

~ 1 ~

STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)

**DISCIPLINARE AZIENDALE  
PER L'USO DEGLI STRUMENTI  
ELETTRONICI E PER LA  
GESTIONE DEI DATI  
AZIENDALI**

<b>Anno</b>	<b>2014</b>
<b>Versione</b>	<b>1/2014</b>

## ***INDICE GENERALE***

- **A) Introduzione**
- **B) Le fonti normative**
- **C) Glossario**
- **D) Il sistema di gestione dei dati aziendali**
- **E) La tutela della riservatezza**
- **F) La tutela copyright**
- **G) L'organigramma dei ruoli privacy**
- **H) La gestione del dato sensibile**
- **I) La gestione dell'accesso ai documenti personali**
- **L) Il personal computer**
- **M) I software aziendali**
- **N) L'uso della fotocopiatrice**
- **O) Le attività ludiche**
- **P) La gestione dell'errore e del guasto tecnico**
- **Q) La gestione dell'anomalia**
- **R) La comunicazione dei dati nel web**
- **S) La regola per l'uso dei dispositivi di firma**

- T) L'uso dei supporti usb
- U) La gestione dei profili di accesso
- V) Le regole per l'uso del telefono aziendale
- Z) Le regole per l'uso di internet
- W) Le regole per l'uso della posta elettronica
- X) Antiriciclaggio
- Y) Le attività informative e formative
- X1) Conservazione sostitutiva
- XX.1) Il piano di monitoraggio della sicurezza dei dati
- XX) La disciplina dei controlli
- YY) Conclusioni
- DOCUMENTI ALLEGATI
  - Organigramma degli Amministratori di Sistema ALLEGATO A)
  - Analisi dei Rischi Informatici ALLEGATO B)
  - Procedura per la gestione e la conservazione delle password  
ALLEGATO C)
  - Procedura Delega conoscenza credenziali Utente ALLEGATO D)
  - Registro di Emergenza ALLEGATO E)
  - Comunicazione agli Utenti del Disciplinare Aziendale ALLEGATO F)

## **A) Introduzione**

La redazione di questo Disciplinare Aziendale sull'uso degli strumenti elettronici e sulla gestione dei dati risponde alle esigenze aziendali e normative di definire le regole precise per la tutela del Sistema Informativo della Studio Marco Mondadori.

Si precisa che, nel presente contesto, il termine Sistema Informativo comprende<< l'insieme delle informazioni utilizzate, prodotte e trasformate dalla Studio Marco Mondadori durante l'esecuzione dei processi aziendali e delle modalità in cui essi sono gestiti e dalle risorse sia umane che tecnologiche coinvolte>>. Tale concetto non deve essere confuso, né tantomeno considerato un sinonimo del termine Sistema Informatico ovvero<< la porzione di sistema che fa uso delle tecnologie informatiche e di automazione>>. Questo documento si integra con i diritti e doveri sanciti dal Codice Disciplinare di cui all'art 7, comma 1, Legge 20/05/1970, n. 300 (Statuto dei Lavoratori); unitamente a quanto sancito negli articoli 1775 e 1375 del codice civile che impongono al lavoratore i principi di correttezza e buona fede e di tenere un comportamento leale nei confronti del datore di lavoro astenendosi dal compiere qualsiasi atto idoneo a nuocergli anche potenzialmente.

Si rileva che i dati oggetto di trattamento devono essere custoditi in maniera tale da evitare accessi non autorizzati (ex art 31- 34 del Codice Privacy). Inoltre il trattamento dei dati con strumenti elettronici necessita dell'adozione di misure minime di sicurezza descritte nel Disciplinare Tecnico – Allegato B al D.lgs. 196/2003. Questo decreto prevede che vengano impartite istruzioni scritte :

- a) agli incaricati per non lasciare accessibile lo strumento elettronico;
- b) per individuare la modalità atta a garantire la disponibilità dei dati e/o degli strumenti elettronici in caso di prolungata assenza o impedimento dall'incarico.

La definizione di regole nell'uso degli strumenti elettronici e nell'organizzazione del flusso dei dati deve essere intesa come segno di trasparenza e di garanzia per tutti in quanto lo scopo principale è quello di evitare il generarsi di rischi che potrebbero provocare effetti lesivi dei diritti individuali.

*STUDIO MARCO MONDADORI*  
*Consulenza del Lavoro e Tributaria*  
*Viale Vittorio Veneto, 110*  
*62029 TOLENTINO (MC)*

D'altra parte si evidenzia la predominanza di comunicazione in forma digitale nell'ambito lavorativo ed, essendo tali processi in continua evoluzione, non è possibile sottrarsi dalla definizione di precisi confini, dalla determinazione di policy per una corretta operatività. Si parla di confini in quanto le regole di sicurezza di seguito descritte devono rispettare un giusto bilanciamento di interessi con le norme sancite dallo Statuto dei Lavoratori e dalle disposizioni presenti nel Codice Civile in materia di rapporto di lavoro. Pertanto l'oggetto principale di questo Disciplinare è il "modus operandi" dell'utente ovvero il rispetto di quanto stabilito dalla Studio Marco Mondadori per garantire l'integrità dei dati aziendali, per tutelare la loro sicurezza, per ottimizzare i processi lavorativi, per gestire e suddividere i compiti e le relative responsabilità in maniera trasparente ed equa.

Il presente documento è rivolto a tutti gli Utenti ovvero ad ogni singolo soggetto che presta un'attività lavorativa per conto dello scrivente studio a prescindere dalla tipologia contrattuale qualificante il rapporto di lavoro. Il Disciplinare può essere soggetto a modifiche che dovranno, comunque, essere comunicate agli Utenti e che saranno caratterizzate dal numero della versione, riportato nel frontespizio della copertina e dalla data di entrata in vigore.

Viene considerata *versione ufficiale*, il documento riportante la firma dell'Amministratore e del Responsabile del Trattamento dei Dati che sarà inoltrato agli Utenti attraverso i canali ufficiali di comunicazione aziendale ( affissione in bacheca, pubblicazione nel sito internet aziendale, invio tramite e.mail oppure tramite pec). La presente versione corrisponde alla prima versione dell'anno 2014 (vers. 1/2014).

• **STRUTTURA DEL DOCUMENTO**

Il documento è suddiviso in sessioni, ogni sessione è contraddistinta da una lettera progressiva e da un titolo che riguarda la trattazione di un determinato argomento di cui ne viene fornita una spiegazione generale.

Al suo interno, la sessione contiene la descrizione delle regole definite dallo Studio per l'uso degli strumenti elettronici e per la gestione dei dati.

Nell'ultima pagina del documento viene riportata la data di entrata in vigore delle policy e la firma del titolare, del Responsabile del Trattamento Dati e dell'Amministratore di Sistema.

Inoltre questa versione (1/2014) prevede l'integrazione di:

*STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)*

- Allegato A “Organigramma degli Amministratori di Sistema dello Studio Marco Mondadori Allegato B “Analisi dei Rischi Informatici”
- Allegato C “Procedura per la gestione e conservazione delle password”
- Allegato D “Procedura Delega conoscenza credenziale Utente”
- Allegato E “Registro di Emergenza”
- Allegato F “Comunicazione del Disciplinare agli Utenti”

### ***B)Le fonti normative***

In questo capitolo vengono elencate le principali fonti normative da cui traggono l'autorevolezza le regole contenute in questo documento.

- D. LGS. 196/2003 e s.m.i.
- CODICE PENALE ( art. 615 bis- 615 ter- Reati Informatici)
- CODICE CIVILE ( art. 2104- art. 2105- art. 1175- art. 1375)
- LEGGE 20/05/1970 N. 300 ( Statuto dei Lavoratori)
- PROVVEDIMENTO AUTORITA' GARANTE PRIVACY SUGLI AMMINISTRATORI DI SISTEMA ( anno 2009)
- CONVENZIONE EUROPEA SUI CRIMINI INFORMATICI
- D. LGS. 82/2005- D. LGS. 235/2010 ( Codice dell'Amministrazione Digitale)
- NORMATIVA FIRMA DIGITALE
- D. LGS. 69/2009 (Posta Elettronica certificata)
- CIRCOLARE MINISTERO DEL LAVORO E DELLE POLITICHE SOCIALI ( Maggio 2011)
- AUTORIZZAZIONE N 2/2013 AUTORITA' GARANTE PRIVACY ( dati sensibili nel rapporto di lavoro)
- AUTORIZZAZIONE N 7/2013 AUTORITA' GARANTE PRIVACY ( dati giudiziari)
- Normativa Diritto d'Autore e Codice della Proprietà Industriale
- Normativa sito web (luglio 2013)
- Provvedimento Autorità Garante Privacy relativo all'uso dei cookie (Maggio 2014)

- Codice del Consumatore –Modifiche apportate dal D.Lgs.21 febbraio 2014 n. 21 in materia di vendita a distanza;
- Direttiva 2010/45 UE e DM 55/2013 in materia di Fattura Elettronica nei confronti delle Pubbliche Amministrazioni.

### **C) Glossario**

- **SYSTEM ADMINISTRATOR** <<è colui che decide in autonomia, coordinandosi con il titolare, sulle policy di sicurezza della rete, sulla designazione dei compiti agli incaricati, sulle attività di monitoraggio; inoltre è colui che propone interventi migliorativi, decisione sugli acquisti ICT ed a volte budget in autonomia>>
- **NET ADMINISTRATOR** <<è colui che si occupa del networking: parco informatico presente, layout, funzionamento, assistenza, sicurezza, copie, posta elettronica, internet, dominio e sito>>
- **DATA ADMINISTRATOR** <<è colui che si occupa dell'amministrazione di base dati intendendo i software in uso e quindi tutta l'attività di programmazione e manutenzione>>
- **RESPONSABILE DEL TRATTAMENTO DEI DATI** <<un soggetto interno oppure esterno all'ente ed identificato quale persona fisica o giuridica preposta alla gestione ed al coordinamento del sistema privacy aziendale ed al suo controllo. Nel caso in cui le esigenze organizzative lo richiedono, possono essere nominati più responsabili di trattamento anche mediante suddivisione dei compiti>>
- **INCARICATI AL TRATTAMENTO DI TALUNE BANCHE DATI** << ogni soggetto che per mansione è chiamato a compiere determinate operazioni (elaborazione, consultazione, comunicazione, conservazione,interposizione etc.) sulle diverse tipologie di banche dati presenti. Nell'ambito di questo incarico generico devono essere individuati alcuni ruoli specifici come ad esempio: INCARICATO AL CONTROLLO DEL BACK UP- INCARICATI ALL'ACCESSO AGLI ARCHIVI STORICI>>
- **INCARICATI IN OUTSOURCING** <<ogni soggetto che per ambiti definiti in base a specifici rapporti di lavoro è demandato alla gestione, alla tenuta di alcune informazioni dell'Azienda Titolare presso la sua struttura. Normalmente questo ruolo comprende i consulenti, i partners con cui l'Azienda stipula contratti di servizio o di prestazione con modalità ed ambiti ben definiti>>

STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)

- **ATTO DI INCARICO** Ogni ruolo deve essere redatto per iscritto, collocato in un preciso riferimento temporale, deve aver evidenziate le principali fonti legislative, deve contenere in maniera precisa gli ambiti oggetto della connessa responsabilità, la sottoscrizione di entrambe le parti ( titolare/responsabile e incaricato) >>
  
- **INFORMATIVA PER IL PERSONALE IN MATERIA DI TRATTAMENTO DATI NEL RAPPORTO DI LAVORO**- è un documento con cui l'Azienda dichiara in trasparenza le modalità di gestione, le finalità ed i soggetti coinvolti nel processo di elaborazione e conservazione dei dati del personale in relazione al rapporto di lavoro in essere. Tale documento prescinde dalla tipologia contrattuale applicata alla parte interessata e può essere rilasciata diverse volte in seguito a variazioni nel modus operandi dell'Ente oppure in seguito all'emanazione di aggiornamenti legislativi.>>
  
- **ATTO DI INCARICO PER COLLABORATORI**: tale atto è rivolto a tutti i soggetti che in modalità di outsourcing per differenti ambiti e finalità interagiscono con le informazioni aziendali. Tale documento necessita della forma scritta e deve contenere le finalità precise del rapporto professionale in corso, quindi, la tipologia di banche dati interessate dalle attività di trattamento e le policy di sicurezza definite dall'azienda. E' importante indicare la data insieme alla sottoscrizione di entrambe le parti e l'eventuale arco temporale di riferimento delle regole indicate nel documento medesimo quale trasparenza dei diritti e doveri dell'incaricato>>
  
- **FIRMA DIGITALE**<<la firma digitale è un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici>>
  
- **LA POSTA ELETTRONICA CERTIFICATA (PEC)** è un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici. "Certificare" l'invio e la ricezione - i due momenti fondamentali nella trasmissione dei documenti informatici - significa fornire al mittente, dal proprio gestore di posta, una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale allegata documentazione. Allo stesso modo, quando il messaggio perviene al destinatario, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna con precisa indicazione temporale. Nel caso in cui il mittente smarrisca le ricevute, la traccia informatica delle operazioni svolte, conservata per legge per un periodo di 30 mesi, consente la riproduzione, con lo stesso valore giuridico, delle ricevute stesse>>



- **LA PASSWORD** <<è una sequenza alfanumerica priva di spazi che un utente deve inserire, in combinazione con un User-ID, per accedere ad un'area protetta di un computer, un sito o una rete. Per questi motivi, la password è nota solo all'utente e non deve essere divulgata a terzi.>>
  
- **PROFILO UTENTE** <<Creare o acquistare un ACCOUNT vuol dire fare una richiesta affinché vengano dati ad una persona un user ID e una password con i quali l'utente può accedere ad un servizio. Gli esempi più noti sono:  
1) l'account che si chiede ad un ISP per accedere ad Internet e alla posta elettronica  
2) l'account che un amministratore di rete crea per fare in modo che un dipendente acceda a determinati servizi di rete. Creare un account corrisponde a fornire i dati utente con cui essere riconosciuto univocamente quando si accede ad un servizio in rete. In informatica, attraverso il meccanismo dell'account, il sistema mette a disposizione dell'utente un ambiente con contenuti e funzionalità personalizzabili, oltre ad un conveniente grado di isolamento dalle altre utenze parallele. Il termine deriva dal gergo bancario, ed infatti in molte lingue la stessa parola indica un conto corrente ed un conto in banca, ad esempio in lingua inglese (*account*, parola presa in prestito in italiano) o polacco (*konto*), quasi ad evidenziare la possibilità di usufruire di servizi che ha un utente registrato ed identificato presso un sito web (paragonabile ai servizi del cliente che ha mostrato il proprio documento presso la sua banca). Infatti, il sistema informatico è in grado di riconoscere l'identità del titolare di un account, ne memorizza e conserva un insieme di dati ed informazioni attribuite ad esso, spesso da esso unicamente gestibili ed accessibili per un utilizzo futuro. In questo si differenzia da altre modalità di accesso a sistemi di servizio interattivi che non presuppongono la ripetizione del rapporto con l'utente.>>
  
- **HARDWARE** <<Tutto ciò che in un computer si riconosce fisicamente e quindi le periferiche, le parti elettriche, meccaniche, elettroniche ed ottiche>>
  
- **SOFTWARE** <<Software è un termine generico che definisce programmi e procedure utilizzati per far eseguire al computer un determinato compito. Viene in generale suddiviso in:  
- software di base o di sistema perchè è indispensabile al funzionamento del computer dal momento che senza di esso non sarebbe che hardware inutilizzabile. Viene identificato con il sistema operativo;  
- software applicativo. Esso comprende i programmi che il programmatore realizza utilizzando le prestazioni che offre il sistema operativo e tra essi troviamo ad esempio

**STUDIO MARCO MONDADORI**  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)

applicazioni gestionali destinati alle esigenze specifiche di un utente o di un'azienda e tutto ciò che riguarda l'[office automation](#).>>

- **INTRANET**<< inglese [da intra+net, rete interna], usato in italiano come sf. Sistema di rete privata, interna a una azienda, che utilizza i servizi della struttura di comunicazione locale LAN esistente e gli standard e i protocolli del World Wide Web (WWW). Creata e gestita direttamente dagli utenti in base alle loro esigenze, è utilizzata per facilitare la pubblicazione di documenti e per la comunicazione e la condivisione di informazioni all'interno di un'azienda, in collegamento anche con le sedi distaccate>>
  
- **NOME A DOMINIO ( DOMAIN NAME)** <<Il nome a dominio (*domain name*) è il nome assegnato ad un sito web. Il nome a dominio è composto da tre parti. La prima è l'acronimo **www** (che sta per *world wide web*), la terza (detta anche **Top Level Domain**) corrisponde ad una specifica sigla che è l'identificativo della nazione di emissione oppure individua la tipologia del sito (ad esempio .it indica un sito italiano, .com indica un sito commerciale). La seconda parte, invece, è quella che ha reale capacità distintiva, essendo impossibile che sia uguale per due siti diversi. Quindi, quando ci si riferisce genericamente al nome a dominio, in realtà ci si riferisce al **secondo livello del nome a dominio**. Sia gli Ip che i nomi a dominio vengono assegnati da organizzazioni con varia natura giuridica, detti **registri** (Naming Authority), sparsi in tutto il mondo, tramite la cosiddetta delega IANA, correntemente gestita dall'**ICANN** ([Internet Corporation for Assigned Names and Numbers](#)), società non profit USA, per conto del governo federale statunitense, che rimane a tutt'oggi titolare dell'effettivo ultimo controllo sul sistema dei nomi a dominio. In Italia tale compito è svolto dal **NIC**, un organismo privato con delega dell'ICANN costituito in seno al CNR.>>
  
- **SERVER**<< **Computer** che utilizza un [sistema operativo](#) di [rete](#) e destinato a svolgere uno o più servizi quali ad esempio la gestione di una [LAN](#), lo scambio e la condivisione di files ([file server](#)), la gestione della [posta elettronica](#) (mail server), l'ospitare sit [web](#) ([web server](#)), la gestione di periferiche come le stampanti ([print server](#)), il backup dei dati (server raid).  
Le mansioni dei diversi tipi di server possono essere gestite da un solo computer o possono essere suddivise tra più macchine dedicate a ognuno dei servizi descritti. I computer ad esso collegati vengono definiti come [client](#). Server è anche il [software](#) destinato ai server (server software) e viene suddiviso in:  
- [file](#) server quando tutti i client hanno [accesso](#) per lettura e scrittura ai files memorizzati sul

*STUDIO MARCO MONDADORI*  
*Consulenza del Lavoro e Tributaria*  
*Viale Vittorio Veneto, 110*  
*62029 TOLENTINO (MC)*

server;

- application server quando tutti i client utilizzano e condividono un applicativo memorizzato sul server.>>

- **CHIAVE USB o chiavetta USB o penna USB**<< (anche in [inglese](#) *USB flash drive*, o *pendrive*) è una [memoria di massa](#) portatile di dimensioni molto contenute (qualche centimetro in lunghezza e intorno al centimetro in larghezza) che si collega al [computer](#) mediante la comune [porta USB](#).>>
- **ORGANIGRAMMA RUOLI** <<Scopo dell'organigramma è quello di fornire una specie di mappa dell'organizzazione di riferimento.>>
- **DATO SENSIBILE**<< i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose e filosofiche, le opinioni politiche, l'adesione a partiti o sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale>
- **DATO GIUDIZIARIO**<< i dati personali idonei a rivelare provvedimenti di cui all'art 3, comma 1 lettera da a) a o) e da r) a u) del D.P.R. 14 novembre 2002,n.313 in materia di casellario giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reato e dai relativi carichi pendenti o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice penale>>
- **DATO PERSONALE COMUNE**<< qualunque informazione relativa a persona fisica, giuridica, ente, associazione, identificati o identificabili anche indirettamente mediante riferimento a qualsiasi altra informazione ivi compreso un numero di identificazione personale>>
- **TRATTAMENTO**<< qualunque operazione o complesso di operazioni effettuati anche senza l'ausilio degli strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione e la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati anche se non registrati in una banca dati>>
- **FATTURA ELETTRONICAPA**<< la fattura che è stata emessa e ricevuta in un qualunque formato elettronico; in particolare nei confronti della Pubblica Amministrazione, essa si considera trasmessa per via elettronica secondo le modalità riportate nel DM 55/2013 e si considera ricevuta dalla amministrazioni pubbliche solo a fronte del rilascio della ricevuta di consegna>>.

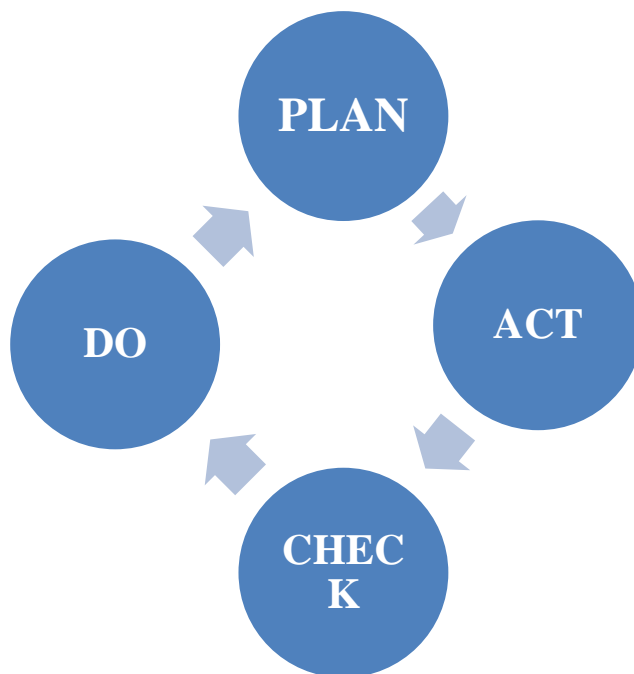
## ***D) Il sistema di gestione della sicurezza dei dati aziendali***

Un Sistema per la gestione della sicurezza delle informazioni include i requisiti per la sicurezza dei dati personali di cui fanno parte quelli stabiliti per legge.

Di seguito vengono elencati alcuni elementi considerati fondamentali per stabilire un quadro organico che garantisca la coerenza dell'approccio seguito con i principi sottostanti la tutela dei dati personali:

- coordinamento delle diverse aree aziendali in materia di gestione dei dati personali;
- definizione di regole interne per la gestione dei dati personali, da rispettare nelle procedure, formalizzate o meno, seguite nell'operatività;
- chiara e precisa definizione dei trattamenti di dati personali, specificandone le finalità, le modalità di trattamento e le categorie di interessati e predisponendo le relative informative e notifiche, se necessario;
- gestione delle attribuzioni di responsabilità interne ed esterne e delle comunicazioni rese da esse necessarie;
- controllo e dimostrabilità sia delle azioni sia dell'approccio complessivo mantenuto per la gestione dei dati personali.

**SCHEMA DEL SISTEMA DI GESTIONE DEI DATI AZIENDALI**



**a) PLAN**

Con il termine Plan dall'inglese "Pianificare", si vuol intendere che il primo fondamento di un buon sistema di gestione è rappresentato dalla sua organizzazione che comprende vari aspetti di seguito descritti.

In primo luogo devono essere definiti *i Ruoli e le Responsabilità*. Altro aspetto importante è la redazione e corretta tenuta di tutta la documentazione relativa alla politica di sicurezza dei dati in conformità con le disposizioni legislative. Ovviamente l'insieme della documentazione è rappresentato sia da documenti analogici che da file ed è, comunque, parimenti importante che siano attuate anche le misure tecniche di sicurezza reputate più idonee alle caratteristiche del

sistema, del work flow e della tipologia di banche dati trattate. Tutto il sistema deve essere garantito da aggiornamenti su base periodica o comunque in occasione sia di modifiche strutturali ed organizzative che in caso di presenza di rischi.

Infatti viene sempre effettuata *un'analisi dei rischi* a cui fa seguito un'adeguata procedura di trattamento degli stessi.

Affinché l'analisi del rischio sia poi utile al processo decisionale, deve essere seguita dai seguenti passi:

1. *Ponderare i rischi*: valutare se i rischi individuati sono accettabili;
2. *Identificare e ponderare le opzioni di trattamento dei rischi*: a fronte dei rischi valutati come inaccettabili, è necessario individuare le possibili azioni da intraprendere e valutarne la fattibilità (per esempio, in alcuni casi le azioni potrebbero introdurre più rischi di quelli attuali oppure avere costi eccessivi);
3. *Pianificare il trattamento dei rischi*: stabilire scadenze, budget e responsabilità per le azioni che si è deciso di intraprendere.

E' importante mantenere il collegamento tra azioni intraprese e minacce contrastate, anche al fine di fornire una giustificazione per le scelte compiute.

Le misure di sicurezza dovranno essere controllate nel tempo; in particolare, ne dovrà essere verificata la corretta realizzazione e, periodicamente, il loro buon funzionamento, anche attraverso attività di manutenzione ordinaria o straordinaria (per esempio, a seguito di incidenti).

## ***b) DO***

L'allocazione delle responsabilità per la sicurezza delle informazioni, così come le nomine richieste dalla normativa in materia di Privacy, devono essere mantenute aggiornate in modo che tutti gli inserimenti di nuovo personale, i cambiamenti di ruolo e le dimissioni siano immediatamente e correttamente riflessi nel quadro della gestione delle informazioni e dei dati personali dell'azienda.

In particolare, si deve curare la corretta attribuzione delle nomine di:

- Responsabili per il Trattamento dei dati Personali.
- Incaricati per il Trattamento dei Dati Personali
- Amministratori di sistema

Si osservi che le nomine possono riguardare sia personale con contratto da dipendente, sia altro personale con rapporto di lavoro regolamentato da altre forme contrattuali, inclusa quella di stage. Normalmente, in una azienda l'area delle risorse umane e quella dei sistemi informativi si occupano di gestire questo processo nel tempo, tenendo anche conto dei profili di accesso fisico e logico alle informazioni. Tali profili sono creati in base all'area aziendale di appartenenza, ai dati da essa trattati e alla funzione svolta dalla singola persona, sempre rispettando il principio di conferire il minimo livello di accesso necessario per permettere di svolgere le proprie mansioni. E' opportuno effettuare un riesame periodico, con cadenza almeno annuale, della correttezza delle nomine e dei corrispondenti profili di accesso

Ad ogni trattamento di dati personali deve essere associata **un' informativa** indirizzata agli interessati, che può essere realizzata in forme diverse (con maggiore o minore dettaglio) e che lega il trattamento ad una specifica finalità. Le informative sono i principali documenti da creare e mantenere aggiornati in relazione all'acquisizione dei dati personali. Le necessità di trasmissione di nuove informative agli interessati devono essere valutate di conseguenza all'evoluzione dei trattamenti.

Inoltre il personale deve essere sempre consapevole delle corrette modalità di trattamento delle informazioni e dei dati personali e dei rischi che incombono su di essi. Oltre a predisporre **una formazione** iniziale sul tema (ai neo-assunti), l'azienda deve periodicamente predisporre delle sessioni di aggiornamento, anche attraverso strumenti elettronici, che permettano di ricordare i concetti inizialmente espressi e di allinearli all'evoluzione del contesto aziendale.

Necessità puntuali di formazione specifica, in particolar modo per il personale con responsabilità in merito di sicurezza delle informazioni, devono inoltre essere rilevate e fatte confluire nei piani di formazione dell'azienda.

### **c) CHECK**

Con cadenza periodica il Responsabile del Trattamento Dati effettua delle verifiche sulla correttezza del trattamento delle informazioni e dei dati personali, sul livello di conformità delle attività effettuate rispetto alle regole e procedure stabilite dall'azienda.

Nell'ambito dell'esecuzione di tali verifiche è necessario includere quelle sull'operato degli amministratori di *sistema* (comprendenti l'eventuale *System, Net e Data Administrator*), in modo da

controllare la sua rispondenza alle misure organizzative e tecniche stabilite per i trattamenti dei dati personali, così come richiesto dalla normativa vigente

I risultati delle attività di verifica dovrebbero essere documentati e utilizzati come base per decidere quali azioni mettere in atto per rimediare eventuali criticità riscontrate.

#### **D) ACT**

Dovrebbero quindi essere fissati dei meccanismi, controllati del Responsabile del Trattamento Dati, per poter identificare, valutare, stabilire, attuare e controllare azioni di miglioramento del sistema. Aspetti significativi per il miglioramento continuo possono emergere dalle analisi degli incidenti, dai risultati delle verifiche interne ma anche dalle semplici attività di monitoraggio della sicurezza delle informazioni o da suggerimenti del personale. Le decisioni dovrebbero essere documentate e lo stato di avanzamento delle azioni monitorato.

#### ***E) La tutela della riservatezza nell'espletamento della propria mansione***

Ciascun soggetto è tenuto a garantire la segretezza dei fatti di cui viene a conoscenza nell'ambito della prestazione lavorativa e dell'eventuale contesto di lavoro in cui opera. Questa attenzione deve essere attuata su due livelli:

- a) il primo riguarda le modalità con cui sono utilizzati gli strumenti di lavoro con esplicito riferimento a quelli elettronici (come computer, fax, telefono, tablet ecc..). Questo significa che nel caso di abbandono temporaneo della postazione di lavoro, l'Utente è tenuto ad inserire lo screensaver in maniera da non permettere accessi da parte di persone non autorizzate; oppure nel caso di impiego del fax o della fotocopiatrice, è consigliabile non



lasciare i fogli ed i documenti per lungo tempo “abbandonati” nello strumento, ma cercare contestualmente all’invio o alla ricezione di collocarli nell’apposito fascicolo. Al tempo stesso è importante prestare attenzione e garantire la riservatezza quando si effettuano determinate attività: ad esempio i pagamenti on line, la consultazione dei conti correnti, l’accesso al gestionale o a programmi specifici, la consultazione della posta elettronica.

Infatti, se durante il compimento delle operazioni sopra descritte fosse presente un soggetto non autorizzato, l’Utente è tenuto ad adottare taluni accorgimenti aventi lo scopo di tutelare la segretezza delle informazioni:

- 1) orientare il monitor del computer in maniera da non rendere visibile alcun dato;
- 2) togliere o coprire con una cartella eventuali documenti presenti nella scrivania;
- 3) attendere l’uscita del soggetto prima di svolgere quel compito.

**b)** Il secondo livello di attenzione riguarda le azioni di comportamento individuale della persona. Con tale espressione si vuole far riferimento al tono di voce che, nel caso di trattamento di situazioni particolari, deve essere tenuto basso; in particolare durante le conversazioni telefoniche e durante i colloqui effettuati nei corridoi degli uffici o in prossimità di stanze altrui.

Al tempo stesso l’Utente, al fine di tutelare la segretezza di fatti e notizie inerenti un affare lavorativo, non può comunicarlo e diffonderlo tramite invio di sms o e-mail o post-note.

## ***F) La tutela del copyright aziendale***

L’oggetto principale di questo capitolo è la tutela del materiale di proprietà dello Studio sia esso rappresentato da pubblicazioni, da testi, da disegni, da immagini e da video. Tali materiali devono essere impiegati esclusivamente per le attività a cui sono destinati e non possono formare oggetto di finalità differenti. L’uso della carta intestata dello Studio risponde a scopi di comunicazione commerciale ed amministrativa per la gestione del business di questa realtà; pertanto nessuno è autorizzato ad impiegarla per motivi non congrui con gli obiettivi aziendali e per scopi personali.

Nel caso di brochures o di corporate identity dello Studio ogni soggetto è comunque tenuto, in caso di dubbio, ad accertarsi della possibilità e della relativa modalità di diffusione al fine di evitare che

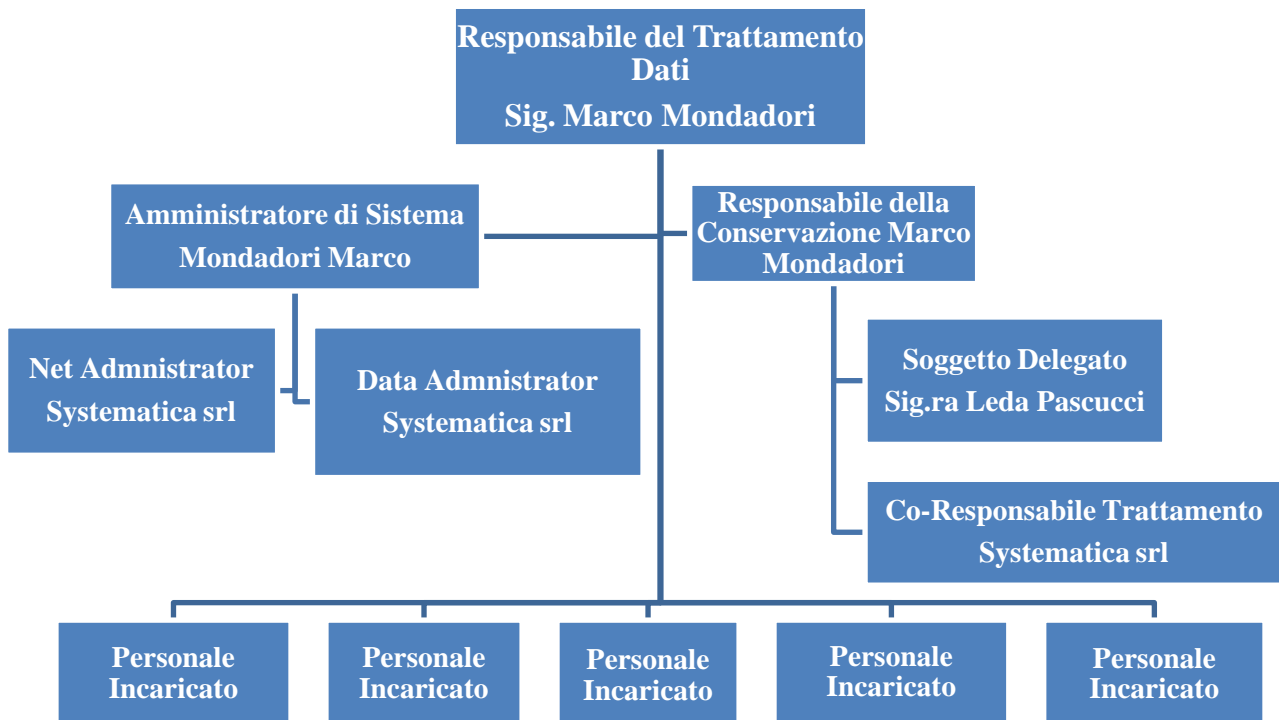
~ 18 ~

*STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)*

siano state già stabilite delle regole specifiche, come, ad esempio, nel caso di organizzazione di eventi informativi e formativi. Nel presente contesto un'attenzione deve essere rivolta anche al logo aziendale che non può essere inserito in file o documenti senza uno scopo di natura lavorativa; inoltre l'immagine rappresentativa del logo non può essere modificata in alcuna parte dagli Utenti in assenza di una precisa disposizione da parte del titolare medesimo.

Ogni testo, foto, video identificativa dello Studio non può essere impiegata in contesti o contenuti a sfondo discriminatorio per ragioni di sesso, di razza, di religione, di lingua, di professione, lesivi dei diritti e della dignità umana.

**G) L'organigramma ruoli privacy**



## **H) La gestione del dato sensibile**

Il dato qualificato come sensibile ai sensi dell'art. 4 del D.Lgs. 196/2003 e succ. integrazioni comprende le informazioni relative al sesso, alla razza, all'opinione, alla salute ovvero a tutte quelle situazioni particolarmente delicate di ogni soggetto. La gestione del dato sensibile richiede obbligatoriamente l'adozione di procedure atte a garantirne la massima riservatezza sia quando esso è elaborato, acquisito e trattato in modalità cartacea, sia quando tale attività avviene mediante gli strumenti elettronici. E' obbligatorio non comunicare ad alcuno le informazioni relative al personale ed ai collaboratori di cui si può venire a conoscenza durante lo svolgimento della prestazione lavorativa. In questo contesto tale divieto ha valore assoluto nel senso che ciascuno è responsabile della tutela della riservatezza nei confronti degli altri; l'eventuale condivisione di taluni dati tra un numero definito di soggetti all'interno della realtà dello studio, può avvenire solo come conseguenza di una determinata attività lavorativa. Inoltre i documenti contenenti dati sensibili devono essere archiviati tempestivamente nelle apposite cartelle al fine di evitare il rischio di un accesso non autorizzato all'informazione oppure il rischio di una loro perdita.

Ogni diverso settore dello studio gestisce taluni dati sensibili, pertanto ognuno deve provvedere a garantire la riservatezza di queste informazioni. Pertanto non è consentito intraprendere **in maniera autonoma** operazioni di scambio, di estrapolazione, di copia, di montaggio, di cancellazione, di comunicazione e di diffusione dei dati sensibili siano essi presenti in documenti o immagini cartacee che digitali. Ogni responsabile ed ogni incaricato trova nel proprio "documento privacy" denominato "*gestione della sicurezza dei dati aziendali (d.lgs. 196/2003 e s.m.i.) comunicazione aziendale per il rispetto della riservatezza dei dati trattati*" le tipologie di dati oggetto del loro ambito di competenza e trattamento.

Attualmente le tipologie di dati sensibili oggetto delle attività di trattamento sono rappresentati:

Tipologia di Dati (Art.4 D.lgs. 196/2003)	Categoria di appartenenza	Soggetti coinvolti	Modalità di trattamento
Personali Sensibili e Sanitari	Personale Dipendente	✓ Addetta Ufficio Amministrativo. ✓ Medico del Lavoro. ✓ Consulente del Lavoro ✓ Consulente Sicurezza sul Lavoro	<b>X Cartaceo</b> <b>X Informatico</b>
Personali Sensibili	Clienti	✓ Ufficio Amministrativo	<b>X Cartaceo</b> <b>X Informatico</b>

### ***1) La gestione dell'accesso ai documenti personali***

Il diritto di accesso ai documenti rientra tra le fattispecie collegate all'art 7 del codice della Privacy e leggi successive, in quanto esso riguarda l'esercizio del diritto di ciascun interessato a visionare e ad accedere alle proprie informazioni. Pertanto la richiesta di accesso deve avere ad oggetto esclusivamente dati personali dell'interessato. Non sono accettate richieste di informazioni proposte da colleghi o altri soggetti facenti parte della struttura siano essi collaboratori esterni o partners.

Ai fini dell'espletamento dei suoi diritti l'interessato può conferire delega o procura a persone fisiche o giuridiche. Si precisa che l'accesso ai dati consente di ottenere solo la comunicazione di informazioni personali detenute dal titolare (studio) oppure da estrarre da atti e documenti; non permette il diritto ad un illimitato accesso ad intere tipologie di atti o la creazione di documenti allo stato inesistenti negli archivi o la loro aggregazione in base a specifiche modalità prospettate dall'interessato.

*STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)*

Nel fornire riscontro il titolare comunica le informazioni richieste ed effettivamente detenute, ma non ha l'obbligo di ricercare altri dati che non siano nella propria disponibilità. La domanda può essere inviata da parte dell'interessato sia in forma cartacea che via e-mail. La scelta tra l'esibizione o la consegna in copia dei documenti può essere eseguita dal titolare nel solo caso in cui l'estrapolazione degli atti risulti essere particolarmente complessa; deve essere comunque omesso ogni dato riferito a terzi.

E' diritto di ogni lavoratore ottenere l'aggiornamento dei suoi dati che verrà eseguito solo alla presenza di un documento attestante la variazione intercorsa.

Ogni lavoratore riceve un'informativa dettagliata nella quale sono esplicate tutte le modalità di trattamento dei dati personali-comuni e sensibili unitamente ai soggetti autorizzati alla loro consultazione per le finalità lavorative.

In questa realtà le persone di riferimento per l'esercizio dei diritti di cui sopra sono:

- **Sig. Marco Mondadori** (*Legale Rappresentante e Responsabile Trattamento Dati*)

## **L) Il personal computer**

Il Personal Computer (ivi compreso il computer portatile ed il tablet) affidato al personale è uno strumento di lavoro; pertanto ogni utilizzo non conforme alla finalità lavorativa può contribuire a creare disservizi, costi di manutenzione e minacce alla sicurezza. L'accesso deve essere protetto da una credenziale di autenticazione e di autorizzazione.

Gli utenti possono utilizzare soltanto le applicazioni fornite ed installate dalla Studio Marco Mondadori. Le caratteristiche impostate nel proprio Pc non possono essere modificate senza l'autorizzazione scritta del Responsabile del Trattamento Dati e dell'Amministratore di Sistema; pertanto è vietata ogni libera iniziativa dell'utente.

Il Personal Computer non deve essere lasciato incustodito con particolare riferimento ai casi di assenze prolungate dall'ufficio, in questi casi l'elaboratore dovrà essere spento oppure dovranno essere attivati i blocchi di protezione.

In caso di collegamento al PC di supporti esterni, come web cam, penna usb, hard disk, l'Utente non è autorizzato a modificare le suddette impostazioni, né a cambiarne la posizione e la sua destinazione d'uso.

Infine si precisa che ogni computer dello Studio non può essere venduto, ceduto a titolo gratuito, né oneroso e non può formare oggetto di alcuna donazione a terzi. Al termine del suo utilizzo oppure al momento della cessazione del rapporto di lavoro, ciascun bene in possesso dovrà essere restituito allo Studio.

Nessun PC può essere trasportato in luoghi esterni diversi da quelli aziendali né portato nell'abitazione privata dell'Utente senza la presenza di un'autorizzazione del Titolare.

In qualsiasi momento ogni personal computer può essere oggetto di verifica e manutenzione delle sue componenti hardware e dei software presenti al fine sia di migliorarne le prestazioni funzionali che di accertarsi dell'assenza di applicativi o file non autorizzati e/o privi della relativa licenza; questa attività tecnica deve svolgersi nelle modalità e nei tempi che saranno comunicati di volta, in volta dal responsabile del trattamento dati.

## **M) Software aziendali**

Con questo termine si fa riferimento alle varie applicazioni che sono utilizzate presso questa struttura per consentire lo svolgimento delle attività lavorative in modalità elettronica. Tali applicazioni possono essere installate nell'unità server, nei singoli computer oppure possono essere fruibili direttamente on line attraverso la registrazione ad aree o siti ben definiti e con il rilascio di specifiche credenziali di accesso.

Non è consentito per autonoma iniziativa effettuare il download di software, di file musicali, di video in ogni postazione. Ogni eventuale installazione di applicativi necessari allo svolgimento delle prestazioni lavorative è consentito solo al personale tecnico appositamente incaricato sotto la direzione del Responsabile del Trattamento e dell'Amministratore di Sistema.

L'uso degli applicativi aziendali deve avvenire secondo le modalità definite dallo Studio ed in base alla formazione ricevuta nel rispetto dei principi di correttezza, pertinenza e non eccedenza.

### ***N) Le regole per l'uso delle fotocopiatrici***

L'uso delle fotocopiatrici è legato esclusivamente ad esigenze lavorative. Non possono essere fotocopiati documenti, libri e altro materiale per scopi personali; inoltre, per fini di riservatezza è buona prassi ricordarsi di non lasciare i documenti aziendali fotocopiati nella macchina fotocopiatrice, nel fax, nello scanner in maniera da ridurre il rischio di acquisizione indebita di dati e perdita degli stessi. Infatti al termine di ogni utilizzo, l'incaricato è tenuto a riporre i documenti nel luogo preposto; tuttavia, nel caso in cui, ci si accorga della presenza di fogli dimenticati in queste attrezzature, è buona norma, onde evitare il verificarsi dei rischi sopra citati, di consegnarli al Responsabile del Trattamento Dati il quale provvederà alla loro corretta archiviazione.

Si precisa che in questo contesto con il termine fotocopiatrice si comprende e pertanto si estende la policy anche al fax ed allo scanner.



### ***O) Le attività ludiche***

E' vietata l'installazione di qualsiasi applicazione avente scopo ludico e di gioco. E' fatto altresì divieto di effettuare giochi on line mediante registrazione a siti specifici dal computer di lavoro e con la connessione appartenente a codesto Studio.

E' tassativamente vietata qualsiasi attività di gioco di azzardo

Inoltre l'Utente non è autorizzato ad effettuare acquisti on line di natura privata mediante l'utilizzo dei sistemi hardware e software aziendali.

### ***P) La gestione dell'errore e del guasto tecnico***

Nell'ambito delle regole atte a definire una politica di sicurezza del patrimonio informativo, lo Studio Marco Mondadori ritiene importante delineare nei confronti degli Utenti le azioni corrette da effettuare nel caso in cui si manifestano degli errori rilevanti o che potrebbero originare situazioni spiacevoli e problematiche durante l'uso degli strumenti elettronici. Di seguito si riportano taluni esempi di fattispecie quale parametro di riferimento per la gestione dell'errore:

- errata battitura di un tasto di salvataggio all'interno di una procedura, di un applicativo specifico (software gestionale, software di produzione tec.);
- oppure nel caso in cui sia stata inviata una e-mail per errore o con un allegato non corretto.
- forzatura nel compimento di un'operazione in presenza di problemi già rilevati (ad esempio virus)
- errata cancellazione di file o dati;

Nella gestione di un errore è comunque sempre importante che il lavoratore, prestando la dovuta diligenza e correttezza, nel momento in cui se ne accorga, provveda subito alla sua correzione; nei casi in cui la risoluzione sia per problemi tecnici che per eventuali situazioni correlate non possa essere autonoma e di facile sistemazione, l'Utente sarà tenuto a darne immediata comunicazione al soggetto preposto alla direzione di quel determinato settore.

In questa maniera ed in conformità con il principio della buona fede, si potrà evitare un danno maggiore e si potrà procedere al ripristino di un dato in tempi veloci senza arrecare problemi anche ad altri colleghi o ad altre procedure informatiche collegate.

L'altro aspetto da valutare riguarda il verificarsi di un guasto tecnico agli strumenti elettronici utilizzati per lo svolgimento della prestazione. Le attività di assistenza tecnica sono demandate ai soggetti appositamente incaricati e l'Utente non è legittimato ad intraprendere autonome iniziative.

Infine, per motivi di sicurezza fisica e personale è vietato toccare i quadri elettrici di accensione e spegnimento, è vietato manomettere i cavi di rete, i cavi di collegamento elettrico e le corrispondenti prese.

## ***Q) La gestione dell'anomalia***

In questa sessione lo Studio Marco Mondadori intende fornire delle policy al lavoratore ogniqualvolta si possano manifestare delle anomalie di tipo hardware e software.

Con il termine *anomalia* si comprende tutti quegli eventi non "ordinari" di durata sia temporanea, istantanea che permanente e che possono verificarsi in momenti diversi e durante l'impiego di differenti strumenti elettronici. Un primo esempio di anomalia è rappresentato dalla presenza di un virus nel nostro computer quando questo stesso non viene eliminato, ma compare la maschera recante la scritta "virus in quarantena".

Un altro caso si può incontrare nel nostro account di posta elettronica aziendale quando riceviamo e-mail di spam in numero elevato oppure messaggi pericolosi che potrebbero nascondere tentativi di phishing o altra tipologia di truffa informatica.

Inoltre rientra nel concetto di questo paragrafo, ogni eventuale anomalia che si verifica durante le attività lavorative nei software specifici in uso oppure nel funzionamento dello stesso computer. Si cita, a titolo di esempio, il caso in cui il pc all'improvviso si spenga, oppure il caso in cui al momento dell'accensione o del riavvio del pc, compaia una maschera nel desktop di colore blu ed eventuali altri messaggi o funzionamenti non regolari.

Un altro aspetto da considerare attiene alla navigazione in internet, laddove l'utente venisse "deviato" in un sito diverso da quello di partenza o meglio da quello ricercato.

In tutti questi casi è necessario darne comunicazione all'Amministratore di Sistema, cercando di fornire una descrizione precisa dell'anomalia presente. La modalità di comunicazione può avvenire sia in forma orale che mediante contatto telefonico oppure mediante l'invio di un e-mail aziendale purchè il tutto venga effettuato tempestivamente alla sua scoperta.

### ***R) La comunicazione delle informazioni aziendali nel web***

Con il termine “*informazioni aziendali*” si fa riferimento a tutte quelle notizie ed a tutti quei documenti ed immagini sia digitali che analogiche contenenti dati appartenenti a codesto studio; mentre con il termine “*comunicazione nel web*” si vuol intendere l'azione di rendere pubbliche nel web le informazioni di cui sopra.

Non è consentito inserire qualsiasi dato aziendale a partire da un numero di telefono, da un indirizzo e-mail fino a quelle di natura più riservata come il codice iban, in moduli contenuti nei siti web anche di natura istituzionale senza che sia pervenuta dal datore di lavoro o da un soggetto da lui incaricato una specifica autorizzazione e fatto salvo che non si tratti delle ordinarie operazioni amministrative verso clienti e fornitori.

Il divieto di diffusione di dati in internet si estende anche alla loro eventuale pubblicazione nei social network.

L'unica eccezione è costituita dalla pubblicazione di informazioni nel sito internet aziendale [www.studiomondadori.com](http://www.studiomondadori.com) che ovviamente avviene nel rispetto di precisi compiti lavorativi; pertanto non sono consentite iniziative autonome e non è ammessa alcuna integrazione alla logica di impostazione stabilita, non possono essere aggiunti link ad altri siti senza che tale operazione sia stata concordata ed autorizzata dal titolare. Inoltre è necessario che ogni eventuale richiesta di partnership, mediante scambio di banner nel sito e di logo aziendale, venga accettata da entrambe le parti con invio, anche tramite posta elettronica, del materiale, delle modalità e dei tempi di uso.

## **S) Le regole per l'uso dei dispositivi di firma**

I dispositivi di firma attualmente in uso presso la *Studio Marco Mondadori* sono quelli relativi **all'home banking** con cui viene autorizzato il compimento di un'operazione bancaria e la sua effettiva realizzazione e validità unitamente all'impiego per taluni scopi della **firma digitale**, in particolare quest'ultima viene utilizzata per la firma di documenti lavorativi. I soggetti legittimati all'uso dei dispositivi di firma sono tenuti a rispettare le indicazioni di corretta tenuta in segretezza del luogo di conservazione dello stesso e delle relative credenziali.

Nel caso di malfunzionamento del dispositivo, l'incaricato è tenuto, tempestivamente, ad informare il titolare prima di procedere con la chiamata al servizio di assistenza del corrispondente istituto di credito.

La sua conservazione deve rispettare i principi di accesso legittimato solo agli incaricati previo accertamento delle condizioni del luogo medesimo ossia un ambiente idoneo a garantire il funzionamento di un microchip, quindi ad esempio, lontano da fonti eccessive di calore, da fonti alterabili o da piani sdruciolevoli che possano graffiare e quindi danneggiare il funzionamento della carta stessa.

Alla luce di quanto appena affermato lo studio stabilisce quanto segue:

- a) obbligo per l'utente di rispettare la segretezza circa il luogo di tenuta del dispositivo e dei relativi codici di accesso;
- b) l'utente non può per sua iniziativa modificare né il luogo di tenuta della firma né il codice senza consenso del titolare;
- c) l'impiego della firma deve essere limitato alle finalità stabilite **dallo Studio**;
- d) il dispositivo non può essere utilizzato in presenza di altre soggetti non autorizzati;
- e) l'utente è tenuto ad osservare le modalità di impiego del dispositivo di firma impartite dall'azienda senza apporre alcuna variazione;
- f) l'utente è tenuto ad informare il titolare in caso di guasto o malfunzionamento del dispositivo e conseguente impossibilità ad effettuare un'operazione;

*STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)*

g) nel caso di firma digitale l'incaricato è tenuto a verificare la scadenza del certificato di firma prima di apporre ad un documento tale sottoscrizione elettronica

Per l'uso del dispositivo di firma digitale i soggetti autorizzati sono : Marco Mondadori, Leda Pascucci

### ***T) Le regole per l'uso dei supporti usb***

L'uso dei supporti personali usb non è consentito agli Utenti. E' ammesso l'uso di eventuali supporti usb solo se appartenenti all'azienda e nei limiti autorizzati e per le finalità comunicate agli eventuali soggetti interessati. Pertanto salvo diversa comunicazione di modifica all'attuale policy, ogni Utente è tenuto a rispettare quanto sopra esposto.

### ***U) La gestione dei profili di accesso***

Il Sistema Informativo Aziendale è caratterizzato dalla presenza di regole precise basate sull'impostazione dei profili di accesso alle varie banche dati\* in relazione a ciascun utente ed ai compiti allo stesso attribuiti. Questo significa che ogni incaricato può avere anche profili differenti di accesso e di uso a seconda del tipo-lavoro da svolgere; pertanto può accadere che nell'uso di un software sia prevista un'autorizzazione generale, mentre in un altro sia attivato solo un profilo di consultazione.

*Banche Dati<< l'insieme dei dati elaborati, acquisiti, organizzati, estrapolati, conservati, consultati, confrontati dall'azienda per il trattamento delle attività lavorative. Le Banche Dati sono raggruppate in base alle loro finalità oppure in base alla suddivisione interna degli uffici ( Amministrazione, Direzione Generale e Servizi Generali) Esse comprendono la gestione del dato sia nella modalità elettronica che in quella cartacea purchè di appartenenza all'azienda anche se non sempre di sua esclusiva proprietà. Inoltre le operazioni effettuate sulle Banche Dati possono avvenire dal personale interno alla struttura e da soggetti esterni specificatamente incaricati, ognuno in base al proprio ambito di competenza.>>*

*STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)*

L'esistenza di una gestione dei profili risponde alle logiche di organizzazione del lavoro e dei compiti ed, al tempo stesso, è un criterio di rispetto delle responsabilità individuali.

Ogni profilo di accesso è caratterizzato da due elementi:

- 1) *USER* << nome utente, ovvero l'identificativo della persona nei confronti del sistema
- 2) *PASSWORD* << codice alfa numerico e riservato, unico per ogni user >>

L'impostazione iniziale dei profili viene eseguita dall'Amministratore di Sistema secondo la procedura di seguito descritta:

- ✓ *ACCOUNT I° LIVELLO* = si tratta del profilo che viene subito creato dall'Amministratore di Sistema ovvero nel momento stesso in cui egli ne riceve la comunicazione. Tale profilo ha una durata temporale, valida solamente in corrispondenza dell'orario lavorativo; esso riguarda l'accesso al Sistema Informativo.
  
- ✓ *ACCOUNT II° LIVELLO* = L'amministratore di Sistema assegna ad ogni Utente un profilo per l'accesso agli applicativi in uso in base ai compiti da svolgere.

La responsabilità della corretta tenuta e, quindi, della riservatezza della password appartiene ad ogni Utente dal momento che il Sistema in automatico, dopo la prima assegnazione, procede con la richiesta di cambio.

Non è consentita la trascrizione del proprio profilo in post-note esposti nella scrivania o comunque lasciati alla visione di terzi non legittimati così come la comunicazione del profilo a terzi mediante invio di e-mail o sms; è altresì vietata la comunicazione verbale ad alcun altro Utente di tali identificativi.

Si precisa che, ai fini delle responsabilità, nel caso di non osservanza del dovere di segretezza, l'utente sarà chiamato a rispondere del fatto.

In caso di temporanea sostituzione di un Utente, le credenziali del profilo non dovranno essere rese note; infatti le attività verranno svolte dal soggetto delegato per il tempo stabilito di cui il Sistema ne conserverà traccia.

In caso di cessazione del rapporto di lavoro oppure in caso di cambio della mansione, l'Amministratore di Sistema procederà con la chiusura di quel determinato account che, pertanto, cesserà immediatamente di essere operativo.

Inoltre nel caso in cui un Utente fosse venuto a conoscenza dell'account di un collega, egli sarà ritenuto parimenti responsabile se venisse fornita prova certa del compimento di attività.

### ***V) Le regole per l'uso del telefono aziendale***

L'uso del telefono aziendale è legato a scopi di natura lavorativa.

I soggetti autorizzati all'uso del cellulare aziendale sono tenuti al rispetto delle regole di seguito indicate.

Si ricorda, infatti, che i numeri mobili appartengono ad un contratto stipulato dallo studio con un gestore di telefonia, la conoscenza dei contatti lavorativi contenuti nella rubrica deve essere resa nota solamente ai collaboratori, al personale e ai soggetti collegati con le esigenze lavorative derivanti dalla mansione svolta; inoltre è vietato effettuare la copia del contenuto della sim dello studio.

Non è possibile apportare delle modifiche alle impostazioni attivate sul telefono cellulare ed al suo relativo profilo. In caso di cessazione del rapporto di collaborazione, il telefono dovrà essere restituito alla proprietà. Per tutta la durata di impiego di tale strumento, ciascun lavoratore è tenuto ad usare la diligenza del prestatore di lavoro dall'art 2104 del codice civile.

Inoltre non è consentito effettuare tramite il cellulare aziendale foto e filmati ai colleghi o allo studio senza un'esplicita e motivata autorizzazione; pertanto queste immagini non devono essere inviate a terzi né tantomeno pubblicate in rete. In caso contrario lo Studio intende sanzionatorio tale atteggiamento contrario alle regole stabilite e, soprattutto, lesivo della persona e del rispetto della sua riservatezza.

## ***Z) Le regole per l'uso di internet***

Internet può essere definito quale struttura portante di tutto il Sistema Informativo Aziendale. Tuttavia la rete è, al tempo stesso, un forte pericolo se non vengono attivate le giuste misure di tutela e un costante controllo. Nell'ambito di internet è compreso sia l'accesso alla rete pubblica che a quella interna (LAN , WI-FI,VPN) e questa disciplina investe entrambi gli aspetti. La connessione ad internet costituisce oggi uno strumento di lavoro appartenente allo studio e, quindi, sotto la "sua libertà di regolamento". L'utilizzo di internet è disponibile a tutti gli utenti esclusivamente per lo svolgimento delle prestazioni lavorative. Durante la navigazione, ad eccezione di particolari ed autorizzate esigenze lavorative, nessun soggetto può registrarsi e, quindi, lasciare informazioni aziendali all'interno dei siti; parimenti non è consentito creare profili riferiti alla società nei social network. Non sono consentite *chat* e non è consentita l'autonoma installazione di web-cam. Durante la navigazione ciascun utente non può partecipare a giochi on-line di alcun genere, né scaricare suonerie o immagini per i telefoni cellulari anche quando questi ultimi appartengono all'azienda. La *Studio Marco Mondadori* ritiene importante fornire un'ulteriore precisazione (con valore di avviso immediatamente esecutivo) in materia di navigazione in internet che può verificarsi nel caso in cui qualcuno provi a superare i blocchi di sicurezza già impostati: è tassativamente vietato collegarsi con la rete aziendale a siti dal contenuto pornografico ed a siti discriminatori e contrari alla tutela dei diritti umani. La possibilità di collegarsi ai social network durante lo svolgimento dell'attività lavorativa non è consentita. Nell'ambito della definizione delle policy di internet, va evidenziata la non autorizzazione per ogni utente di partecipare durante l'orario di lavoro e mediante gli strumenti elettronici dell'azienda a forum e blog non aventi alcuna funzionalità con i compiti attribuiti. E' vietata la pubblicazione di commenti, notizie, foto, documenti aziendali nelle pagine dei social network; infatti, Facebook e altri, per il loro stesso meccanismo, sono un ambiente pubblico o quantomeno semi-pubblico. Quindi, per i commenti e le opinioni espresse dal lavoratore sul proprio datore di lavoro, si pone lo stesso problema di bilanciamento tra diritto di critica e dovere di fedeltà e riservatezza più volte affrontato dalla giurisprudenza con riferimento a dichiarazioni diffuse tramite giornali, televisioni e altri mezzi di manifestazione del pensiero. La Cassazione, al riguardo, ha più volte affermato che il diritto di critica del lavoratore è sottoposto a peculiari limiti in considerazione degli obblighi di collaborazione e fedeltà che gravano sul dipendente. E così



potranno essere disciplinarmente sanzionabili anche i commenti denigratori che possano recare danno all'impresa, tanto più se arbitrari e gratuiti, così come la diffusione di notizie e informazioni riservate. Naturalmente, spetterà al giudice valutare in concreto la gravità del fatto e, quindi, la proporzionalità della sanzione eventualmente irrogata dal datore di lavoro al dipendente, tenendo conto del contenuto delle dichiarazioni, dell'ambito di pubblicità e della finalità delle medesime, dell'intenzionalità della condotta. Per quanto attiene all'uso corretto della Intranet Aziendale, ogni Utente è tenuto al suo impiego esclusivamente per finalità di comunicazioni lavorative e di scambio di documenti. Pertanto sono vietate le attività di elaborazione, confronto, scambio di informazioni e dati di natura privata; l'intranet aziendale rappresenta anch'essa uno strumento di lavoro sotto la responsabilità ed il controllo **dello studio**.

### ***W) Le regole per l'uso della posta elettronica***

L'uso della e-mail rientra dunque nella disciplina dei beni di proprietà della **Studio Marco Mondadori** e, quindi, fa capo alle regole di corretto utilizzo definite da questa struttura. Sono state definite delle regole precise per la gestione sia delle e-mail aziendali che di quelle a valore legale in conseguenza del maggior loro uso e delle responsabilità connesse.

La posta elettronica aziendale di tipo "ordinario" ovvero quella contraddistinta dal [nome@marcomondadori.it](mailto:nome@marcomondadori.it), viene impiegata per lo svolgimento delle attività lavorative da parte dei soggetti autorizzati. Essa può formare oggetto di controllo da parte del datore di lavoro. Non è consentito inviare dall'indirizzo dello studio ad un indirizzo personale dati, documenti, foto, immagini, video appartenenti allo studio fatto salvo che ciò non sia stato disposto dal titolare. I messaggi di posta elettronica possono essere inviati solamente ai soggetti che hanno rapporti di lavoro con codesta realtà e nel rispetto degli ambiti stabiliti dall'azienda.

Gli account aziendali non possono essere conferiti come indirizzi di riferimento all'interno di siti o portali il cui accesso risponde a finalità personali dell'utente così come è fatto divieto di lasciare i riferimenti di posta elettronica aziendale in siti di e-commerce per completare un determinato acquisto privato.

Ogni Utente è responsabile del corretto uso della propria casella di posta elettronica aziendale.

*STUDIO MARCO MONDADORI*  
*Consulenza del Lavoro e Tributaria*  
*Viale Vittorio Veneto, 110*  
*62029 TOLENTINO (MC)*

Le policy aziendali in materia di posta elettronica sono caratterizzate dalla creazione di account individuali contraddistinti dal *nome* dell'Utente e dal nome a dominio della Studio Mondadori Marco, quindi la configurazione tipo è: *nome@marcomondadori.it*

L'accesso alla consultazione ed all'invio di e-mail è protetto da user-id e password che devono restare riservate e nella sola disponibilità del singolo Utente.

La posta elettronica è equiparata alla posta epistolare e, pertanto, i messaggi via e-mail sono soggetti alle **medesime regole di riservatezza e inviolabilità che tutelano**

**la posta.**

L'Utente non è autorizzato alla consultazione delle e-mail di altri colleghi seppur appartenenti alla medesima struttura o al medesimo settore; altresì non è tenuto ad inviare i messaggi ricevuti o inoltrati per scopi lavorativi ad altri Utenti del Sistema non legittimati alla trattazione di quella determinata fattispecie.

In caso di assenza temporanea dal posto di lavoro, l'utente non può per autonoma iniziativa, rilasciare ad un collega le proprie credenziali per consentire l'uso della sua casella di posta elettronica; infatti, in questo caso, deve essere osservata la procedura aziendale caratterizzata dalla compilazione dell'apposito modulo unitamente all'autorizzazione formale da parte del Responsabile Trattamento dati .

Inoltre, in caso di cessazione del rapporto di lavoro, l'Amministratore di Sistema provvederà tempestivamente alla chiusura e alla disabilitazione di quel determinato account di posta elettronica. L'archivio delle e-mail aziendali e la loro copia è patrimonio dell'Azienda e non rientra nella personale disponibilità dell'Utente.

Per quanto attiene all'uso **della posta elettronica a valore legale** ( in sigla PEC-  
m.mondadori@consulentidellavoropec.it) gli Utenti autorizzati sono tenuti a rispettare scrupolosamente le regole fornite dallo Studio sia nel caso dei tempi di consultazione che nel caso delle attività di inoltro; si ricorda, a tal proposito, che tale indirizzo rappresenta oggi il domicilio informatico dello Studio riportato anche nella visura camerale.

Nella gestione dell'account pec, gli Utenti autorizzati sono tenuti alla conservazione delle ricevute di "accettazione " e "consegna" provenienti dal server dell'ente certificatore; la loro cancellazione non può aver luogo per autonoma iniziativa data la natura di prova giuridica che le caratterizza.

*STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)*

Non possono essere comunicati a terzi, senza un fondato ed esplicito motivo, gli indirizzi di posta elettronica a valore legale; ogni richiesta diversa da quanto disposto dallo Studio, deve pervenire in forma scritta con l'indicazione della relativa motivazione e deve essere prontamente inoltrata al titolare per la valutazione.

Per quanto attiene all'operazione di invio delle comunicazioni mediante pec, esse devono avvenire nei casi in cui sia obbligatorio (ad esempio perché richiesto per quella particolare fattispecie) oppure quando è necessario attribuire una valenza rafforzata e probatoria alla situazione oggetto di comunicazione. Pertanto non deve essere utilizzato l'account pec per le ordinarie comunicazioni lavorative che possono essere gestite e conservate mediante la posta elettronica aziendale.

All'interno della Studio Marco Mondadori gli utenti autorizzati all'uso della PEC\_ m.mondadori@consulentidellavoropec.it risulta nel relativo atto di incarico.

## **L'ANTIRICICLAGGIO**

Con il termine Antiriciclaggio nell'ambito del presente contesto, si intende far riferimento sia al corretto adempimenti degli sanciti dal D.lsg. 231/07- D.Lgs. 151/2009 e succ modifiche, sia alla riservatezza ed alla sicurezza attuata all'interno dello studio nella tenuta e conservazione della documentazione correlata a questo tema. L'elaborazione dei dati acquisiti dai clienti è svolta direttamente dalla titolare compresa l'attività di Adeguata Verifica e Profilo di Rischio. Nessuna informazione viene resa nota a terzi, ivi compresi gli eventuali collaboratori. E' attuata un'attività di controllo periodico volta a verificare l'esatta tenuta del "Fascicolo del Cliente" il quale è archiviato in base a criteri di personale identificazione. Nell'anno 2014 la tenuta dell'Archivio Antiriciclaggio avviene in modalità elettronica, mentre la gestione e la tenuta e degli originali della documentazione per l'adeguata verifica ed il Profilo di Rischio sono conservati in modalità cartacea e tenuti presso la sede della studio.

## ***Y) Le attività informative e formative***

La formazione rappresenta un importante elemento di crescita professionale che viene attuata in vari modi: dalla partecipazione ad eventi a tema, a seminari fino alle attività formative organizzate ed effettuate all'interno della struttura.

Rientra nel concetto di informazione, ogni tipo di comunicazione effettuata dallo Studio verso i lavoratori sia nella modalità di e-mail informativa che di circolari o di avvisi al personale.

La formazione segue, invece, un programma dedicato che può riguardare tutti i lavoratori oppure solo alcuni gruppi a seconda delle necessità riscontrate e delle tematiche affrontate. Sicuramente esistono delle argomentazioni che obbligatoriamente devono essere portate a conoscenza di tutti per le quali vengono pianificati degli incontri in sede alla presenza del personale al completo.

La modalità di svolgimento degli eventi di formazione può essere sia on line che on site e viene stabilita sulla base dei fattori economici e di organizzazione esistenti in quel determinato periodo di riferimento ovviamente in concomitanza la sussistenza del corso. Al termine di ogni attività formativa lo Studio ne attesta la sua realizzazione nella propria documentazione e provvede alla consegna di un attestato di partecipazione a ciascun interessato provvedendo, in tal modo, a conferire il materiale necessario per l'aggiornamento del Libretto Formativo del Lavoratore.

Alla luce di quanto sopra esposto, gli Utenti possono essere chiamati a partecipare ad eventi formativi in materia di sicurezza dei dati e sicurezza informatica.

## ***X.1) Conservazione Digitale***

***Per Conservazione Digitale*** s'intende il processo di dematerializzazione dei documenti fiscali rappresentati dal Libro Giornale, Registro Iva, LUL, Fatture Acquisto e Fatture Vendita dei propri clienti in conformità alle Nuove Regole Tecniche pubblicate in G.U. del 12/03/2014.

Il ruolo del responsabile della conservazione è rappresentato dal titolare dello studio Rag. Marco Mondadori che ha nominato quale soggetto delegato la Sig.ra Leda

Pascucci. Ai sensi di quanto sancito dal Codice dell'Amministrazione Digitale e dalle Nuove Regole Tecniche sulla conservazione digitale (DPCM 03/12/2013-G.U. 12/03/2014), i compiti attribuiti al delegato sono:

- apposizione della firma digitale e della marca temporale nei documenti fiscali entro la fine dell'anno n. nel rispetto delle disposizioni legislative;
- acquisizione dei documenti e loro eventuale trasformazione dallo status di documento analogico a quello di documento digitale;
- accesso tramite proprie credenziali al software "Archivia" con il quale viene gestito l'intero sistema di conservazione;
- gestione delle problematiche tecniche con la ditta incaricata dell'assistenza software e verifica della corretta attività di trattamento dei dati;
- partecipazione alle attività formative in materia di gestione dei documenti digitali organizzate dal titolare.

Il sistema di conservazione digitale prevede anche il coinvolgimento della Systematica srl quale società incaricata dell'assistenza ed aggiornamento del software Archivia, la quale viene a conoscenza di tutti i file presenti nel nostro server. Pertanto ai fini dello scopo del disciplinare si rimanda alle regole di sicurezza e riservatezza che sono state predisposte nell'atto di incarico.

## ***X.2) La co-responsabilità nel trattamento dati***

L'art. 29 del D.Lgs. 196/2003 e s.m.i. stabilisce la possibilità di esistenza nella stessa Azienda titolare di più soggetti Responsabili del Trattamento anche mediante la suddivisione dei compiti. Alla luce di quanto appena descritto, lo Studio Marco Mondadori pianifica l'esistenza di un co-responsabile del trattamento dati nel momento in cui viene concluso il processo di corretta conservazione dei documenti a rilevanza tributaria. Infatti lo studio ha adottato un sistema di

*STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)*

conservazione digitale dei documenti dei propri clienti ed ha nominato un Responsabile della Conservazione, un soggetto delegato ed un co-responsabile della sicurezza e riservatezza rappresentato dalla Systematica srl. A questo proposito si precisa che lo studio sarà tenuto a descrivere nel Manuale della Conservazione e nel Piano della Sicurezza Informatica lo sviluppo in dettaglio dell'intero sistema di gestione delle banche dati digitale sopra citate, monitorando, al tempo stesso, il grado di sicurezza del proprio sistema informativo prevedendo anche le eventuali azioni correttive.

## ***XX) La disciplina dei controlli***

L'ambito dei controlli rispetta le previsioni legislative dettate sia dalle norme sulla protezione dei dati che quelle contenute nella normativa del lavoro. Le attività di controllo devono avvenire nei limiti dei cd. **controlli difensivi**, diretti cioè ad accertare condotte illecite del lavoratore. Infatti il controllo difensivo si sostanzia in un controllo *ex post* diretto a fronteggiare un atto illecito del dipendente. Naturalmente i controlli, ex art. 11 Codice Privacy, devono essere proporzionati, pertinenti, leciti, corretti ed eseguiti in modo trasparente. Nel caso in cui si manifestano talune anomalie, la fase di controllo non è mai diretta in prima istanza. Le verifiche hanno un carattere generale e anonimo; esse possono assumere valenze più significative nel momento in cui le anomalie persistono e aumentano, specie se della medesima tipologia. Infatti l'attività correttiva prevede in primo luogo una forma generale di comunicazione volta a mettere in luce la "scoperta" di un determinato evento "inconsueto". La policy scelta prevede l'invio di ripetute comunicazioni al fine di invitare a desistere dal compimento di talune operazioni. Laddove la violazione persiste e tende ad assumere implicazioni pericolose per lo studio o per terzi, l'attività di verifica verrà eseguita in base a criteri più definiti e selettivi. Ovviamente nel caso di grave e continua reiterazione l'azienda provvederà all'attuazione del regime sanzionatorio previsto dai CCNL o dalle norme del diritto civile nel caso di contratti di collaborazione.

L'Amministratore di Sistema, nell'ambito delle responsabilità e dei compiti propri di questo ruolo, è tenuto ad effettuare periodicamente delle attività di controllo volte a tutelare l'integrità del Sistema Informativo Aziendale, la sicurezza dei dati e l'eventuale miglioramento delle procedure tecniche in uso.

### ***XXX.1) Il piano di monitoraggio della sicurezza dati.***

La Studio Marco Mondadori ha previsto un Piano di monitoraggio dei rischi affinché le regole stabilite e descritte nel presente Disciplinare mantengano nel tempo la loro efficacia. In primo luogo va precisato che è dovere previsto dalle norme che sia il Responsabile del Trattamento Dati che l'Amministratore di Sistema devono attuare delle azioni di controllo ed agire tempestivamente in caso di verifica di anomalie che possono rappresentare un rischio per l'integrità, la riservatezza e la sicurezza dei dati aziendali. Inoltre bisogna tener presente che, dal punto di vista giuridico, l'attività di trattamento dei dati è considerata un'attività pericolosa ai sensi dell'art. 2050 del Codice Civile << Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno >> dove l'onere probatorio spetta a colui che ha subito il danno e non al soggetto attore. Alla luce di questo principio il Responsabile del Trattamento e l'Amministratore di Sistema devono dimostrare le misure attivate al fine di salvaguardare la loro tutela e responsabilità per fatti ed eventi non dipendenti dalla loro volontà.

Il Piano di monitoraggio della sicurezza si basa su due principali elementi:

- 1) rilevazione documentata del sistema informativo;
- 2) analisi del contesto normativo.

Il primo punto riguarda i flussi informativi, quindi non solo quelli di natura informatica, per individuare l'andamento delle regole stabile nei differenti processi di lavoro valutando anche la funzionalità degli strumenti elettronici utilizzati ( in questo contesto il termine "*strumento elettronico*" comprende sia le risorse hardware che quelle software).

Nel secondo punto si cerca di individuare la conformità con le evoluzioni normative in materia di sicurezza informatica, di riservatezza, di gestione digitale delle informazioni al fine di garantire l'adeguamento dello Studio a questo contesto.

*STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)*

Per ogni eventuale vulnerabilità, si procederà a valutare le azioni correttive tenendo presente sia i costi diretti che i costi indiretti dal momento che ogni contro/misura va valutata nel rapporto costo/efficienza (una contromisura non può essere più costosa di quanto lo Studio perderebbe in caso di attacco).

▪ **SCHEMA CHECK LIST CONTROLLO**

<b>Ambito di controllo</b>	<b>Data</b>	<b>Soggetto attuatore del controllo</b>	<b>Report</b>	<b>Attività di intervento</b>
Ruoli della sicurezza			<input type="checkbox"/> Piano delle misure adottate da <b><u>non</u></b> modificare. <input type="checkbox"/> Piano delle misure adottate <b><u>da</u></b> modificare.	
La gestione delle credenziali di autorizzazione ed autenticazione			<input type="checkbox"/> Piano delle misure adottate da <b><u>non</u></b> modificare. <input type="checkbox"/> Piano delle misure adottate <b><u>da</u></b> modificare	
La gestione dei dati sensibili			<input type="checkbox"/> Piano delle misure adottate da <b><u>non</u></b> modificare. <input type="checkbox"/> Piano delle misure adottate <b><u>da</u></b> modificare	
La sicurezza dei			<input type="checkbox"/> Piano delle misure	



*STUDIO MARCO MONDADORI*  
*Consulenza del Lavoro e Tributaria*  
*Viale Vittorio Veneto, 110*  
*62029 TOLENTINO (MC)*

dati nei rapporti con i clienti e con i collaboratori			adottate da <b><u>non</u></b> modificare. <input type="checkbox"/> Piano delle misure adottate <b><u>da</u></b> modificare.	
La sicurezza dei dati nei rapporti con i fornitori			<input type="checkbox"/> Piano delle misure adottate da <b><u>non</u></b> modificare. <input type="checkbox"/> Piano delle misure adottate <b><u>da</u></b> modificare.	
Controlli di accesso fisico			<input type="checkbox"/> Piano delle misure adottate da <b><u>non</u></b> modificare. <input type="checkbox"/> Piano delle misure adottate <b><u>da</u></b> modificare.	
Manutenzione delle apparecchiature			<input type="checkbox"/> Piano delle misure adottate da <b><u>non</u></b> modificare. <input type="checkbox"/> Piano delle misure adottate <b><u>da</u></b> modificare.	
Sicurezza dei cablaggi			<input type="checkbox"/> Piano delle misure adottate da <b><u>non</u></b> modificare. <input type="checkbox"/> Piano delle misure adottate <b><u>da</u></b> modificare.	
Dismissione di apparecchiature			<input type="checkbox"/> Piano delle misure adottate da <b><u>non</u></b> modificare. <input type="checkbox"/> Piano delle misure adottate <b><u>da</u></b> modificare.	
Gestione delle			<input type="checkbox"/> Piano delle misure	

comunicazioni			adottate da <b><u>non</u></b> modificare. <input type="checkbox"/> Piano delle misure adottate <b><u>da</u></b> modificare.	
Controlli di rete			<input type="checkbox"/> Piano delle misure adottate da <b><u>non</u></b> modificare. <input type="checkbox"/> Piano delle misure adottate <b><u>da</u></b> modificare.	
Controllo dei software			<input type="checkbox"/> Piano delle misure adottate da <b><u>non</u></b> modificare. <input type="checkbox"/> Piano delle misure adottate <b><u>da</u></b> modificare.	
Procedura di Back up			<input type="checkbox"/> Piano delle misure adottate da <b><u>non</u></b> modificare. <input type="checkbox"/> Piano delle misure adottate <b><u>da</u></b> modificare.	
Gestione dei supporti rimovibili			<input type="checkbox"/> Piano delle misure adottate da <b><u>non</u></b> modificare. <input type="checkbox"/> Piano delle misure adottate <b><u>da</u></b> modificare.	
Attività di informazione e formazione			<input type="checkbox"/> Piano delle misure adottate da <b><u>non</u></b> modificare. <input type="checkbox"/> Piano delle misure adottate <b><u>da</u></b> modificare.	

• **LEGENDA**

•

- **Ambito di controllo** <<indica gli elementi e le attività che vengono sottoposte al monitoraggio>>.
- **Data** << inserire la data in cui viene effettuato il controllo>>.
- **Soggetto attuatore del controllo** << inserire il ruolo del soggetto attuatore individuato tra il Responsabile del Trattamento Dati e l'Amministratore di Sistema; possono essere inseriti anche entrambi i soggetti>>.
- **Report** << selezionare tra le due opzioni quella corrispondente a ciascun evento controllato>>.
- **Attività di intervento** << questa sezione va compilata solo se vengono apportate delle modifiche alle misure già attuate e quindi vengono posti in essere taluni interventi migliorativi o vengono attivate delle contromisure>>

## ***YY) Conclusioni***

Questa sessione rappresenta la conclusione della vers. 1/2014.

Questo documento viene portato a conoscenza di tutti gli Utenti del Sistema Informatico Aziendale.

Tolentino, lì...../...../.....

~ 44 ~

*STUDIO MARCO MONDADORI*  
*Consulenza del Lavoro e Tributaria*  
*Viale Vittorio Veneto, 110*  
*62029 TOLENTINO (MC)*

*Studio Mondadori Marco*\_\_\_\_\_

*Per presa visione e accettazione*

*Il Responsabile del Trattamento Dati*

*Sig. Marco Mondadori*

\_\_\_\_\_

*L'Amministratore di Sistema –*

*Sig. Marco Mondadori*

\_\_\_\_\_

~ 45 ~

STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)

# ***DOCUMENTI ALLEGATI***

***Organigramma degli amministratori di  
sistema***

**ALLEGATO A)**

## **A) Introduzione**

L'Organigramma degli Amministratori di Sistema (*in sigla AdS*) riguarda l'attribuzione delle competenze di natura tecnico-informatica sia hardware che software caratterizzanti la struttura dello *Studio Marco Mondadori*.

La conoscenza della suddivisione dei compiti di natura tecnica è portata a conoscenza degli utenti del Sistema Informativo Aziendale non solo quale corretta osservanza di un adempimento legislativo, ma anche come dovere di trasparenza nei confronti del personale ed, al contempo, quale elemento di supporto nel caso di problematiche tecniche. Il criterio seguito è quello di rendere noti i nominativi dei soggetti incaricati allo svolgimento di specifiche operazioni appartenenti sia all'ambito tecnico-sistemistico che software.

Di seguito è fornita una breve illustrazione delle definizioni tecniche riportate nel presente organigramma, sottolineandone la validità all'interno della struttura per una sua più agevole lettura e comprensione.

### **\*GLOSSARIO**

a) *Data Administrator* << Amministratore di base di dati >>

b) *Net Administrator* << Amministratore di rete >>

c) *System Administrator* << Amministratore di Sistema >>

*STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)*

E' dovere della *Studio Marco Mondadori* provvedere alla comunicazione di ogni modificazione dei ruoli e dei soggetti nel momento in cui essi dovessero aver luogo.

L'operato degli Amministratori di Sistema è oggetto con cadenza annuale di un'attività di verifica da parte del responsabile del trattamento dati, al fine di accertare la rispondenza agli standard organizzativi e tecnici di tutto il Sistema Informativo Aziendale con particolare attenzione all'aspetto del monitoraggio dei livelli di rischio.

La *Studio Marco Mondadori* per l'anno 2014 conferisce i seguenti incarichi secondo le disposizioni emanate dal Provvedimento dell'Autorità Garante del 27 Novembre 2008.

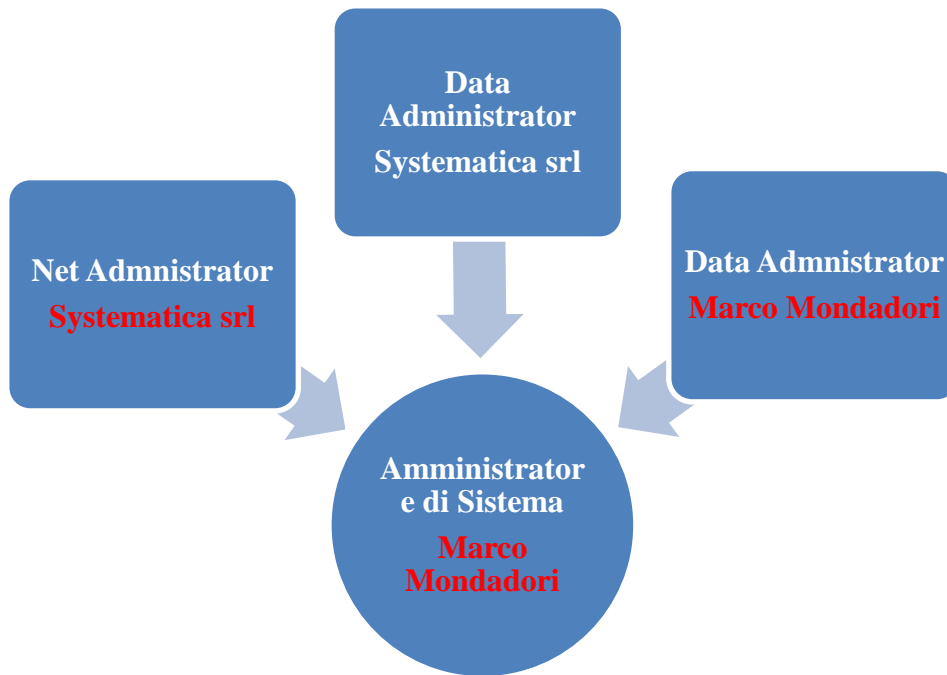
## ***B)Le fonti normative***

In questa sessione sono riportate le fonti normative di riferimento da cui derivano i principi e le regole stabilite.

1. **Provvedimento Generale Autorità Garante della Protezione dei Dati pubblicazione in Gazzetta Ufficiale nr 300 del 24 gennaio 2008**
2. **Provvedimento dell'Autorità Garante della Protezione dei Dati – Linee Guida per l'utilizzo degli strumenti elettronici e rete internet- Disciplinare Aziendale**
3. **Codice dell'Amministrazione Digitale (D.lgs. 82/2005) e successive modificazioni**

## ***C)I ruoli***

*STUDIO MARCO MONDADORI*  
*Consulenza del Lavoro e Tributaria*  
*Viale Vittorio Veneto, 110*  
*62029 TOLENTINO (MC)*





~ 49 ~

STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)

## **ANALISI DEI RISCHI INFORMATICI**

**ALLEGATO B)**



**CRITERI E VALUTAZIONI UTILIZZATI PER LA DESCRIZIONE DELLE VARIE**

**DISCIPLINARE AZIENDALE Vers. 1/2014**

## **TIPOLOGIE DI RISCHIO**

Le descrizioni riportate sono caratterizzate da una non grave incidenza di situazioni anomale che, comunque, hanno una probabilità più alta di verificarsi dal momento che il sistema informativo è in corso di implementazione.

I criteri che sono stati utilizzati hanno preso in considerazione i potenziali pericoli cui una mancata ottimizzazione ed un poco frequente controllo possono generare.

Nel caso di cessazione di qualsiasi rapporto di collaborazione si provvederà immediatamente alla chiusura di quel determinato account aziendale e parallelamente alla chiusura dei profili di accesso alla rete o a software specifici. Per quanto riguarda la situazione degli strumenti elettronici che come elaborato nelle precedenti tabelle, non è rischiosa, le motivazioni derivano dallo svolgimento di un servizio di assistenza e manutenzione tecnica eseguito dagli incaricati tecnici dell'azienda con una discreta periodicità che ha consentito di non avere situazioni bloccanti e di gestire in maniera più ordinata i vari interventi tecnici. Si può affermare che pur avendo non sottovalutato i pericoli derivanti da una non idonea gestione della riservatezza ed integrità dei dati, nel corso di quest'anno lo Studio ha considerato l'argomento con un'ottica diversa caratterizzata da un maggiore indice di prevenzione. Tuttavia ai fini del valore giuridico del contenuto della relazione sul piano della sicurezza dati, le descrizioni delle situazioni e, soprattutto, le considerazioni ivi riportate esprimono in maniera realistica le azioni correttive definite e le scelte idonee adottate dai vertici apicali. E' importante, infatti, ricordare che l'attività di trattamento dati (intendendo per tale ogni operazione avente ad oggetto il complesso informativo delle aziende) implica una responsabilità oggettiva disciplinata dall'art 2050 del codice civile; per cui sussiste un'inversione dell'onere probatorio che attribuisce a colui che è chiamato in causa la dimostrazione dell'aver optato per misure idonee nell'ambito del contesto fisico, lavorativo, delle risorse umane presenti.

La valutazione dei rischi viene in realtà svolta in maniera piuttosto continuativa proprio per verificarne la corrispondenza alle norme o per migliorarne la sicurezza in relazione ad ogni specifico tema e per ogni specifico settore.

Rispetto alla fase di analisi relazionata fino ad oggi, non si sono riscontrate situazioni pericolose né per la struttura né per la sicurezza ed integrità delle informazioni e dello stesso sistema.

**PREFAZIONE ALLE SINGOLE ANALISI**

Il **Responsabile della sicurezza dei dati personali** in collaborazione con gli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, anche avvalendosi di consulenti interni o esterni, deve verificare ogni anno:

- La situazione delle apparecchiature hardware installate con cui vengono trattati i dati
- La situazione delle apparecchiature periferiche
- La situazione dei dispositivi di collegamento con le reti pubbliche

La verifica ha lo scopo di controllare l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica, per quanto riguarda:

1. La sicurezza dei dati trattati.
2. Il rischio di distruzione o di perdita.
3. Il rischio di accesso non autorizzato o non consentito
4. La sicurezza dei dati trattati.
5. Il rischio di distruzione o di perdita.
6. Il rischio di accesso non autorizzato o non consentito
7. Rischi connessi al comportamento degli operatori
8. Rischi connessi al contesto fisico ed ambientale

Gli **Incaricati della gestione e della manutenzione degli strumenti elettronici** debbono aggiornare il **Report annuale dei rischi hardware**.

In conformità a quanto disposto dal **punto 19.3 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003)** il modulo deve essere allegato al presente Documento Programmatico sulla Sicurezza.

Gli **Incaricati della gestione e della manutenzione degli strumenti elettronici** nel caso in cui esistano rischi evidenti debbono informare tempestivamente il **Responsabile della sicurezza dei dati personali** affinché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

## RISCHI SOFTWARE

### □ VIRUS

La tipologia di rischio causato dal virus rappresenta una situazione frequente, ma caratterizzata da un basso grado di pericolo. Infatti gli elementi antintrusione attuati come misure di contrasto permettono di rilevare solamente il file infetto e permettono successivamente di eliminarlo.

Nell'unità server centrale e nei vari clients è installato l'antivirus\_ per bloccare ed eliminare la presenza di file infetti. L'aggiornamento costante in modalità automatica del software antivirus consente di ridurre la percentuale di insidie; tuttavia in alcuni casi si sono verificate situazioni in cui alcuni strumenti sono stati "colpiti". L'entità del danno è stata ridotta e soprattutto non ha riguardato i database principali.

### □ BUGS

I programmi utilizzati per la gestione della contabilità che dei servizi gestionali risultano essere stabili.

Tale spiegazione è collegata al fatto che tali programmi vengono costantemente controllati, facendo riferimento alla società incaricata dell'assistenza e dell'aggiornamento del software:

- MULTI per paghe e contabilità

### □ ERRORI DI INSTALLAZIONE ED UTILIZZO DEI SOFTWARE

L'ipotesi in esame non trova riscontri in questa realtà quindi, evidenzia un basso grado di rischio.

Per quanto attiene alle fasi di installazione del programma ed eventuali sui aggiornamenti, il personale incaricato alla gestione di tale software è in grado di eseguire tali operazioni senza determinare errori per i database presenti. Inoltre, oggi, le modalità di installazione ed aggiornamento degli applicativi sono migliorate ed avvengono in molti casi mediante collegamento ad internet e scarico del plug in relativo alla nuova versione rilasciata. Tale attività tecnicamente definita "live-update" risulta essere anche più veloce, meno pesante ed in molti casi riduce il rischio di conflitti con altri software. Per quanto riguarda l'ipotesi di errori causati da un non corretto

utilizzo dei software si afferma che il livello di rischio è basso anche se, a volte, questa situazione si è verificata nella nostra realtà.

#### **□ RISCHIO DI FRODE INFORMATICA**

Il rischio che si possa verificare una frode informatica connessa è considerato basso. Nell'ambito di questo paragrafo si precisa che le misure contro il rischio prendono in considerazione anche le credenziali rilasciate dagli enti istituzionali per lo svolgimento dei corrispondenti adempimenti legislativi. L'organizzazione del sistema informatico è caratterizzata dall'attuazione di misure di sicurezza finalizzate a prevenire intrusioni ed accessi non autorizzati; pertanto questi elementi rappresentano una barriera al tentativo di effettuare una frode informatica.

#### **□ RISCHIO CAUSATO DA FENOMENI COME PHISHING O PHARMING**

La valutazione del grado di rischio come medio è motivata dalla rapida evoluzione di questi reati rispetto alle misure di protezione attuate ed alla capacità di discernimento degli utenti. L'unico elemento che costituisce un freno alla rigidità delle misure presenti è determinato dal comportamento degli utenti. Infatti ciò che si vuol evidenziare è la non esperienza tecnica del personale il quale nonostante sia stato informato potrebbe non essere in grado di distinguere prontamente i fenomeni in oggetto.

#### **□ RISCHIO DI VIOLAZIONE DEL DIRITTO D'AUTORE**

Questa ipotesi di rischio viene esaminata in conseguenza della definizione delle policy di corretto comportamento stabilite da questo studio e portate a conoscenza di tutto il personale. E' stato espressamente vietata l'effettuazione di download da internet o da supporti senza licenza né autorizzazione dei responsabili. Non è parimenti consentito scaricare file musicali o di altro tipo e per ragioni di sicurezza, lo *Studio Marco Mondadori* ha disposto il divieto ad effettuare operazioni di questo tipo. Inoltre il personale è a conoscenza anche delle responsabilità e delle relative sanzioni che verranno attuate nel caso di download di materiale non autorizzato ed illecito, basti pensare all'installazione di software musicali o film coperti dal diritto d'autore. Alla luce della

situazione odierna le probabilità di accadimento di questo evento rischioso non sono alte, ma si consiglia di monitorarne l'evoluzione.

#### **□ RISCHIO DI PERDITA DELLE CREDENZIALI**

Il rischio di perdita delle credenziali di autorizzazione ed autenticazione non ha, ad oggi, trovato riscontro. Lo Studio ha comunicato sia mediante l'elaborazione degli atti privacy di trattamento dati per ciascun collaboratore, sia attraverso la redazione di un Disciplinare Aziendale, le regole e le responsabilità in merito alla custodia delle password. Ogni utente è, infatti, profilato all'interno del sistema informativo in base alle diverse competenze ed è tenuto a non comunicare la credenziale né a renderla visibile a terzi (ad esempio con la sua trascrizione in post-it o in fogli lasciati incustoditi sopra le scrivanie). In caso di perdita, intesa come dimenticanza, ciascun utente è tenuto ad inviare la richiesta al Responsabile Interno della Sicurezza dati per una nuova assegnazione dal momento che è vietato il riutilizzo della medesima password. Si precisa che ai fini della presente Analisi dei Rischi il termine credenziale è esteso ad ogni tipologia di autenticazione definita comprese (come sopra riportato) quelle rilasciate dai vari Enti Istituzionali.

#### **□ RISCHIO DI PERDITA DELLE INFORMAZIONI**

Lo Studio Marco Mondadori ha disposto il divieto di copiare qualsiasi tipo di dato ed in qualunque formato contenente informazioni aziendali. Sicuramente l'introduzione di policies scritte dovrebbe rappresentare, accanto alla sua conformità normativa, un deterrente a seguito della sua pubblicazione ufficiale.

#### **□ RISCHIO DI INTEGRITA' DEI DATI**

Il rischio di integrità è qui inteso come assenza di alterazioni dei database nel medio termine. E' un elemento che viene sempre più monitorato dallo Studio Marco Mondadori in conseguenza della crescita delle elaborazioni digitali. Attualmente l'azione preventiva intrapresa è caratterizzata dall'impostazione di due diverse procedure che vengono effettuate giornalmente in modalità automatica dal server stesso.

#### **□ RISCHIO CAUSATO DAI COMPORTAMENTI DEGLI OPERATORI PER IL MANCATO RISPETTO DELLE POLICY AZIENDALI**

*STUDIO MARCO MONDADORI*  
*Consulenza del Lavoro e Tributaria*  
*Viale Vittorio Veneto, 110*  
*62029 TOLENTINO (MC)*

La valutazione del livello di rischio è stata per il momento considerata bassa in quanto lo *Studio Marco Mondadori* ha iniziato da poco la redazione e la comunicazione di un Disciplinare in cui vengono riportate tutte le regole da osservare nell'ambito del rapporto lavorativo. Le fattispecie analizzate fanno riferimento sia alle modalità di gestione dei dati attinenti al rapporto di lavoro che all'utilizzo della posta elettronica e rete internet. Il disciplinare è stato consegnato a mano a tutto il personale interno e vi sono state descritte le policy da seguire unitamente alle modalità di controllo ed all'applicazione delle relative sanzioni.

**□ EVENTI RELATIVI AL CONTESTO: GUASTO AI SISTEMI COMPLEMENTARI . (IMPIANTO ELETTRICO, CLIMATIZZAZIONE, ECC.)**

Attualmente all'interno di questa realtà sono presenti dei gruppi di continuità all'interno del sistema informativo aziendale. La struttura dell'impianto elettrico, di climatizzazione è conforme agli standard di sicurezza e viene sottoposta a periodica manutenzione.

**➤ RISCHIO DERIVANTE DALLA VIOLAZIONE DELLA RISERVATEZZA**

Questa situazione si può verificare nel caso in cui qualcuno comunichi informazioni riservate dello *Studio Marco Mondadori* e dei suoi clienti a terzi. Ovviamente è difficile riuscire a mettere subito in luce tale evento; tuttavia la definizione di un assetto organizzativo piuttosto rigido e distinto con profili specifici rappresenta un valido supporto. Il rischio di comunicazioni non autorizzate potrebbe aver luogo anche mediante azione di copia su supporti esterni di file. Quest'ultima fattispecie potrebbe risultare più facile da rintracciare. Nell'ambito dell'adozione di misure preventive, si sottolinea che è stato comunicato a tutto il personale il divieto e le relative sanzioni in caso in cui qualcuno attui l'evento sopra descritto; inoltre non è consentito trasportare fuori dagli uffici della sede documenti e pratiche salvo che non sussista una motivazione da parte del responsabile e per gli scopi connessi con le prestazioni svolte.

A conclusione dell'analisi il grado di pericolo è ad oggi considerato basso.

**□ RISCHIO DI GUASTO DEGLI STRUMENTI DERIVANTE DA UN NON CORRETTO UTILIZZO**

*STUDIO MARCO MONDADORI*  
*Consulenza del Lavoro e Tributaria*  
*Viale Vittorio Veneto, 110*  
*62029 TOLENTINO (MC)*

Sono state definite le policy inerenti la corretta tenuta degli strumenti da lavoro, come quelli elettronici. Il rischio di danni causati volontariamente per incuria è basso dal momento che periodicamente i computer vengono a turno sottoposti ad un'ordinaria manutenzione da parte del consulente tecnico incaricato della pianificazione degli interventi di assistenza..

Le misure di contrasto definite permettono una valutazione bassa del rischio in esame.

#### **RISCHIO DI ERRORI NELLE ELABORAZIONI**

Durante le elaborazioni dei dati può capitare che si generano degli errori di trascrizione da parte degli operatori, ma questo acquisisce solo una valenza positiva, cioè non origina danni contingenti e volontari. Nell'ordinaria attività lavorativa, la correzione degli errori di trascrizione avviene quasi sempre dal personale e per questo non si creano situazioni rischiose.

#### **NOTE CONCLUSIVE**

Al momento della rilevazione dei rischi sopra elencati e descritti la *Studio Marco Mondadori* in conseguenza anche delle misure di prevenzione adottate, attesta un range di **RISCHIO BASSO** con la prescrizione di effettuare un monitoraggio semestrale quale intervento migliorativo e di contrasto alle evoluzioni tecnologiche e normative unitamente al controllo dell'eventuale problema dell'obsolescenza tecnologica.



## **PROCEDURA PER LA GESTIONE E CONSERVAZIONE DELLE PASSWORD**

**ALLEGATO C)**

Lo *Studio Marco Mondadori* ha definito una procedura volta a garantire la riservatezza e la sicurezza nella conservazione delle password di accesso ai vari programmi e/o altri applicativi in conformità a quanto stabilito dalle recenti disposizioni legislative in materia di reati informatici e sicurezza nel trattamento dei dati.

Ogni utente autorizzato all'accesso al sistema informatico dello *Studio Marco Mondadori* viene identificato mediante l'attribuzione da parte del system administrator di un nome (definito user) e di un codice (definito password) con cui può effettuare le operazioni consentite al suo ambito di competenza.

Nel linguaggio informatico-giuridico questi elementi prendono il nome di "credenziali di autenticazione" e "credenziale di autorizzazione" e richiedono l'osservanza di precise regole a cui sono correlate in caso di mancato rispetto, talune responsabilità anche di natura penale.

Di seguito viene descritta la procedura:

- al momento della sua impostazione a ciascun utente viene consegnato un modulo specifico in cui egli deve trascrivere il proprio user e la password che gli è stata preventivamente comunicata dal system administrator;
- questi codici che devono essere composti da un numero di elementi non inferiore a 8 e preferibilmente con unione di lettere e numeri, non devono essere comunicati ad alcuno
- il responsabile è tenuto a garantire la massima sicurezza nella conservazione di questi dati;
- attualmente lo Studio ha adottato una periodicità di cambio delle password fissata in tre mesi, ma con una modalità automatica di gestione;
- la busta contenente tali codici deve essere firmata da ciascun utente e consegnata chiusa all'Amministratore di Sistema Signor Marco Mondadori attualmente incaricato dalla scrivente società quale soggetto responsabile della custodia delle password.
- nel caso di sostituzione degli attuali incaricati alla gestione delle password la società dovrà procedere ad effettuare una nuova nomina a cui verrà sottoposta la presa visione della presente procedura;

*STUDIO MARCO MONDADORI*  
*Consulenza del Lavoro e Tributaria*  
*Viale Vittorio Veneto, 110*  
*62029 TOLENTINO (MC)*

- tutti i computer hanno una password d'accesso;
- Ogni variazione delle credenziali che deve essere attuata per esigenze lavorative, potrà essere effettuata solo a seguito di autorizzazione da parte dell'Amministratore di Sistema; infatti non sono consentite iniziative autonome e personali.

Le modalità sopra descritte riguardano ogni eventuale tipo di credenziale (user id e password) impostata e comunicata all'utente dallo *Studio Marco Mondadori* sia essa riferita ad applicazioni installate all'interno di questo sistema informatico sia riferita ad accessi a sistemi esterni.

Il soggetto preposto al controllo delle regole stabilite è l'Amministratore di Sistema Signor Marco Mondadori che potrà procedere alla comunicazione di eventuali anomalie al fine di definire un'eventuale disciplina correttiva.

Questa procedura viene attuata a partire dal\_\_\_\_\_

### ***PROCEDURA DELEGA CONOSCENZA CREDENZIALI UTENTE***

**ALLEGATO D)**

#### ▪ **SCOPO**

La presente procedura ha lo scopo di definire le modalità di impiego del "*Modulo Delega per l'Accesso alle Credenziali di Autenticazione ed Autorizzazione*" da parte di tutti gli Utenti del Sistema Informativo dell'Ente Titolare. Si precisa che in questo contesto, il termine "Ente Titolare" identifica sia una persona giuridica di diritto pubblico che di diritto privato e sia una persona fisica in qualità di interessato.

#### ▪ **MODALITA' DI USO**

*Il Modulo Delega per l'Accesso alle Credenziali di Autenticazione ed Autorizzazione* deve essere utilizzato dall'Utente quando:

- a) in caso di assenza prolungata nel momento in cui vengono attribuiti temporaneamente i compiti lavorativi ad un terzo;
- b) in caso di sostituzione temporanea di un Utente per il compimento di determinate attività;

c) in caso di necessità urgente e straordinaria.

▪ **VALIDAZIONE DEL MODULO**

La validazione del Modulo Delega per l'Accesso alle Credenziali di Autenticazione ed Autorizzazione deve avvenire da parte del titolare o del Responsabile di Settore ( se autorizzato) mediante l'apposizione della sottoscrizione in calce al modulo stesso. Costituisce requisito di validità l'apposizione della data.

• **MODALITA' DI COMUNICAZIONE DEL MODULO**

Il Modulo Delega per l'Accessi alle Credenziali di Autenticazione deve essere portato a conoscenza a tutti i soggetti delegante e delegato sia in modalità cartacea che elettronica mediante inoltro agli indirizzi email degli interessati.

**MODULO DELEGA PER L'ACCESSO ALLE CREDIZIALI DI AUTENTICAZIONE E DI  
AUTORIZZAZIONE**

Come disposto dal Provvedimento Generale emanato dall'Autorità Garante della Privacy in data 1 marzo 2007, il/la sottoscritto/a \_\_\_\_\_ con questo atto delego/a il/la Sig.ra \_\_\_\_\_ al compimento delle seguenti attività:

accesso alla mia casella di posta elettronica aziendale \_\_\_\_\_ per la consultazione dei messaggi presenti sia *in arrivo* che *in invio*;

accesso alla mia casella di posta elettronica aziendale \_\_\_\_\_ per l'invio dei messaggi di posta;

~ 60 ~

*STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)*

- accesso alla gestione delle banche dati a me autorizzate mediante l'uso del mio profilo utente e della relativa credenziale (*indicare le banche dati* \_\_\_\_\_);
- stampa, fascicolazione ed organizzazione della documentazione cartacea delle trattative temporaneamente gestite;

Il delegato s'impegna ad osservare le regole di riservatezza relative ad ogni tipologia di dato aziendale cui viene a conoscenza. Al rientro il delegante è tenuto a modificare il proprio profilo di accesso e a darne comunicazione al Responsabile Interno del Trattamento Dati ed all'Amministratore di Sistema.

Il presente documento ha efficacia tra le parti fino al cambio del profilo del delegante e quindi fino al momento di ripristino delle ordinarie autorizzazioni del delegante e del delegato.

Tolentino, lì \_\_\_\_\_

In fede

*Data e Firma del delegante*

*Data e firma del delegato*

\_\_\_\_\_

\_\_\_\_\_

*Per presa visione ed accettazione-*

*Il Responsabile Interno del Trattamento Dati- Signor Marco Mondadori* \_\_\_\_\_

*Per presa visione ed accettazione*

*L'Amministratore di Sistema- Signor Marco Mondadori* \_\_\_\_\_

**REGISTRO DI EMERGENZA**

**ALLEGATO E)**

*STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)*

Nel caso di inconvenienti tecnici, che dovessero protrarsi oltre le 48 ore, il Responsabile del Trattamento Dati congiuntamente con l'Amministratore di Sistema attivano un **Registro di Emergenza** in cui vengono annotati gli eventi anomali che hanno originato la situazioni di rischio, black out, interruzione all'intero sistema informativo aziendale.

Per attivare il registro di emergenza si deve verificare almeno una delle seguenti condizioni:

- 1) guasto al software;
- 2) guasto al sistema informatico di gestione;
- 3) mancanza di energia elettrica;
- 4) attacco Hacker;
- 5) calamità naturale;
- 6) altro (specificare)

Qualora una di queste condizioni si protraesse oltre le 48 ore, è attivato il Registro di Emergenza su supporto cartaceo in cui dovranno essere riportate le seguenti informazioni:

<b>Data evento</b>	
<b>Ora interruzione</b>	
<b>Causa</b>	

<b>Risoluzione dell'anomalia</b>	
<b>Data ripristino</b>	
<b>Ora ripristino</b>	
<b>Commento</b>	

Ogni verbale, costituente il Registro di Emergenza, dovrà essere numerato in modalità progressiva, dovrà essere conservato presso la sede dell'azienda nel fascicolo in cui viene conservata la documentazione in materia di sicurezza e riservatezza dei dati e dovrà essere sottoscritto sia dal Responsabile del Trattamento Dati che dall'Amministratore di Sistema. Il Registro di Emergenza dovrà essere aggiornato ogni anno ovvero, nel caso di assenza di eventi anomali, dovrà contenere un verbale di chiusura ed uno di apertura dell'anno corrente.

~ 62 ~

STUDIO MARCO MONDADORI  
Consulenza del Lavoro e Tributaria  
Viale Vittorio Veneto, 110  
62029 TOLENTINO (MC)

## COMUNICAZIONE AGLI UTENTI DEL DISCIPLINARE AZIENDALE

ALLEGATO F)

Il presente Disciplinare Aziendale viene portato a conoscenza degli Utenti del Sistema Informativo dello *Studio Marco Mondadori* che provvedono ad apporre la loro sottoscrizione, nella tabella sottostante, per ricevuta ed accettazione:

Nome e Cognome	Firma
Petrelli Eleonora	

~ 63 ~

*STUDIO MARCO MONDADORI*

*Consulenza del Lavoro e Tributaria*

*Viale Vittorio Veneto, 110*

*62029 TOLENTINO (MC)*

<b>Pascucci Leda</b>	
<b>Perroni Pisana</b>	
<b>Loncorelli Monica</b>	
<b>Ranieri Emanuela</b>	