricato dalla possibilità di accedere a determinati sistemi hardware o software mediante la rimozione delle sue credenziali d'accesso

Nel tempo anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza.

Regole per la corretta gestione delle password

L'Incaricato, da parte sua, per una corretta e sicura gestione delle proprie password deve rispettare le regole seguenti:

1. Occorre cambiare immediatamente una password non appena si abbia il dubbio che sia diventata poco "sicura";
2. Le password sono formate da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'incaricato.;

[2] procedura che consente di terminare l'attività in un'area riservata di un sistema informatico, alla quale l'utente ha avuto accesso mediante l'operazione di login.

3. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
4. Le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password.
5. Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'ente;
6. Le password sono assolutamente personali e non vanno mai comunicate ad altri;
7. non deve essere uguali alle precedenti.

In alcuni casi, sono implementati meccanismi che consentono all'Incaricato fino ad un numero limitato di tentativi errati di inserimento della password oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account può essere bloccato.

Divieto di uso

Al fine di una corretta gestione delle password, è fatto divieto di utilizzo come propria password di:

1. Nome, cognome e loro parti;
2. Lo username assegnato;
3. Un indirizzo di posta elettronica (e-mail);
4. Parole comuni (in Inglese e in Italiano);
5. Date, mesi dell'anno e giorni della settimana, anche in lingua straniera;
6. Parole banali e/o di facile intuizione, ad es. pippo, security e palindromi (simmetria: radar);
7. Ripetizioni di sequenze di caratteri (es. abcabcabc);
8. Una password già impiegata in precedenza.

La password nei sistemi

Ogni Incaricato può variare autonomamente la propria password di accesso, qualora il sistema in questione metta a disposizione degli Utenti una funzionalità di questo tipo (Change password), oppure facendone richiesta al Titolare. La password può essere sostituita dal Titolare, anche qualora l'Utente l'abbia dimenticata.

Uso del personal Computer dell'ente

Corretto utilizzo del COMPUTER aziendale

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Il computer che viene consegnato contiene tutti i software necessari a svolgere le attività affidate dall'organizzazione. Per necessità aziendali, gli amministratori di sistema utilizzando la propria login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente documento, sia alle memoria di massa locali di rete (repository e backup) che ai server aziendali nonché, previa comunicazione al dipendente, accedere al computer, anche in remoto.

In particolare l'Incaricato deve adottare le seguenti misure:

1. Utilizzare solo ed esclusivamente le aree di memoria della rete dell'ente ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri files fuori dalle unità di rete;
2. Spegnere il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché 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;
3. Mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), disposti dall'organizzazione;
4. Non dare accesso al proprio computer ad altri utenti, a meno che siano incaricati con cui condividono l'utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

Divieti Espressi sull'utilizzo del COMPUTER

All'incaricato è vietato:

1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali dell'incaricato o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere.
2. Modificare le configurazioni già impostate sul personal computer.
3. Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta dell'ente.
4. Installare alcun software di cui l'ente non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione dell'organizzazione. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale.
5. Caricare sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.
6. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell'organizzazione.
7. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'organizzazione, quali per esempio virus, trojan horses ecc.
8. Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.
9. Effettuare in proprio attività manutentive.
10. Permettere attività manutentive da parte dei soggetti non espressamente autorizzati dell'organizzazione.

Antivirus

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, via mail ...

Per questo DELTA 2000 SOC. CONS A R.L. ha disposto su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.

L'incaricato, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer, e, in particolare, deve rispettare le regole seguenti:

1. Comunicare all'ente ogni anomalia o malfunzionamento del sistema antivirus;
2. Comunicare all'ente eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, all'incaricato:

1. È vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione;
2. È vietato ostacolare l'azione dell'antivirus aziendale;
3. È vietato disattivare l'antivirus senza l'autorizzazione espressa dell'ente anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer;
4. È vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani.

Contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

Posta elettronica

La Posta Elettronica è uno strumento di lavoro

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo i casi di assegnazione di notebook e/o telefoni cellulari ad uso promiscuo. Anche in questi ultimi casi sarà comunque necessario attenersi alle misure di salvaguardia della sicurezza nel trattamento dei dati aziendali; in caso di ricezione sulla e-mail aziendale di posta personale si avverte di cancellare immediatamente ogni messaggio al fine di evitare ogni eventuale e possibile back up dei dati;

avvisare l'organizzazione quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

È inoltre espressamente vietato, salvo autorizzazione espressa del proprio Responsabile, salvare/stampare/inoltrare e portare fuori dai luoghi di lavoro documentazione aziendale. A titolo esemplificativo e non esaustivo è vietato:

- stampare e-mail aziendali per scopi personali;
- inviare informazioni sensibili ad indirizzi di posta personali;
- fotocopiare/scansionare documentazione aziendale per scopi personali;
- inoltrare a terzi estranei all'azienda documentazione interna/informazioni ricevute per mezzo di strumenti informatici o via cartacea, salvo che non sia funzionale allo svolgimento di prestazioni professionali a favore della stessa Azienda.
- È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio dell'organizzazione per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'organizzazione, nonché utilizzare il dominio dell'organizzazione per scopi personali.
- È vietato redigere messaggi di posta elettronica utilizzando l'indirizzo aziendale, diretti a destinatari esterni dell'organizzazione, senza utilizzare il seguente disclaimer:

  "Questo messaggio di posta elettronica contiene informazioni di carattere confidenziale rivolte esclusivamente al destinatario sopra indicato. E' vietato l'uso, la diffusione, distribuzione o riproduzione da parte di ogni altra persona. Nel caso aveste ricevuto questo messaggio di posta elettronica per errore, siete pregati, di segnalarlo immediatamente al mittente e distruggere quanto ricevuto (compresi i file allegati) senza farne copia. Qualsivoglia utilizzo non autorizzato del contenuto di questo messaggio costituisce violazione dell'obbligo di non prendere cognizione della corrispondenza tra altri soggetti, salvo più grave illecito, ed espone il responsabile alle relative conseguenze.

  Informativa Privacy: Si avvisa che eventuali sue risposte, potranno essere lette dal sottoscritto e da altri operatori di nome, se competenti sulla sua richiesta."

- È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.
- È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.

Gli Incaricati possono avere in utilizzo indirizzi nominativi di posta elettronica.

Le caselle e-mail possono essere assegnate con natura impersonale (tipo info@xxx.it, info, amministrazione, fornitori, direttore, direttore sanitario, consulenza, ecc...) proprio per evitare ulteriormente che il destinatario delle mail possa considerare l'indirizzo assegnato al dipendente "privato", ai sensi dei suggerimenti del Garante a tal proposito. Gli Incaricati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Posta Elettronica in caso di assenze programmate ed assenze non programmate

Nel caso di assenza prolungata sarebbe buona norma attivare il servizio di risposta automatica (Auto- reply).
In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, l'Incaricato deve nominare un collega fiduciario con lettera scritta che in caso di assenza inoltri i files necessari a chi ne abbia urgenza.
Qualora l'Incaricato non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, l'organizzazione, mediante personale appositamente incaricato, potrà verificare il contenuto dei messaggi di posta elettronica dell'incaricato, informandone l'incaricato stesso e redigendo apposito verbale.

Utilizzo Illecito di Posta Elettronica

1. È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
2. È vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
3. Qualora l'Incaricato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'organizzazione.

Internet

Internet è uno strumento di lavoro

La connessione alla rete internet dal dispositivo avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento.

In particolare si vieta l'utilizzo dei social network, in orario di lavoro.

Uso di altri dispositivi (PC Portatile, Tablet, Smartphone e di altri Device elettronici)

L'utilizzo del notebook, tablet o smartphone

L'utente è responsabile dei dispositivi mobili assegnatogli da DELTA 2000 SOC. CONS A R.L. e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai dispositivi mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare i files creati o modificati sui Device devono essere trasferiti sulle memorie di massa aziendali al primo rientro in ufficio e cancellati in modo definitivo dai Device mobili (Wiping). I Device mobili utilizzati all'esterno (convegni, visite in azienda, ecc...), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto deve far seguito la denuncia alle autorità competenti.
All'Incaricato è vietato lasciare i device mobili incustoditi e a vista dentro l'auto o in luoghi accessibili.
Laddove il device mobile sia accompagnato da un'utenza, l'Incaricato è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, ...) e a rispettarli. Qualora esigenze lavorative richiedessero supporti differenti l'Incaricato è tenuto ad informare tempestivamente e preventivamente l'ente.

Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc.)

Agli Incaricati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, ...) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, ...).

I supporti rimovibili quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.).

Device personali

Per evitare rischi di "contaminazione"ai dipendenti non è permesso svolgere la loro attività con strumentazione personale (PC fissi, portatili, device).

Al dipendenti, se espressamente autorizzati dall'ente, è permesso solo l'utilizzo della posta elettronica aziendale sui loro device personali.

In tal caso è necessario che il device abbia password di sicurezza stringenti approvate dall'ente e l'eventuale furto o smarrimento del device deve essere immediatamente segnalato anche all'ente per eventuali provvedimenti di sicurezza.

Al collaboratore è vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, ...).

Gli Incaricati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri device personali per memorizzare dati dell'ente solo se espressamente autorizzati dall'ente stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Distruzione dei Device

Ogni Device ed ogni memoria esterna affidati agli incaricati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all'ente che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.

In particolare l'ente provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

Istruzioni per l'uso degli strumenti "non elettronici"

Clear Desk Policy

Gli Incaricati sono responsabili del controllo e della custodia, degli atti e dei documenti contenenti dati personali per tutto il tempo di svolgimento delle operazioni di trattamento.

L'Incaricato deve attenersi a una serie di prescrizioni:

- in nessun caso è consentito l'accesso a documentazione contenente Dati Personali per motivi differenti da esigenze di lavoro;
- Gli Incaricati sono invitati dall'organizzazione ad adottare una "politica della scrivania pulita": la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
- i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non sicuro (ad es. a seguito della stampa dei documenti su stampante di rete);
- cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
- la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;
- dove non siano presenti strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio esterni di distruzione, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo;
- è vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

È obbligatorio per tutti gli Utenti attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e delle successive disposizioni.

Validità, aggiornamento ed affissione

Validità

Il presente Disciplinare ha validità a partire dalla data di comunicazione dello stesso.

Aggiornamento

Il presente Disciplinare sarà oggetto di aggiornamento quando sarà ritenuto necessario, in caso di variazioni tecniche dei sistemi dell'organizzazione o in caso di mutazioni legislative.
Ogni variazione del presente Disciplinare sarà comunicata agli incaricati.

DELTA 2000 Soc. cons.ar.l.
IL PRESIDENTE
LORENZO MARCHESINI

Firma del Titolare