Policy Sicurezza Informatica

Rev.	Data	Descrizione modifica	Redazione	Verifica	Approvazione CEO
00	18.04.2016	Prima emissione	DG / IT Dept	18-04-2016	18-04-2016
01	20.11.2019	Revisione 2019	DG / IT Dept	31-10-2019	20-11-2019
02	08.02.2022	Revisione 2022	DG / IT Dept	31-01-2022	08-02-2022
03	07.12.2022	Revisione 2023	DG / IT Dept	30-11-2022	07-12-2022
				Francesco Lombardo	Enrico Frizzera

POLICY SULLA SICUREZZA INFORMATICA

DISPOSIZIONI, REGOLE DI COMPORTAMENTO E MISURE ORGANIZZATIVE PER IL CORRETTO UTILIZZO DEGLI STRUMENTI DIGITALI AZIENDALI E PER LA PREVENZIONE DEI REATI INFORMATICI

INDICE

Premessa

Il presente regolamento (di seguito anche Policy) è adottato da Manni Group S.p.A. e consociate (di seguito anche il "Titolare" o la "Società") per disciplinare il corretto comportamento e utilizzo degli strumenti digitali aziendali al fine di prevenire la commissione – nell'interesse o a vantaggio della stessa – di talune condotte, nel rispetto quindi della normativa privacy, delle policies e delle linee guida del Gruppo, la normativa vigente a livello nazionale (Regolamento Europeo 2016/679 GDPR, il Decreto Legislativo 196/2003, il D.Lgs 101/2018, e successive modifiche e integrazioni), individua l'ambito e le modalità con cui possono essere trattati i dati personali.

Attraverso la Policy vengono così definite le regole tecniche ed organizzative da applicare e rispettare, nonché quelle per l'utilizzo della posta elettronica e per la navigazione in Internet da parte dei dipendenti nell'ambito dello svolgimento delle loro mansioni. La progressiva diffusione delle nuove tecnologie informatiche, le maggiori possibilità di interconnessione tra computer e l'incremento di informazioni trattate con strumenti elettronici aumentano, infatti, i rischi legati alla sicurezza e all'integrità delle informazioni, oltre alle conseguenti responsabilità previste dalla normativa vigente in materia.

Pertanto, a seguito dell'adozione della presente Policy, il Titolare auspica che l'utilizzo delle risorse informatiche e telematiche aziendali avverrà nell'ambito del generale contesto di diligenza, fedeltà e correttezza che caratterizza il rapporto lavorativo fra il Titolare e i propri dipendenti e, quindi, che verranno adottate tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose che un utilizzo non avveduto dei suddetti strumenti può comportare.

La presente Policy descrive le regole tecniche ed organizzative da applicare per garantire il corretto uso degli strumenti informatici, nonché per l'utilizzo della posta elettronica e per la navigazione Internet, installati sulle stazioni di lavoro di proprietà del Titolare. Inoltre, esso detta disposizioni dirette a prevenire condotte delittuose poste in essere attraverso comportamenti idonei a integrare, mediante azioni od omissioni, le fattispecie di reato previste dall'ordinamento in tema di reati informatici. L'attuale edizione del Regolamento si ispira ai principi e alle indicazioni presenti nel Modello di Organizzazione Gestione e Controllo redatto ai sensi del D.Lgs. 231/2001.

Il documento sarà periodicamente riesaminato ed aggiornato per assicurare che gli obiettivi in esso indicati siano mantenuti ed adeguati rispetto ai mutamenti normativi ed alle nuove minacce informatiche.

Per limitare al massimo la commissione di suddetti reati, occorre sicuramente partire da una responsabilizzazione di tutti i soggetti che ivi lavorano. Per questo motivo, la Società predisporrà corsi di formazione interna al fine di fornire ai propri dipendenti elementi che consentiranno di perfezionare la loro conoscenza e sensibilità sulle tematiche inerenti alla gestione del rischio informatico e, comprendere al meglio ciò che si può e ciò che non si deve fare con gli strumenti informatici.

Pertanto, saranno previste sanzioni nei confronti di soggetti che violino in maniera intenzionale i sistemi di controllo o le indicazioni comportamentali fornite.

Proprietà delle attrezzature

I personal computer con relative periferiche (di seguito indicati più brevemente come postazione di lavoro), Smartphone o Tablet, gli accessi Internet, le caselle di posa elettronica, gli spazi Web, le applicazioni accessibili tramite la rete, applicazioni (Office365, Posta Elettronica, Microsoft Teams, etc. etc.) concessi in dotazione ai dipendenti (di seguito indicati più brevemente con il termine RISORSE), sono beni di proprietà di Manni Group S.p.A. che, in quanto tali, devono essere utilizzati esclusivamente come strumenti di lavoro per l'attuazione dei compiti aziendali e mai per ragioni private.

Dette risorse sono affidate al dipendente che deve custodirle in modo appropriato e, deve tempestivamente informare il Responsabile e/o il Titolare in caso di un eventuale furto, del loro danneggiamento o smarrimento.

La risorsa è data in uso al dipendente in relazione al ruolo ricoperto e alle mansioni assegnate e, il Responsabile e/o il Titolare, si riserverà il diritto di sospendere l'utilizzo della stessa qualora venga utilizzata in modo improprio, non sia necessaria all'esecuzione delle attività del dipendente o nel caso in cui termini il periodo di rapporto di lavoro tra il dipendente e l'azienda.

L'uso della risorsa è strettamente personale ed è affidato a ciascun dipendente con l'impegno a non cederla o farla utilizzare a terzi non autorizzati.

Poiché, le suddette attrezzature sono concesse al dipendente come strumenti di lavoro, è severamente vietato conservare o memorizzare qualsiasi informazione di carattere personale; nel caso in cui il dipendente contravvenisse a tale disposizione, l'azienda declina ogni responsabilità circa la possibile perdita e/o divulgazione di tali dati, obbligando in ogni caso il dipendente, ad informare il suo superiore responsabile della presenza di dati personali memorizzati sui computer, della ragione di tale azione, nonché dell'indicazione delle cartelle che contengono sia *file* di tipo personale che *file* aziendali.

1. Adozione della Policy di Organizzazione e Gestione da parte della Società

Il Titolare, al fine di assicurare sempre più condizioni di correttezza e di trasparenza nella gestione degli affari e delle attività aziendali, ha ritenuto conforme alle proprie politiche aziendali, ed in sintonia con le indicazioni dei vertici Aziendali di procedere all'adozione di una Policy di organizzazione e di gestione in linea con le prescrizioni del Decreto Legislativo n. 231/2001 e del Regolamento UE 679/2016.

Tale iniziativa è stata assunta nella convinzione che l'adozione di tale Policy possa costituire un valido strumento di sensibilizzazione nei confronti di tutti i dipendenti della Società e di tutti gli altri soggetti alla stessa cointeressati (Clienti, Fornitori, Partners, Collaboratori a diverso titolo), affinché seguano, nell'espletamento delle proprie attività, comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei reati contemplati nel Decreto.

La Policy predisposta da Manni Group S.p.A. si fonda su un sistema strutturato ed organico di procedure nonché di attività di controllo che nella sostanza:

- individuano le aree/i processi di possibile rischio nell'attività aziendale vale a dire quelle attività nel cui ambito si ritiene più alta la possibilità che siano commessi i reati;
- definiscono un sistema normativo interno diretto a programmare la formazione e l'attuazione delle decisioni della società in relazione ai rischi/reati da prevenire, così da fissare le linee di orientamento generali, e procedure formalizzate, tese a disciplinare in dettaglio le modalità operative nei settori "sensibili";
- determinano una struttura organizzativa coerente volta ad ispirare e controllare la correttezza dei comportamenti, garantendo una chiara ed organica attribuzione dei compiti, applicando una giusta

segregazione delle funzioni, assicurando che gli assetti voluti della struttura organizzativa siano realmente attuati;
- attribuiscono all'Organismo di Vigilanza il compito di vigilare sul funzionamento e sull'osservanza della Policy e di proporne l'aggiornamento.

Pertanto la Policy si propone come finalità quelle di:
- predisporre un sistema strutturato ed organico di prevenzione e controllo finalizzato alla riduzione del rischio di commissione dei reati connessi all'attività aziendale con particolare riguardo alla riduzione di eventuali comportamenti illegali;
- determinare, in tutti coloro che operano in nome e per conto del Titolare nelle "aree di attività a rischio", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni sul piano penale ed amministrativo, non solo nei propri confronti ma anche nei confronti dell'azienda;
- informare tutti coloro che operano a qualsiasi titolo in nome, per conto o comunque nell'interesse del Titolare che la violazione delle prescrizioni contenute nella Policy comporterà l'applicazione di apposite sanzioni ovvero la risoluzione del rapporto contrattuale;
- ribadire che la Società non tollera comportamenti illeciti, di qualsiasi tipo ed indipendentemente da qualsiasi finalità, in quanto tali comportamenti (anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio) sono comunque contrari ai principi etici cui Manni Group S.p.A. intende attenersi.

2. Funzioni e poteri dell'organismo di vigilanza in tema di reati informatici

La *mission* dell'Organismo di Vigilanza di Manni Group S.p.A. in tema di reati informatici consiste in generale nel:
1) vigilare sull'applicazione della Policy in relazione alle diverse tipologie di reati contemplate dal Decreto Legislativo n. 231 del 2001;
2) verificare l'efficacia della Policy e la sua capacità di prevenire la commissione dei reati di cui al Decreto legislativo n. 231 del 2001;
3) individuare e proporre al Consiglio di Amministrazione aggiornamenti e modifiche della Policy stessa in relazione alla mutata normativa o alle mutate condizioni aziendali.

Su di un piano più operativo sono affidati all'Organismo di Vigilanza i seguenti compiti:
- verificare periodicamente la mappa delle aree a rischio reato al fine di adeguarla ai mutamenti dell'attività e/o della struttura aziendale. A tal fine il Management e gli addetti alle attività di controllo, nell'ambito delle singole funzioni, devono segnalare all'Organismo di Vigilanza le eventuali situazioni in grado di esporre l'azienda al rischio di reato. Tutte le comunicazioni devono essere scritte (anche via e-mail) e non anonime;
- raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto della Policy, nonché aggiornare la lista di informazioni che devono essere obbligatoriamente trasmesse allo stesso Organismo di Vigilanza;

- condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni della presente Policy portate all'attenzione dell'Organismo di Vigilanza da segnalazioni o emerse nel corso dell'attività di vigilanza dello stesso;
- verificare che i comportamenti e le misure previste dalla Policy per le diverse tipologie di reati siano comunque adeguate e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto, provvedendo, in caso contrario, a proporre aggiornamenti degli elementi stessi.

Per lo svolgimento dei suddetti compiti, l'Organismo di Vigilanza:

- gode di ampi poteri ispettivi e di accesso ai documenti aziendali;
- dispone di risorse professionali adeguate;
- si avvale del supporto e la cooperazione delle varie strutture aziendali che possano essere interessate o comunque coinvolte nelle attività di controllo.

In ambito aziendale dovrà essere portata a conoscenza dell'Organismo di Vigilanza ogni informazione, di qualsiasi tipo, proveniente anche da terzi ed attinente all'attuazione della Policy nelle aree di attività a rischio.
Valgono al riguardo le seguenti prescrizioni:

- devono essere raccolte eventuali segnalazioni relative alla violazione della Policy o comunque conseguenti a comportamenti non in linea con le regole di condotta adottate dalla Società stessa;
- l'Organismo di Vigilanza valuterà le segnalazioni ricevute e le eventuali conseguenti iniziative a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il Responsabile della presunta violazione e motivando per iscritto eventuali rifiuti di procedere ad una indagine interna;
- le segnalazioni dovranno essere in forma scritta e non anonima ed avere ad oggetto ogni violazione o sospetto di violazione della Policy. L'Organismo di Vigilanza agirà in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della società o delle persone accusate erroneamente e/o in mala fede;
- le segnalazioni pervenute all'Organismo di Vigilanza devono essere raccolte e conservate in un apposito archivio al quale sia consentito l'accesso solo da parte dei membri dell'Organismo di Vigilanza.

Oltre alle segnalazioni anche ufficiose, devono essere obbligatoriamente trasmesse all'Organismo di Vigilanza le informative concernenti:

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto Legislativo n. 231/2001;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto Legislativo n. 231/2001;
- i rapporti preparati dai responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo e dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto Legislativo n. 231/2001;

- le notizie relative all'effettiva attuazione a tutti i livelli aziendali della Policy, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i Dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

3. Responsabile del trattamento dei dati personali e Responsabile della protezione dei dati (DPO)

3.1 Responsabile del trattamento dei dati personali

Secondo quanto previsto dall'art. 28 del Regolamento UE n. 679/2016 (di seguito anche GDPR), qualora un trattamento debba essere effettuato per conto del Titolare del trattamento, quest'ultimo ricorra unicamente a Responsabile del trattamento che presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento Europeo e garantisca la tutela dei diritti dell'interessato. Il GDPR stabilisce che il Responsabile del trattamento non ricorra a un altro Responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento. Nel caso di autorizzazione scritta generale, il Responsabile del trattamento informa il Titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri Responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche. I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il Responsabile del trattamento al Titolare del trattamento e che stipuli la materia

disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.

Il contratto o altro atto giuridico prevede, in particolare, che il Responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del trattamento; in tal caso, il Responsabile del trattamento informa il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32 del GDPR;
d) rispetti le condizioni imposte dal GDPR per ricorrere a un altro Responsabile del trattamento;
e) tenendo conto della natura del trattamento, assista il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui all'art. 15 e ss. del GDPR;
f) assista il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR (pseudonimizzazione e cifratura dati; capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; capacità di ripristinare tempestivamente la disponibilità e

l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento; l'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 del GDPR può essere utilizzata come elemento per dimostrare la conformità ai requisiti previsti dal GDPR; notifica di una violazione dei dati personali all'autorità di controllo; comunicazione di una violazione dei dati personali all'interessato; valutazione di impatto sulla protezione dei dati; consultazione preventiva dell'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio);

g) su scelta del Titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

h) metta a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h), il Responsabile del trattamento informa immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Quando un Responsabile del trattamento ricorre a un altro Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento, su tale altro Responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il Titolare del trattamento e il Responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR. Qualora l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile. L'adesione da parte del Responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 del GDPR o a un meccanismo di certificazione approvato di cui all'articolo 42 del GDPR può essere utilizzata come elemento per dimostrare le garanzie previste. Fatti salvi gli articoli 82, 83 e 84 del GDPR di disciplina e responsabilità delle sanzioni amministrative e pecuniarie inflitte nell'ipotesi di violazione del GDPR, se un Responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un Titolare del trattamento in questione.

3.2 Responsabile della protezione dei dati (DPO)

Il Titolare del trattamento e il Responsabile del trattamento designano sistematicamente un Responsabile della protezione dei dati (di seguito anche DPO) ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
c) le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10 del GDPR.

Il Responsabile della protezione dei dati (DPO) è designato in funzione delle qualità professionali, in ragione della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 del GDPR. Il Titolare del trattamento e il Responsabile del trattamento si assicurano che il Responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. Inoltre, essi sostengono il DPO nell'esecuzione dei compiti di cui all'articolo 39 sopra richiamato fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali, ai trattamenti e per mantenere la propria conoscenza specialistica.

Il DPO è individuato tra soggetti che per esperienza, capacità ed affidabilità fornisca idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Egli effettua il trattamento stesso, attenendosi alle istruzioni impartite dal Titolare dei dati il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle istruzioni impartite.

Pertanto, a seguito di formale nomina scritta da parte del Titolare, il Responsabile designato dal Titolare si obbliga a:

- eseguire esclusivamente operazioni di trattamento funzionali alle mansioni ad esso attribuite. Qualora dovesse sorgere la necessità di effettuare trattamenti sui dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, il Responsabile dovrà darne tempestiva informativa al Titolare del trattamento;
- operare nel continuativo rispetto dei principi di correttezza, liceità, esattezza, pertinenza e completezza del trattamento medesimo;
- mantenere la più completa riservatezza sui dati trattati e sulle tipologie di trattamento effettuate; tale obbligo è da considerarsi pienamente vigente anche nel caso di cessazione del rapporto di impiego e/o comunque di collaborazione;
- verificare periodicamente l'adeguatezza delle misure di sicurezza adottate in relazione ai trattamenti di propria competenza, valutando se mutamenti dell'attività di trattamento e/o della tipologia di dati trattati non determinino l'adozione di misure di sicurezza diverse e più adeguate, ed in tal caso provvedere alla relativa adozione dandone tempestiva comunicazione al Titolare;

- individuare e nominare per iscritto i sub-Responsabili, (persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile) impartendo loro, sempre per iscritto, apposite istruzioni che tengano conto delle misure di sicurezza, prescrivendo che essi abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati. Nel caso di trattamento elettronico dei dati, dovrà inoltre verificare che i singoli sub-Responsabili applichino tutte le prescrizioni di sicurezza relative alla custodia delle parole chiave;
- comunicare immediatamente al Titolare del trattamento gli eventuali nuovi trattamenti da intraprendere nel suo settore di competenza, provvedendo alle eventuali e necessarie formalità di legge;
- interagire con i sub-Responsabili incaricati di effettuare eventuali verifiche, controlli o ispezioni, evadendo tempestivamente le richieste di informazioni da parte dell'Autorità Garante e dando immediata esecuzione alle eventuali indicazioni che pervengano dalla medesima Autorità;
- garantire agli interessati l'effettivo esercizio dei diritti previsti dal Capo III del GDPR, ovvero il diritto di accesso ai propri dati personali (origine, finalità, estremi identificativi del Titolare e Responsabile del trattamento, logica applicata per il trattamento con strumenti informatici), l'aggiornamento, l'integrazione, la cancellazione, la limitazione, la rettifica, la portabilità;
- non divulgare, diffondere, trasmettere e comunicare i dati/documenti informatici di proprietà del Titolare del trattamento nella piena consapevolezza che i dati/documenti rimarranno sempre e comunque di proprietà esclusiva dello stesso Titolare del trattamento e, pertanto, non potranno essere venduti o ceduti, in tutto o in parte, ad altri soggetti;
- informare e fornire consulenza al Titolare del trattamento, nonché ai dipendenti;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati;
- cooperare con l'Autorità di controllo;
- fungere da punto di contatto per l'Autorità di controllo, tra cui la consultazione preventiva.

4. Formazione/Aggiornamento del personale e diffusione del modello nel contesto aziendale

Il Titolare promuove la conoscenza della Policy, dei relativi protocolli interni e dei loro aggiornamenti tra tutti i dipendenti e collaboratori, che sono pertanto tenuti a conoscerne il contenuto, ad osservarli e contribuire alla loro attuazione.

Ai fini dell'attuazione della Policy, la formazione del personale sarà articolata sui livelli qui di seguito indicati:

- personale direttivo e con funzioni di rappresentanza dell'ente: informativa in sede di assunzione per i neoassunti; accesso all'intranet aziendale (Portale Zucchetti) con spazio dedicato all'argomento e aggiornato in collaborazione con l'Organismo di Vigilanza; occasionali e-mail di aggiornamento;
- altro personale: nota informativa interna; informativa in sede di assunzione per i neo assunti; accesso a portale Zucchetti; e-mail di aggiornamento.

Inoltre, la Società promuove la conoscenza e l'osservanza della Policy anche tra i partner commerciali e finanziari, i consulenti, i collaboratori a vario titolo, i clienti ed i fornitori. A questi verranno pertanto fornite apposite informative sui principi, le politiche e le procedure adottate sulla base della presente Policy, nonché i testi delle clausole contrattuali che, coerentemente a detti principi, politiche e procedure, verranno adottate dalla Società.

5. Utilizzo delle postazioni di lavoro:

Le postazioni di lavoro, siano esse fisse o portatili, sono dotate dei necessari dispositivi (hardware) e programmi (software) tali da consentirne il corretto funzionamento e la continuità operativa. L'installazione, la configurazione e l'aggiornamento dei suddetti strumenti sono di esclusiva competenza del personale specializzato ed espressamente incaricato dal Titolare.

Le informazioni (documenti, dati aziendali, dati personali, dati particolari etc.) a seconda del loro grado di importanza e riservatezza devono essere trattate (raccolta, elaborazione, cancellazione, modifica, comunicazione, diffusione, etc.) secondo le apposite indicazioni impartite dall'Azienda, dal Responsabile per il trattamento dei dati designato e secondo quanto previsto dal GDPR e dalla presente Policy.
Il Responsabile IT provvede periodicamente ad effettuare attività di salvataggio dei dati (backup) allo scopo di evitare la perdita degli stessi e garantirne un rapido ripristino.

A tale proposito si specifica che il backup è effettuato solo sulle cartelle in rete (folder shared) ed è cura dei dipendenti salvare le informazioni in queste cartelle.
L'ufficio IT ha la facoltà di collegarsi e visualizzare in remoto i contenuti delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza in caso di incidente.
L'intervento può essere effettuato su chiamata dell'utente o a seguito della rilevazione tecnica di pericoli di sicurezza che richiedono un intervento urgente.
Il personal computer deve essere spento al termine del turno o della giornata lavorativa, in caso di assenza prolungate dall'ufficio o in caso di suo inutilizzo. E' responsabilità dell'utilizzatore assicurarsi di non lasciare il proprio computer accessibile ed incustodito anche per brevi periodi.

Inoltre, è vietato:

- utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere o rendere inaccessibile il contenuto di comunicazioni e/o dati informatici;
- distruggere, deteriorare o rendere in tutto o in parte inservibili programmi, informazioni o dati aziendali;
- installare software non espressamente autorizzati;
- accedere, modificare, cancellare o fare copie per sé o per terzi (si considerano tali anche gli altri dipendenti) dei dati aziendali;
- accedere abusivamente (violando i sistemi di sicurezza) ad aree riservate del sistema informatico aziendale;
- salvare *file* personali sui supporti di memorizzazione della propria postazione di lavoro e della rete locale aziendale;
- installare e/o utilizzare qualsiasi tipo di programma che non sia espressamente autorizzato, o che non sia originale, anche per ragioni di lavoro, onde evitare il rischio di infezione di virus informatici e, pertanto, alterare la stabilità del sistema informatico aziendale. Si evidenzia come le violazioni delle norme sulla tutela dei diritti d'autore sul software che impongono l'uso di software correttamente licenziato, vengono sanzionate e possono comportare l'insorgere di responsabilità amministrative a carico di ManniGroup;
- modificare la configurazione del proprio pc aziendale, salvo espressa autorizzazione dell'azienda;

- copiare sui computer aziendali *file* di provenienza incerta o comunque esterna non attinenti alla propria attività lavorativa;
- disattivare, anche temporaneamente, il sistema antivirus e gli altri sistemi di sicurezza installati sui computer aziendali.

6. Disponibilità degli strumenti affidati al dipendente

In caso di assenza del dipendente, per motivi di urgente necessità, al fine di garantire al personale autorizzato l'accesso agli strumenti ed ai dati aziendali devono essere rispettate le seguenti modalità:

Casella di posta Aziendale:

- in caso di assenza del lavoratore il dirigente responsabile può autorizzare per iscritto un altro soggetto ad utilizzare la posta del dipendente assente, previa comunicazione al soggetto interessato. Al rientro dall'assenza il dipendente sarà tenuto a modificare la password al primo accesso;
- in caso di cessazione del rapporto di lavoro la password di accesso viene resettata e alla posta avrà accesso un responsabile per un periodo di tempo normato e definito; tale modalità viene consentita da un'autorizzazione firmata dal dipendente uscente. Contestualmente, nell'account di posta verrà configurato un messaggio fuori sede che indica un altro indirizzo aziendale a cui rivolgersi.

Accesso al computer:

- in caso di assenza solo il dirigente responsabile può autorizzare per iscritto un altro soggetto a sostituirsi alla persona assente e ad utilizzare la sua *user-id* ed il relativo profilo di accesso, previa comunicazione al soggetto interessato;
- al rientro dall'assenza, il lavoratore dovrà sostituire le credenziali di accesso, in modo da garantire la segretezza delle stesse.

7. Gestione delle password

Il sistema informatico di Manni Group S.p.A. prevede modalità di autenticazione e di accesso alle risorse informatiche/telematiche che rispettano i principi di unicità, incedibilità e segretezza stabiliti dalla legge. Pertanto, le informazioni riservate sono protette contro gli accessi da parte del personale non autorizzato e, la rete aziendale, è difesa da appropriate gestioni dei privilegi.

Quindi, è vietato:

- non utilizzare password di accesso al sistema, alla rete, ed ai programmi composte da lettere maiuscole e

minuscole, da numeri, caratteri speciali e simboli (Es. P4$$w0rd_AziEnd@le);

- astenersi dal cambio periodico delle password (ogni 3 mesi se vengono trattati dati particolari, ogni 6 mesi negli altri casi) secondo quanto stabilito e comunicato dal proprio Titolare e/o dal Responsabile;
- comunicare le proprie password a soggetti diversi dalla Direzione aziendale, dal Responsabile del trattamento dei dati, fatto salvo il caso di condivisione autorizzata di risorse hardware;
- nel momento in cui i lavoratori si assentano temporaneamente dalla postazione di lavoro, lasciare la sessione del computer "aperta" (bastano pochi minuti per trasferire e/o copiare dati riservati su un supporto esterno come ad es. CD, USB, etc.);
- appropriarsi, comunicare o diffondere password altrui.

8. Utilizzo della posta elettronica

La posta elettronica è un mezzo di comunicazione messo a disposizione del dipendente esclusivamente per consentirgli lo svolgimento della propria attività lavorativa. Gli utenti a cui è assegnata la casella/indirizzo di posta sono responsabili del corretto utilizzo della stessa.

Le principali raccomandazioni sull'uso della posta elettronica sono:

- va evitato l'invio o la ricezione di messaggi di posta elettronica con oggetto o contenuto estraneo all'attività lavorativa;
- evitare l'utilizzo di posta elettronica per motivi privati e/o per attività non inerente all'uso d'ufficio, nonché per l'adesione alle c.d. "catene di Sant'Antonio", per l'iscrizione a newsletter pubblicitarie e simili o comunque non attinenti con l'attività lavorativa;
- nel caso di ricezione di e-mail insolite o di messaggi provenienti da mittenti sconosciuti che contengono allegati sospetti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli;
- nel caso in cui si debba allegare un documento ad un messaggio inviato all'esterno della rete aziendale, è preferibile utilizzare un formato che consenta di proteggere da scrittura il documento stesso così da renderlo non editabile, es. pdf;
- pur essendo previsto dal sistema antivirus presente sul server di posta e sul PC il blocco di messaggi di posta elettronica contenenti allegati infetti da virus, con contestuale collocazione degli stessi in area di quarantena, potrebbe accadere che messaggi con allegati pericolosi o sospetti riescano a by-passare il suddetto sistema antivirus (ad esempio nell'ipotesi in cui il sistema non riconosca un virus appena creato e diffuso), occorre che l'utente proceda immediatamente all'eliminazione di tali messaggi, senza aprire o salvare per nessun motivo i *file* sospetti allegati.

CRYPTOLOCKER RANSOMWARE: Il *ransomware* è un programma informatico dannoso che infetta un dispositivo (PC, tablet, smartphone) bloccando l'accesso ai contenuti (foto, video, *file*) e chiedendo un riscatto (in inglese, ransom) per

"liberarli". Il suo obiettivo principale è quello di crittografare e rendere illeggibili i *file* presenti sull'hard disk dei dispositivi. Il ransomware (come i Virus o i Trojan) si diffonde soprattutto attraverso messaggi - inviati via e-mail, sms o chat o che appaiono su pagine web e social network - che sembrano provenire da soggetti conosciuti e sicuri. Difatti, chi li riceve è indotto ingannevolmente ad aprire allegati o a cliccare link/banner collegati a software dannosi. Si raccomanda, pertanto, di prestare molta attenzione ai messaggi ricevuti anche se possono sembrare innocui e/o spediti da un mittente di fiducia. Gli allegati e/o i link vanno sempre e comunque trattati con molta cautela: un innocuo *file* di testo potrebbe benissimo contenere un link ad un *file* eseguibile potenzialmente pericoloso per il proprio computer e per il sistema informatico aziendale. Nel caso di presunta infezione, contattare immediatamente il Titolare e/o il Responsabile.

9. Utilizzo di Internet

Internet è uno strumento utilizzato da miliardi di persone nel mondo. Queste non sempre hanno interessi e codici comportamentali adeguati alle politiche aziendali e, pertanto, bisogna prestare molta attenzione al trattamento dei dati e delle informazioni aziendali di cui persone malintenzionate o incaute potrebbero fare un uso improprio.

Il servizio di accesso ad Internet deve essere utilizzato rispettando le regole di comportamento sotto elencate, salvo i casi espressamente autorizzati dalle competenti strutture organizzative.

Al dipendente che accede ad Internet dalla propria postazione di lavoro si raccomanda:

- in caso di registrazioni sul web a servizi attinenti all'attività aziendale, bisogna fornire le proprie generalità lavorative esclusivamente quando si è autorizzati; in tal caso è possibile e consigliato richiedere specifica assistenza del referente informatico interno al fine di evitare l'invio di informazioni eccedenti e non pertinenti alla registrazione stessa;
- non installare sui computer aziendali software che potrebbero essere utilizzati per la fuga di dati, come quelli per la condivisione di *file peer-to-peer* (es. eMule e/o *BitTorrent)*; quelli di *cloud-storage* (DropBox, GoogleDrive, OneDrive) e sistemi di posta elettronica (Client di Posta, Webmail) possono essere utilizzati se autorizzati dall'azienda;
- non scaricare *files* e software su siti Internet, anche gratuiti, se non su espressa autorizzazione dell'azienda;
- non navigare in siti non pertinenti con lo svolgimento delle mansioni assegnate e, in particolare, è fatto assoluto divieto di accesso a siti che per il loro contenuto o tenore possano, secondo valutazioni in base alla diligenza media, comportare inosservanza o violazione di norme di legge.

In particolare non è consentito utilizzare l'accesso ad Internet per:

- scaricare fotografie o *file* multimediali in genere (Jpeg, MP3, AVI, MPEG e/o altri tipi di *file* o programmi per la fruizione di contenuto audio/video/immagini) non strettamente legati ad un uso d'ufficio;

- effettuare tentativi di intrusione sui sistemi interni della Società o di altri soggetti pubblici o privati, anche se non protetti da adeguati sistemi di sicurezza;
- effettuare operazioni o transazioni finanziarie tramite Internet, ivi comprese le operazioni di remote banking, acquisti via Internet e simili; qualora tali operazioni siano necessarie per lo svolgimento dell'attività lavorativa devono essere previamente autorizzate dalle competenti strutture organizzative ed essere eseguite nel rispetto delle normali procedure di acquisto;
- partecipare o iscriversi per motivi non professionali a Forum, chat, bacheche elettroniche, *guestbook*, *mail-list*, o effettuare l'attivazione di servizi RSS, anche utilizzando pseudonimi (nickname);
- effettuare streaming, download o upload da Internet di contenuti non necessari ai fini dell'espletamento delle proprie mansioni.

10. Utilizzo dei dispositivi mobili: Smartphone e Tablet

Oggi, i dispositivi mobili rappresentano un rischio significativo alla sicurezza di dati e informazioni; se non vengono implementate le corrette applicazioni e procedure di sicurezza, possono infatti diventare un vettore per l'accesso non autorizzato ai dati e alla struttura informatica dell'azienda. L'obiettivo è pertanto quello di evidenziare rischi, adempimenti formali e misure di protezione da tenere in considerazione nel trattamento di dati personali mediante tali dispositivi.

Pertanto, le regole per il corretto utilizzo dei dispositivi mobili aziendali come Tablet e Smartphone stabilite dal Titolare sono:

- ai dipendenti è consentito salvare sul o sui dispositivi mobili assegnati solamente i dati essenziali allo svolgimento del proprio lavoro;
- il dispositivo affidato al dipendente non può essere ceduto a colleghi e/o terzi;
- i dispositivi devono essere configurati con una password di accesso (PIN) e un codice di blocco schermo diversi dalle credenziali utilizzate all'interno dell'azienda;
- non è consentito connettere il dispositivo ad un PC o qualsiasi altro dispositivo privo di protezione antivirus aggiornata e non conforme ai criteri aziendali stabiliti;
- il Titolare e/o Responsabile IT della gestione degli strumenti informatici al fine di prevenire vulnerabilità e difetti può disporre dei dispositivi secondo necessità, sostituendo, aggiornando, rimuovendo o adeguando in tutto o in parte le componenti hardware e/o software di cui essi si compongono;
- non è consentita l'installazione di programmi e app diversi da quelli autorizzati e installati dall'azienda;
- il dipendente che abbia necessità di apportare modifiche software o hardware al dispositivo in dotazione, installando nuovi programmi o app, deve farne preventiva richiesta al Responsabile e/o al Titolare;
- in caso di malfunzionamento dei dispositivi o dei relativi accessori, il dipendente dovrà consegnare l'apparecchiatura completa al Responsabile IT (se presente) o al Titolare che provvederà alle dovute verifiche e fornirà, se necessario, un apparecchio sostitutivo;

- è proibito sottoporre i dispositivi a *jailbreak* (Apple) o *root* (Android), ossia a procedure che consentono di sbloccare l'accesso e/o modificare tutti i *file* del sistema operativo di un dispositivo mobile oltre a permettere l'installazione di applicazioni e pacchetti alternativi a quelli ufficiali rilasciati su AppStore e PlayStore;
- non è consentita la riproduzione, la duplicazione, il salvataggio o il download di programmi o *file* di ogni tipo (testo, immagini, video, audio, eseguibili) in violazione delle norme sul diritto d'autore;
- in caso di furto o smarrimento dei dispositivi, i dipendenti hanno l'obbligo di avvisare immediatamente il reparto IT aziendale;
- il dipendente ha l'obbligo di comunicare prontamente all'Azienda ogni sospetto attacco hacking e/o diffusione non autorizzata dei dati contenuti all'interno del dispositivo mobile;
- sui dispositivi verrà installato, a cura del reparto IT, un software di *remote wiping* che permette di cancellare i dati una volta che il dispositivo stesso dovesse cadere in mani sbagliate.

11. Utilizzo dei Social Network

I social network (Facebook, Twitter e altri) sono "piazze virtuali" ossia dei luoghi in cui, via Internet, ci si ritrova, portando con sé e condividendo, con altri: fotografie, filmati, pensieri, indirizzi di amici e tanto altro. Essi sono lo strumento di condivisione per eccellenza e rappresentano straordinarie forme di comunicazione, anche se comportano dei rischi per la sfera personale degli individui coinvolti. Oggi, lo sviluppo tecnologico spinge i social a integrarsi sempre più con i telefoni cellulari, trasformando le informazioni che pubblichiamo on-line in una sorta di messaggio multiplo, che giunge istantaneamente a tutti i nostri amici e non.

I social network sono strumenti che danno l'impressione di uno spazio personale, o di piccola comunità. Si tratta però di un falso senso di intimità, che può spingere gli utenti ad esporre troppo la propria vita privata e/o lavorativa, a rivelare informazioni strettamente personali, provocando di conseguenza "effetti collaterali", anche a distanza di anni, che non devono essere sottovalutati.

È bene precisare che, quando vengono inseriti dati personali su un social network, se ne perde il controllo. I dati possono essere copiati da tutti i propri contatti e dai componenti dei gruppi ai quali si aderisce, nonché rielaborati, diffusi, anche a distanza di anni. A volte, accettando di iscriversi ad un social network, si concede all'impresa, che gestisce il servizio, la licenza di usare senza limiti di tempo il materiale che viene inserito on-line: foto, messaggi, etc. Se si decide di eliminare il proprio profilo da un social network, spesso viene permesso solo di "disattivarlo" e non di "cancellarlo". I dati e i materiali inseriti on-line, potrebbero essere comunque conservati nei server o negli archivi informatici dell'azienda che offre il servizio. Il valore di queste imprese è strettamente legato anche alla loro capacità di analizzare in dettaglio il profilo, le abitudini e gli interessi dei propri utenti, per poi rivendere le informazioni a chi ne ha bisogno. In conclusione, il miglior difensore della propria privacy siamo noi. Meglio riflettere bene prima di inserire on-line dati che non si vogliono diffondere o che possano essere usati a proprio danno o a danno degli altri.

Il presente documento indica le principali norme di comportamento che i dipendenti e i collaboratori della Società sono invitati/tenuti ad osservare quando utilizzano i Social Network. Si raccomanda di:

- attenersi alle disposizioni del GDPR, nonché alla Policy sulla sicurezza informatica adottata da Manni Group S.p.A.;
- non effettuare registrazioni di profili utilizzando dati o marchi del Titolare o di altre aziende con cui si collabora, salvo i casi in cui si è autorizzati;
- considerare lo spazio virtuale del social network come spazio pubblico e non privato, in particolare per quanto riguarda il lavoro e le tematiche aziendali;
- qualora l'appartenenza alla Società sia desumibile dal profilo dell'utente o rilevabile dal contenuto di un intervento, è sempre necessario specificare che le opinioni espresse hanno carattere personale e non impegnano in alcun modo la responsabilità della Società;
- non divulgare attraverso i social network informazioni riservate, come informazioni interne, informazioni di terze parti (soggetti privati, altri dipendenti, altre società etc.) di cui si è a conoscenza, informazioni su attività lavorative, servizi, progetti e documenti non ancora resi pubblici;
- garantire la tutela della privacy delle persone; di conseguenza, si raccomanda di non comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori aziendali, se non con il preventivo e personale consenso di questi;
- evitare, salvo i casi in cui si è autorizzati, la divulgazione di foto, video, o altro materiale multimediale che ritragga locali, personale, bambini, genitori etc., senza l'esplicita autorizzazione delle persone coinvolte;
- astenersi dal porre in essere, nei confronti di terzi, verso la Società, i colleghi, i clienti ed i fornitori, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori, denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo nelle occasioni in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito aziendale;
- non pubblicare contenuti che violino il diritto d'autore e non utilizzare marchi registrati senza autorizzazione;
- segnalare ai propri responsabili eventuali contenuti presenti sui social network che possano danneggiare la privacy, la reputazione o l'immagine del Titolare;
- evitare di collegarsi e/o di "postare" messaggi, foto o altro materiale multimediale dai propri dispositivi privati (pc, tablet, smartphone, etc.) sui social network durante l'orario di lavoro.

12. Blocchi e filtri della navigazione Internet

In Manni Group S.p.A. ogni dispositivo che può accedere a Internet è protetta da un Antivirus e da un Firewall regolarmente aggiornati; infatti, è attivo un meccanismo di controllo e di blocco della navigazione in Internet che interviene attraverso l'esame di indirizzi di siti web (*url*) richiesti dall'utente, con l'esclusione di quelli che sono contenuti con meccanismi identici al punto precedente, in un elenco di "siti vietati" (*black-list*) il cui accesso è interdetto alla navigazione dall'interno dell'azienda.

13. Monitoraggio e verifiche

Per la tutela del proprio patrimonio informativo aziendale, per esigenze organizzative/produttive, per la sicurezza dal lavoro e, in ottemperanza a quanto previsto nel *Jobs Act* dal D.lgs. 151/2015 relativo al controllo a distanza dei lavoratori, al fine di garantire un corretto/lecito utilizzo degli strumenti informatici impiegati dal lavoratore per rendere la propria prestazione, i sistemi informatici del Titolare sono dotati di un software di *LOGGING* (sistema di memorizzazione di tutte le operazioni che sono considerate critiche per l'integrità del sistema informatico aziendale e di verifica dei tentativi di accesso al sistema stesso, autorizzati e non) e di *MONITORING* (monitoraggio) dei sistemi informatici aziendali nei limiti consentiti dalla legge. Infatti, essa si riserva la possibilità di condurre attività di verifica degli accessi e delle presenze, del traffico e-mail in entrata e in uscita dalle singole postazioni dei dipendenti e, sul traffico Internet.

Si sottolinea che tali verifiche, ove effettuate, sono finalizzate unicamente all'accertamento del corretto utilizzo e funzionamento dei dispositivi, della posta elettronica e dei servizi Internet aziendali.

L'accesso e l'analisi dei dati relativi al traffico e-mail ed Internet dei dipendenti è effettuato dal Responsabile di riferimento e/o dal Titolare che ha ricevuto espressa autorizzazione allo svolgimento di tale attività dal Responsabile del trattamento dei dati, dal dirigente responsabile.

I dati anonimi aggregati, riferibili all'intera struttura o a sue aree, sono a disposizione del Titolare per le valutazioni di competenza, e riguardano:

- per ciascun sito web visitato, le seguenti informazioni: il numero di utenti che lo visitano, il tempo totale di connessione, il numero delle relative pagine richieste e la quantità dei dati scaricati;
- per ciascuna stazione abilitata alla navigazione Internet, le seguenti informazioni: il numero di siti visitati, data e ora delle richieste, la quantità totale di dati scaricati.

L'identificazione dell'utente può avvenire attraverso l'incrocio di più informazioni contenute nei log e negli archivi del personale dipendente; tali dati personali, possono essere trattati in via eccezionale e tassativamente nelle seguenti ipotesi:

- se richiesti da organi di polizia su segnalazione dell'autorità giudiziaria;
- se richiesti dal Titolare, anche su segnalazione di un responsabile dell'area con personale assegnato, quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
- se richiesti dal Titolare, anche su segnalazione di un responsabile dell'area con personale assegnato, limitatamente al caso di utilizzo anomalo degli strumenti da parte di uno o più utenti di una specifica struttura organizzativa.

È opportuno precisare che, ai sensi della L. n. 48/2008 (Legge di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica dove sono state delineate definizioni comuni di reato informatico e previsti poteri comuni e di cooperazione nelle indagini) e del D.Lgs. n. 231 del 2001, l'azienda ed i propri dipendenti, sono responsabili per la commissione dei seguenti reati informatici:

- falsità in un documento informatico (art. 491-bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 615-quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.);
- frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.).

Per questo motivo, i dati contenuti nei *LOG* di sistema sono conservati dal Titolare per finalità organizzative e di sicurezza, solitamente per un periodo non superiore a 12 (dodici) mesi e, successivamente cancellati attraverso procedure automatiche.

I dati relativi alla navigazione Internet sono utilizzati per garantire la sicurezza del sistema, per verificare la presenza di eventuali abusi, per la ricerca di possibili errori, e/o per analisi di tipo statistico.

Come già precisato, si sottolinea, che tali dati non sono utilizzati per effettuare controlli diretti sull'attività lavorativa.

Nel caso in cui le attività di verifica rilevino abusi o comportamenti illeciti, saranno eseguiti test più approfonditi al fine di accertare eventuali responsabilità ed irrogare le relative sanzioni.

14. Sanzioni

E' fatto obbligo a tutto il personale di osservare le disposizioni della presente policy.

Il mancato rispetto o la violazione delle regole sopra riportate è perseguibile con provvedimenti disciplinari e risarcitori previsti dai vigenti CCNL, nonché con tutte le azioni civili e penali consentite.

L'azienda si riserva inoltre la facoltà di agire a propria tutela per ottenere il risarcimento di danni eventualmente provocati dal lavoratore con comportamenti non corretti e /o azioni penali in caso di attività dolose o colpa grave.

Infatti, il Decreto Legislativo n. 231 dell'8 giugno 2001, introducendo la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società", prevede che, qualora l'Azienda dovesse venir sanzionata sulla base di

comportamenti del dipendente difformi dalle regole contenute nel Modello di Organizzazione Gestione e Controllo e/o del Codice Etico, possa richiedere il risarcimento dei danni subiti.

Come previsto dall'art. 6, comma 2, lettera e) del Decreto Legislativo 231/2001, la predisposizione di un adeguato sistema sanzionatorio per la violazione delle prescrizioni contenute nella Policy, è condizione essenziale per assicurare l'effettività della Policy stessa.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dalla Policy sono assunte da Manni Group S.p.A. in piena autonomia e indipendentemente dalla tipologia di illecito che le violazioni del modello stesso possano determinare.

Verona, lì 08/02/2022

MANNI GROUP

ALLEGATO **GLOSSARIO DEI TERMINI INFORMATICI E/O TECNICI**

- **Account**: Iscrizione registrata su un server e che, tramite l'inserimento di una *user-Id* e di una password, consente l'accesso alla rete e/o ai servizi;
- **Adobe Acrobat**: programma per la creazione e lettura di documenti in formato PDF;
- **Alias**: attribuire un secondo nome, alternativo, ad una casella esistente appartenente o meno al dominio;
- **Antivirus**: è un software programmato per funzionare su un computer ed atto a prevenire, rilevare ed eventualmente rendere inoffensivi codici dannosi, noti anche come malware, fra i quali virus informatici, *adware, backdoor, BHO, dialer, fraudtool, hijacker, keylogger, LSP, rootkit, spyware, trojan, worm*;
- **Applicazione**: programma che viene eseguito su un computer con lo scopo e il risultato di rendere possibile una o più funzionalità, servizi o strumenti utili e selezionabili su richiesta dall'utente;
- **Attachment/allegato di posta elettronica**: *file* o documento di qualunque genere agganciato ad un messaggio di posta elettronica per essere inviato;
- **AVI**: (*Audio Video Interleaved*) formato per *file* video. I video AVI hanno un'ottima qualità di riproduzione, ma di dimensioni maggiori rispetto ad altri formati video;
- **Bacheca elettronica**: servizio Internet che permette di reperire annunci di vario genere come, ad esempio, annunci di lavoro e di compravendita;
- **Backup**: replicazione/copia, su un qualunque supporto di memorizzazione, di materiale informativo archiviato nella memoria dei computer;
- **Black-list**: è un *file* che può contenere nomi di indirizzi di posta elettronica o di siti web per i quali non viene permesso il traffico Internet;
- **Catena di sant'Antonio**: è un sistema per propagare un messaggio inducendo il destinatario a produrne copie da spedire, a propria volta, a nuovi destinatari;
- **Chat**: sistema di comunicazione interattiva in tempo reale tramite Internet;
- **Client**: software usato sul computer-client per accedere alle funzionalità offerte da un server;

- **Client di posta elettronica**: è un programma che consente di gestire la composizione e l'organizzazione di e-mail (o messaggi di posta elettronica) da parte dell'utente del servizio, nonché, la ricezione e la trasmissione da e verso un server di posta. I client standard utilizzati sono *Mozilla Thunderbird* e Outlook;
- **Cloud**: servizio di memorizzazione dati attraverso la rete Internet, normalmente accessibili con credenziali utente riservate;
- **Database**: "Base di Dati", è un aggregato di dati organizzato;
- **Download**: azione di ricevere o prelevare da una rete telematica (ad esempio da un sito web) un *file*, trasferendolo sul disco rigido del computer o su altra periferica dell'utente;
- **E-commerce**: sito Internet che consente l'acquisto di prodotti/servizi tramite transazioni informatiche;
- **Electronic-mail, posta elettronica**: scambio di messaggi e di *file* attraverso una rete locale o Internet;
- **Estensione di un *file***: è una breve stringa di caratteri alfanumerici aggiunti dopo il nome di un *file* e separati da quest'ultimo da un punto;
- **.exe**: estensione di un *file* che contiene un codice eseguibile, cioè un programma o un driver di dispositivo;
- **Feed-reader/RSS**: un *feed-reader* è un programma in grado di effettuare il download di un RSS (Really Simple Syndication, uno dei più popolari formati per la distribuzione di contenuti e informazioni web);
- ***File***: insieme di informazioni conservate su supporti di memorizzazione;
- **Firewall**: termine inglese che significa letteralmente muro taglia-fuoco, è un componente passivo di difesa perimetrale di una rete informatica che garantisce una protezione in termini di sicurezza informatica della rete stessa;
- **Forum**: insieme delle sezioni di discussione in una piattaforma informatica, o una singola sezione, oppure lo stesso software utilizzato per fornire questa struttura;
- **Guest-book**: servizio Internet che permette ai visitatori di un sito web di lasciare un commento;
- **Hardware**: in informatica si intende l'insieme dei componenti elettronici e meccanici che costituiscono un computer;
- **Indirizzo IP**: (*Internet-Protocol*) è un numero che identifica univocamente nell'ambito di una singola rete i dispositivi collegati alla rete stessa;
- **Internet**: sistema mondiale di reti interconnesse e basate su tecnologie comuni, al quale ogni rete o computer possono essere connessi stabilmente o attraverso collegamenti temporanei;
- **Intranet**: è una rete aziendale privata che utilizza il protocollo TCP/IP;
- **Jailbreaking**: attività effettuata su un dispositivo (generalmente contro le regole che ne determinano l'utilizzo), al fine di permettere un'estensione dei servizi IT disponibili;
- **Log**: registrazione sequenziale e cronologica delle operazioni effettuate, da un utente, un amministratore o automatizzate, man mano che vengono eseguite dal sistema o applicazione; il *file* o insieme di *file* su cui tali registrazioni sono memorizzate ed eventualmente accedute in fase di analisi dei dati, detto anche registro eventi;
- **Mailing list**: è un servizio/strumento offerto da una rete di computer verso vari utenti e, costituito da un sistema organizzato per la partecipazione di più persone ad una discussione asincrona o per la distribuzione di informazioni utili agli interessati/iscritti attraverso l'invio di email ad una lista di indirizzi di posta elettronica di utenti iscritti;
- **MP3**: è un algoritmo di compressione audio in grado di ridurre drasticamente la quantità di dati richiesti per memorizzare un suono, rimanendo comunque una riproduzione fedele del *file* originale non compresso;

- **MPEG**: (Motion Picture Experts Group): è un comitato che stabilisce gli standard digitali per *file* audio e video;
- **Network**: sistema (o rete) di computer collegati tra di loro per il trasferimento o la condivisione di dati, periferiche e programmi;
- **Password**: serie di caratteri alfanumerici che costituisce la parola d'ordine per accedere a un computer, a un programma, a una banca dati o a una rete;
- **.pdf**: (Portable Document Format) formato di *file* molto diffuso che consente di creare documenti protetti da modifiche;
- **Pen-drive**: dispositivo mobile di memorizzazione dati attraverso presa USB;
- **Quicktime**: programma utilizzato per la riproduzione dei filmati video/audio;
- **Remote banking**: servizi automatizzati che consentono ai clienti di collegarsi all'elaboratore della banca presso la quale intrattengono il rapporto di conto corrente. Il cliente può effettuare direttamente una serie di operazioni bancarie o ricevere informazioni in tempo reale;
- **RFC**: (*Request For Comment*) è un documento che riporta informazioni o specifiche riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico o, più nello specifico, di Internet;
- **Scheda di memoria SD**: dispositivi hardware rimovibili di piccole dimensioni che consentono di memorizzare informazioni, facilmente installabili/rimovibili dai sistemi (in particolare da smartphone o tablet);
- **Screensaver**: (salvaschermo) è un'applicazione per computer che provoca l'oscuramento dello schermo o la comparsa di un'animazione o di una serie di immagini in successione sullo stesso dopo un periodo programmato di inattività del mouse e della tastiera (non dell'elaboratore in sé), impostabile attraverso un timer. L'uso dei salvaschermi è considerato una delle misure di sicurezza per proteggere la propria postazione di lavoro;
  Server: è un componente o sottosistema informatico di elaborazione e gestione del traffico di informazioni che fornisce, a livello logico e fisico, un qualunque tipo di servizio ad altre componenti (tipicamente chiamate clients, cioè clienti) che ne fanno richiesta attraverso una rete di computer, all'interno di un sistema informatico o anche direttamente in locale su un computer;
- **Signature**: è un breve contenuto testuale o multimediale che, per scelta dell'utente, viene posto in coda a messaggi di posta elettronica o post su forum o newsgroup;
- **SIM (Subscriber Identity Module)**: particolare Smart card denominata UICC, ma nota informalmente come SIM card, che viene usata nel telefono cellulare per identificare il numero dell'abbonato;
- **Sistema Operativo**: (abbreviato in SO) è un insieme di componenti software che rende operativi apparati e dispositivi informatici;
- **Sito web**: è un insieme di pagine web correlate, ovvero una struttura ipertestuale di documenti che risiede su un server web;
- **Smartphone**: dispositivo che unisce funzionalità tipiche di un telefono cellulare a quelle di un computer e che, normalmente consente la navigazione Internet tramite rete mobile (3G e/o wi-fi);
- **Smartphone**: uno *smartphone* è un dispositivo portatile, alimentato a batteria, che coniuga le funzionalità di telefono cellulare con quelle di elaborazione e trasmissione dati tipiche del mondo dei personal computer;
- **Social-Network**: sito o programma che permette lo scambio di informazioni e contenuti multimediali tra utenti attraverso la rete Internet (es: *facebook, linkedin, instagram* ecc.);
- **Software**: programmi e procedure utilizzati per far eseguire al computer un determinato compito;

- **Stazione di lavoro**: anche chiamata postazione, è il personal computer utilizzato per accedere anche ai servizi internet e alla posta elettronica;
- **Tablet**: i *tablet* sono dispositivi assimilabili per componenti hardware e software agli *smartphone*, dai quali si distinguono per dimensioni dello schermo, possibile assenza del modulo telefonico, destinazione d'uso;
- **Url**: (Uniform Resource Locator) è una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in Internet, ad esempio una pagina web;
- **Usb**: porta standard di connessione dispositivi esterni ad un PC o altra apparecchiatura;
- **User-id**: identificativo univoco dell'utente, da utilizzare associato ad una password;
- **Virus**: programma pirata che si diffonde attraverso lo scambio di dischetti e le connessioni di rete, causa alterazioni di varia entità nel funzionamento dei computer;
- **Web**: (*World Wide Web*) è uno dei principali servizi di Internet che permette di navigare e usufruire di un insieme vastissimo di contenuti;
- **Wi-Fi**: connessione di un dispositivo ad una rete tramite onde radio (senza utilizzo di cavi di connessione);
- **Wikipedia**: servizio Internet che permette la consultazione di un'enciclopedia online, multilingue, a contenuto libero, redatta in modo collaborativo da volontari.