2024

Policy Sicurezza

OPRA ORGANISMO PARITETICO REGIONALE DELL'ARTIGIANATO

Pietro Storti

Data Protection Officer

09/12/2024

1. OGGETTO

Il presente documento (d'ora in poi "Policy") raccoglie la Policy aziendale e le Prescrizioni generali per il trattamento dei dati di ***Opra – Organismo Paritetico Regionale dell'Artigianato*** (di seguito anche ***Società***) al fine di regolamentare l'utilizzo delle proprie risorse informatiche, e non, da parte del personale dipendente e non dipendente comunque ad essa legato da un contratto di lavoro subordinato, di prestazione d'opera occasionale, di rapporti di collaborazione a progetto, di lavoro interinale, collaborazioni occasionali (di seguito anche ***Utenti***).

2. PREMESSA

Opra – Organismo Paritetico Regionale dell'Artigianato ha fra gli obiettivi principali per la sicurezza delle informazioni la sensibilizzazione e responsabilizzazione degli ***Utenti*** sulla necessità di avere un approccio corretto e globale alla sicurezza delle informazioni, evidenziando gli obblighi che ne derivano e, al contempo, le sanzioni disciplinari e normative in cui può incorrere in caso di violazione degli stessi.

Poiché la maggior parte del trattamento delle informazioni avviene per via informatica, la presente Policy ha come obiettivo principale definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione informatica – e sulla corretta gestione delle informazioni ad essa correlate – da parte degli ***Utenti***, al fine di tutelare la ***Società*** ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre la stessa a problematiche di sicurezza, di immagine, patrimoniali e per eventuali danni cagionati anche a terzi.

Verranno tuttavia descritte e trattate, con le stesse finalità, anche le modalità di corretta gestione e trattamento di informazioni veicolate anche su altri supporti, ad esempio cartacei.

La legislazione italiana prevede sanzioni per le imprese che non vigilino sull'osservanza di modelli organizzativi volti a prevenire la commissione di specifici reati nell'interesse della ***Società*** (D. Lgs. 231/01) ed impone alla stessa di controllare il corretto impiego degli strumenti aziendali per la propria attività e di dettare le disposizioni per il corretto utilizzo degli stessi, di cui essa assume le responsabilità nei confronti degli ***Utenti*** nonché nei confronti dei terzi.

In particolare, il Regolamento Europeo 2016/679 "Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" (d'ora in poi "**Regolamento**") introduce rilevanti obblighi a carico della ***Società*** sanzionati civilmente e penalmente, imponendo di trattare i dati personali rispettando il diritto di riservatezza degli interessati, prescrivendo un trattamento lecito e corretto.

La presente Policy si pone l'obiettivo di creare una "best practice" (buona pratica) nelle relazioni di lavoro/collaborazione improntate alla trasparenza, all'accordo e all'uniformità dei comportamenti.

Essa intende, pertanto, garantire la ***Società***, la quale ha diritto di richiedere una corretta esecuzione della prestazione da parte degli ***Utenti***; ma anche gli ***Utenti*** che vengono, in tal modo, resi edotti della politica aziendale in materia di utilizzo di risorse informatiche e non.

L'insieme delle norme comportamentali incluse nella presente Policy è volto a conformare ***Opra – Organismo Paritetico Regionale dell'Artigianato*** ai principi di diligenza, informazione e correttezza nell'ambito di rapporti di lavoro e collaborazione, con l'ulteriore finalità di prevenire

eventuali comportamenti illeciti degli ***Utenti***, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano.

La presente Policy intende regolamentare l'esercizio del potere di controllo, direttivo e disciplinare della ***Società*** nei confronti degli ***Utenti*** al solo ed esclusivo scopo di tutela della ***Società***.

Opra – Organismo Paritetico Regionale dell'Artigianato garantisce, pertanto, che gli eventuali controlli ivi previsti escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e che non intende adottare apparecchiature per finalità di controllo a distanza degli ***Utenti***, effettuare indagini ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali degli ***Utenti***, nonché su fatti rilevanti ai fini della valutazione dell'attitudine professionale degli stessi; violare la disciplina sulla tutela dei dati personali; violare la normativa sulla tutela della corrispondenza privata.

3. RESPONSABILITA'

Il ruolo di Amministratore di Sistema, responsabile della sicurezza informatica della ***Società*** (nel seguito ***IT Manager***) è affidato ad un professionista esterno.

4. ACCETTAZIONE DELLA POLICY

Ogni Utente del trattamento di dati personali e comunque ogni utente dei Sistemi Informatici di ***Opra – Organismo Paritetico Regionale dell'Artigianato*** deve attenersi alle prescrizioni contenute nel presente documento.

Una copia della presente Policy è visionabile da ogni interessato presso gli uffici della ***Società***. La *Società* si riserva la possibilità di un invio diretto della presente Polizza ad ogni singolo ***Utente*** o alla pubblicazione della stessa sul proprio sito internet. La presente Policy verrà comunque esplicata e analizzata nel dettaglio a favore di tutti gli ***Utenti*** dal D.P.O. (Data Protection Officer) durante i corsi di aggiornamento.

L'inosservanza delle regole di comportamento contenute nella presente Policy configura per gli ***Utenti*** (sia dipendenti che non dipendenti) altrettanti illeciti disciplinari la cui previsione integra il codice disciplinare vigente ed i contratti di collaborazione in corso.

5. GENERALE

a) Titolarità dei beni e delle risorse informatiche

I beni e le risorse informatiche, i servizi informatici e le reti informative costituiscono beni aziendali rientranti nel patrimonio sociale e sono da considerarsi di esclusiva proprietà della ***Opra – Organismo Paritetico Regionale dell'Artigianato***.

Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni lavorative affidate ad ogni ***Utente*** in base al rapporto in essere (ovvero per scopi professionali) afferenti alle attività svolte a favore di ***Opra – Organismo Paritetico Regionale dell'Artigianato***), e comunque per l'esclusivo perseguimento degli obiettivi aziendali.

Ogni ***Utente*** è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dalla ***Opra – Organismo Paritetico Regionale dell'Artigianato*** nonché dei relativi dati trattati per finalità aziendali.

A tal fine ogni ***Utente***, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con ***Opra – Organismo Paritetico Regionale dell'Artigianato***, è tenuto a tutelare (per quanto di propria competenza) il patrimonio aziendale da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse aziendali.

Ogni ***Utente***, pertanto, è tenuto, in relazione al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica aziendale, riportando all' IT Manager per il tramite della ***Società***, e senza ritardo, eventuali rischi di cui è a conoscenza ovvero violazioni della presente Policy.

Sono vietati comportamenti che possano creare un danno, anche d' immagine, alla ***Società***.

b) Regole generali di comportamento dell'Utente

È dovere di ogni ***Utente*** uniformarsi ai principi descritti nella presente Policy. In particolare, è obbligo di tutti gli ***Utenti***:

- Usare i device a lui affidati responsabilmente e professionalmente.
- Tenere sotto controllo l'accesso fisico ai device e consentire l'accesso agli ambienti ove si trovano i sistemi informativi o le periferiche, solo alle persone autorizzate.
- Adottare ed applicare puntualmente la politica "schermo pulito e scrivania pulita", ovvero non portare sullo schermo o sulla scrivania informazioni non necessarie allo svolgimento delle attività in corso, e riporre in luogo sicuro le informazioni una volta terminata l'attività.
- Disabilitare la messaggistica 'pop up' nel caso di esame congiunto di documenti o condivisione dello schermo con terzi.
- Orientare gli schermi dei device in maniera che essi non possano essere osservati da persone non autorizzate.
- Asportare tutti i fogli stampati e togliere l'originale messo in una fotocopiatrice.
- Al termine del trattamento o se si sta per lasciare la postazione di lavoro, chiudere sempre i programmi secondo le appropriate procedure di sicurezza.
- Cifrare le informazioni riservate eventualmente memorizzate su chiavette USB o altri supporti.
- Se ci si accorge di aver accesso a dati e programmi di trattamento non di competenza esclusiva, informare subito la ***Società*** che ne farà verifica tramite ***l'IT Manager***.
- Sospendere ogni attività in caso di minacce virus o altri malfunzionamenti, segnalando prontamente l'accaduto alla ***Società*** che ne farà verifica tramite l'***IT Manager***.
- Segnalare con la massima tempestività alla ***Società*** eventuali guasti tecnici, problematiche tecniche o il cattivo funzionamento delle apparecchiature.
- Proteggere sempre i device da condizioni climatiche avverse.

In particolare, è esplicitamente vietato:

- Permettere l'accesso logico ai device e/o ad informazioni riservate a persone non autorizzate.

- Lasciare, al termine dell'utilizzo, carichi buffer eventualmente ritenuti in memorie di stampanti, di fax computerizzati ed altri terminali e dispositivi informatici.
- Modificare la configurazione hardware e software del proprio device, se non previa esplicita autorizzazione della ***Società***, che la eseguirà per mezzo dell'***IT Manager***.
- Rimuovere, danneggiare o asportare componenti hardware dai device.
- Installare autonomamente programmi informatici, software ed ogni altro applicativo non autorizzato espressamente dalla ***Società***.
- Utilizzare CD/DVD o chiavette USB con dati e programmi di provenienza ignota, onde evitare infezioni da virus nei device e danneggiare i dati.
- Lasciare incustodite le postazioni di lavoro con le sessioni utenti attive e/o con dati personali visualizzati sullo schermo. In caso di temporaneo allontanamento dalla postazione di lavoro, l'***Utente*** deve bloccare la stazione con un programma salvaschermo (screensaver) protetto da password o effettuare il log-out dalla sessione.
- Cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi.
- Lasciare incustoditi dispositivi mobili di lavoro in caso di trasporto, spostamento (es. nell'auto parcheggiata, in treno, ecc..) o utilizzo in zone non protette.

Ogni volta che l' ***Utente*** cambierà mansione o profilo di accesso ai dati dovrà prendere contatto con la ***Società*** che contatterà l' ***IT Manager*** per la costruzione di un nuovo idoneo profilo di autorizzazione.

c) Accessi "esclusivi" ma non "personali"

Ad ogni ***Utente***, autorizzato al trattamento dei dati, viene fornito una username (a volte con riferimento al nome e cognome dell'utente) per l'accesso alla rete aziendale che è abilitato anche alla navigazione su internet.

Può, inoltre, venir fornita una casella di posta aziendale (anche in questo caso con possibili riferimenti al nome e cognome o al ruolo dell' ***Utente***).

L'uso del nome e del cognome come indirizzo di posta è solo una semplificazione rispetto all'uso di un indirizzo esplicitamente riferito alla funzione aziendale ricoperta dall' ***Utente***.

L'uso del nome e del cognome come username per l'accesso alle risorse informatiche aziendali non autorizza ad un uso privato delle stesse ma all'uso per le funzioni aziendali ricoperte dall' ***Utente***. Allo stesso è quindi fatto espresso divieto di utilizzo delle risorse informatiche per scopi personali.

Se l' ***Utente*** lo desidera è suo diritto chiedere di non utilizzare lo standard aziendale ed avere per la casella di posta un indirizzo che non sia riferibile al proprio nome e cognome.

All' ***Utente*** è fatto espresso divieto di utilizzo delle risorse informatiche per scopi personali.

Per contro, non devono essere utilizzate e-mail personali per la registrazione a servizi esterni offerti da terze parti.

L'assegnazione di un accesso alla rete aziendale e di una casella di posta ad "uso esclusivo" non deve essere confusa con la possibilità di "uso personale".

d) Proprietà e controllo del corretto utilizzo delle strutture aziendali

Compete alla ***Società*** assicurare la funzionalità e il corretto impiego delle strutture aziendali da parte degli ***Utenti***, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo pur conto della disciplina in tema di diritti e relazioni sindacali. È inoltre necessario adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità.

La ***Società*** è pertanto tenuta a controllare il corretto impiego degli strumenti per le finalità aziendali ed a dettare le disposizioni per il corretto utilizzo degli stessi, di cui la ***Società*** assume la piena responsabilità nei confronti degli ***Utenti***.

In caso di guasti o malfunzionamenti delle apparecchiature elettroniche i responsabili delle società (esterne) addetti alla manutenzione, opportunamente nominati Responsabili, possono accedere a tutte le informazioni contenute nei dischi dei device, su tutte le cartelle personali e di gruppo memorizzate sul server e al contenuto della posta.

In caso di assenza imprevista e prolungata dell' ***Utente***, una risorsa assegnata ad esso potrebbe dover essere resa disponibile ad altri ***Utenti*** o a società esterne.

Tutti questi controlli ed attività, qualora gli ***Utenti*** non si limitino ad un uso strettamente aziendale degli strumenti informatici, potrebbero rilevare dati "particolari" (ex sensibili) protetti dal Regolamento rendendo impossibile eseguire i controlli stessi.

Per consentire di compiere senza problemi questi controlli e queste attività è proibito un uso personale degli strumenti informatici, dell'accesso ad internet e della posta elettronica messi a disposizione dalla ***Società***. Nessun dato personale (se non quelli strettamente legati all'attività lavorativa) deve essere presente sulle risorse informatiche aziendali neppure provvisoriamente.

Le mail ed i log di navigazione e tutti i documenti relativi alle dotazioni aziendali (es. fatture telepass, bollette cellulari, ecc.) degli ***Utenti*** potrebbero essere lette dal datore di lavoro nell'ambito e per necessità legate all'attività lavorativa potendo così rilevare dati personali dello stesso. Anche per evitare questo rischio è espressamente vietato l'utilizzo delle dotazioni aziendali (quali, ad esempio, notebook, tablet, cellulari/SIM, telepass, auto, mail, rete internet) per scopi privati.

La restrizione nell'utilizzo delle risorse informatiche aziendali è finalizzata a mettere in atto misure tecniche ed organizzative per garantire un livello di sicurezza adeguato così come prescritte dal Regolamento.

e) Utilizzo delle risorse informatiche aziendali

Tutto quanto compone la dotazione delle risorse informatiche, l'accesso ad internet e la casella di posta elettronica con dominio aziendale appartengono al patrimonio aziendale.

Gli ***Utenti*** utilizzano le risorse informatiche e quanto sopra solo ed esclusivamente per fini professionali per il perseguimento degli obiettivi fissati dalla ***Società*** e quant'altro sia dalla stessa espressamente autorizzato.

Gli ***Utenti*** sono tenuti ad un uso corretto delle risorse ed attrezzature messe a loro disposizione per l'esecuzione dell'attività lavorativa. Essi rispondono dei danni

eventualmente occorsi sia durante l'esecuzione della prestazione lavorativa sia al di fuori della medesima, fintanto che risorse e attrezzature rientrino nella loro disponibilità.

In particolare, si ricorda la finalità esclusivamente aziendale dell'uso degli strumenti informatici e il divieto di utilizzo degli stessi da parte di persone esterne alla ***Società***.

L'utilizzo delle apparecchiature informatiche dovrà avvenire in conformità alle prescrizioni previste dalla presente Policy.

La prescrizione riguarda l'intera attrezzatura messa a disposizione degli ***Utenti*** per lo svolgimento dell'attività lavorativa (ad esempio: smartphone, tablet) e quant'altro possa servire.

Agli ***Utenti*** è fatto, altresì, espresso divieto di:

- modificare le configurazioni impostate sul proprio device;
- installare o utilizzare programmi non distribuiti ufficialmente;
- scaricare file contenuti in supporti magnetici od ottici che non abbiano diretta attinenza con la prestazione lavorativa;
- navigare in siti non strettamente attinenti allo svolgimento della prestazione lavorativa, con particolare riferimento a quelli che possano rivelare le preferenze ed opinioni politiche, religiose, sessuali, o sindacali del dipendente.

6. CLASSIFICAZIONE DELLE INFORMAZIONI

a) Dati Personali

Viene definito "Dato personale" qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

I dati personali possono essere:

- Dati identificativi – I dati personali che permettono l'identificazione diretta dell'interessato (sono classificati come Riservati).
- Dati particolari (o ex-sensibili) – Sono i dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (sono classificati come confidenziali).

In particolare, fra i dati particolari (o ex-sensibili), possiamo avere:

- «dati genetici»: sono i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

- «dati biometrici»: sono i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
- «dati relativi alla salute»: sono i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Il Regolamento Europeo prevede che il trattamento sia regolato dai principi previsti dall'Articolo 5 (trattati in modo lecito, raccolti per finalità determinate, limitati a quanto necessario, esatti, conservati in funzione delle necessità) e comunque sia ridotto al minimo l'utilizzazione di dati personali, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Il trattamento di dati personali è ammesso quando ricorrono alcune condizioni specifiche (es. quando necessario all'esecuzione di un contratto, per adempiere ad obblighi legali, per la salvaguardia degli interessi vitali, per il perseguimento del legittimo interesse della Società o di terzi) o, altrimenti, solo con il consenso espresso dell'interessato che deve essere esplicito per ogni specifica finalità per quelli particolari.

b) Dati Aziendali

Ai fini aziendali ogni informazione, compresi i dati personali trattati, può essere classificata come:

- CONFIDENZIALE – il Livello di classificazione "Confidenziale" si applica alle informazioni la cui diffusione potrebbe causare serio danno alla Società, comportando conseguenze economiche e legali significative e danneggiando seriamente la reputazione della Società, delle società ad essa collegate o delle partecipate, con notevoli impatti su beni e asset aziendali. In genere solo un ristretto numero di persone, debitamente autorizzate, può accedere a queste informazioni.
- RISERVATA – il Livello di classificazione "Riservata" si applica alle informazioni il cui utilizzo è limitato a un gruppo di persone, come ad esempio un Ufficio. In genere le informazioni classificate Riservate sono considerate importanti ai fini della sicurezza aziendale, da un punto di vista gestionale, finanziario ed organizzativo, o per l'elevato contenuto tecnologico. La perdita, anche accidentale, di tali informazioni può causare un danno grave alla Società. La conoscenza di tali informazioni può costituire rilevante valore per la concorrenza. Le informazioni soggette a norme di sicurezza di programmi / progetti specifici o a normative di legge nazionali/internazionali (come ad esempio i dati personali soggetti al GDPR) rientrano nella classificazione "Riservata".
- INTERNA – il Livello di classificazione "Interna" si applica alle informazioni il cui utilizzo è limitato ai dipendenti della Società e al personale di società esterne che svolgono lavori in appalto o in outsourcing o attività di consulenza per la Società. Questo livello di classifica si applica a quelle informazioni la cui compromissione potrebbe causare un danno lieve per la Società. In genere tali informazioni sono accessibili anche ai partner commerciali o industriali.
- PUBBLICA – il Livello di classificazione "Pubblica" si applica alle informazioni il cui utilizzo non può causare alcun danno alla Società. Tali informazioni possono essere considerate di pubblico dominio, essendo generalmente accessibili o disponibili al pubblico.

Le informazioni che potrebbero essere pubblicate sul sito internet della Società, ad esempio, rientrano all'interno di tale categoria.

c) Misure di sicurezza

Ogni ***Utente*** è tenuto ad osservare in via generale le idonee misure di sicurezza volte a prevenire i rischi di distruzione o perdita, anche accidentale, dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

d) Responsabilità degli *Utenti*

Nei confronti dell' ***Utente*** che ha commesso una violazione della sicurezza delle informazioni verranno applicate le sanzioni disciplinari previste, per i lavoratori, dal contratto di lavoro e, per i collaboratori, da penali contrattuali.

La sanzione sarà proporzionale alla:

- Consapevolezza, in funzione del ruolo e della formazione ricevuta, dell'importanza delle informazioni oggetto della violazione relativamente a riservatezza, disponibilità ed integrità.
- Gravità delle operazioni che hanno portato alla violazione (operazioni svolte anche se espressamente proibite, mancanza delle comunicazioni previste, ripetitività dell'operazione errata, ecc.).

e) Segnalazioni all'Autorità Giudiziaria

Ogni utilizzo delle risorse informatiche aziendali da parte degli ***Utenti*** tale da comportare una responsabilità anche penale della ***Società*** verrà tempestivamente segnalato dalla stessa all'Autorità Giudiziaria senza che a tal fine sia necessaria una preventiva contestazione d'addebito all' ***Utente*** responsabile.

7. INCARICO PER IL TRATTAMENTO DEI DATI

Il Regolamento disciplina la gestione dei dati personali ed impone che all'interno di ogni realtà aziendale sia costituita una gerarchia, comprendente le figure del titolare, di eventuali referenti privacy e degli Utenti, funzionale alla sua applicazione. Tale gerarchia non comporta alcuna modifica della qualifica professionale o delle mansioni assegnate.

Ogni singolo ***Utente*** (visto che nello svolgimento delle proprie funzioni viene necessariamente a conoscenza dei contenuti delle banche dati) è autorizzato al trattamento di dati personali nell'ambito delle mansioni ad esso assegnate. Le banche dati cui potrà accedere per il trattamento – previa abilitazione ed indicazione delle modalità di utilizzo – sono unicamente quelle previste per la mansione d'appartenenza.

Per trattamento di dati deve intendersi: "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

L’accesso è in ogni caso consentito ai soli dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati. Pertanto, nella gestione dei dati dovrà osservare scrupolosamente le istruzioni impartite.

Qualora all’ ***Utente*** sia affidata la responsabilità di una apparecchiatura o di un’area di memorizzazione, sarà sua cura definire le regole di controllo di accesso, diritti di accesso e limitazioni per i ruoli specifici.

a) Riservatezza

L’ ***Utente*** si impegna alla riservatezza e a non divulgare a terzi, estranei alla ***Società***, dati e informazioni di cui venga a conoscenza per motivi di lavoro.

L’ ***Utente*** è responsabile dell’uso non corretto di tali dati e informazioni.

Nessun dato può essere trasmesso all’esterno in qualunque forma, sia come comunicazione che come diffusione, se non previa autorizzazione della ***Società***.

In caso di affidamento di documenti contenenti dati riservati o critici, sarà cura dell’ ***Utente*** controllarli e custodirli fino alla restituzione, in modo che ad essi non accedano soggetti privi di autorizzazione, e restituirli al termine delle operazioni affidate.

8. ACCESSO ALLA RETE AZIENDALE

a) Configurazione dispositivi ad uso esclusivo

La rete locale offre la possibilità di accesso ad Internet e la possibilità di utilizzare tutte le periferiche ad essa associate.

Solo i device appositamente configurati in dominio o in remoto possono però essere collegati alla rete. In particolare, non possono essere connessi alla rete i device configurati per altre reti o device personali senza l’autorizzazione della ***Società***.

Non è consentito all’ ***Utente*** modificare le caratteristiche dei dispositivi ad uso esclusivo senza la preventiva autorizzazione della ***Società***. In particolare, è proibito installare dispositivi di memorizzazione e di comunicazione o software.

È proibito attivare la password all’accensione del device (BIOS) da parte dei singoli *Utenti* senza la preventiva autorizzazione della *Società*.

b) Password

La password è lo strumento che consente di limitare l’accesso ai dati da parte di persone diverse da quelle espressamente autorizzate. È quindi indispensabile che sia elemento certo di identificazione per proteggersi contro accessi indesiderati.

La segretezza della password è infatti l’unico scoglio reale tra un attaccante e l’identità digitale della vittima (il nome utente è infatti tipicamente un’informazione pubblica o facilmente identificabile). Una corretta gestione delle password è quindi indispensabile per garantire la sicurezza dei sistemi aziendali e delle informazioni che questi contengono.

Il primo aspetto da tenere in considerazione è relativo alla corretta definizione delle password che devono essere di una complessità adeguata. Le recenti best practices suggeriscono di scegliere password:

- lunghe più di 8 caratteri;
- con almeno un numero e un carattere non alfanumerico;
- che non contengano:
    - termini noti del vocabolario, informazioni facilmente riconducibili all'utente (nomi di familiari, animali domestici, date di anniversari e qualunque informazione possa essere facilmente trovata sui social network);
    - semplici composizioni quali ad esempio "qwerty123 o Password123";
    - caratteri sequenziali ripetuti (ad esempio 1111, aaaa, ecc.);
    - cifre in progressivo ordine crescente o decrescente;
    - Caratteri speciali ($! ?) sempre e solo alla fine della sequenza.

L'uso di password complesse protegge l' ***Utente*** visto che renderebbe molto laborioso per l'attaccante cercare di identificare le password provando tutte le combinazioni possibili (il cosiddetto "attacco a forza bruta"). Al tempo stesso la password non deve essere troppo difficile da ricordarsi tale da doverla scrivere.

È responsabilità di ogni ***Utente*** provvedere a modificare la password fornita dall' ***IT Manager*** al primo accesso.

La password dovrà quindi essere modificata periodicamente (sei mesi per il trattamento di dati comuni e/o ogni tre mesi nel caso di trattamento di dati personali particolari) senza mai riutilizzare le vecchie per evitare che attraverso tentativi possa essere identificata da elementi esterni malintenzionati (procedura che dovrebbe essere imposta obbligatoriamente dal sistema ad ogni ***Utente***).

Non dovrà essere usata come password per i sistemi aziendali, una password utilizzata per servizi personali, per evitare che la compromissione di un'utenza su un servizio personale permetta ad un attaccante di accedere a un servizio aziendale.

Sarà responsabilità dell' ***Utente*** mantenere la massima riservatezza sulla propria password (non andrà comunicata ad altri o scritta in chiaro).

La password associata alla usermane dovrà essere nota al solo ***Utente*** poiché garantirà l'associazione solo ad esso delle attività svolte con quell'username che potranno essere registrate in vari archivi e contestate all' ***Utente*** in caso di violazione di norme aziendali (es. comunicazioni all'esterno di informazioni riservate) o segnalate all'Autorità Giudiziaria in caso di responsabilità penali (es. navigazione su siti pedo-pornografici).

L'*IT Manager* potrà modificare la password per poter recuperare le informazioni in caso di assenza dell' ***Utente*** ed al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale.

L' ***Utente***, al primo tentativo di accesso alla rete, si accorgerà della modifica e dovrà richiedere alla ***Società***, tramite l'***IT Manager***, la nuova password (che poi dovrà immediatamente modificare).

c) Salva schermo (Screen Saver)

Ogni device deve essere spento prima di lasciare la postazione lavoro o in caso di assenza prolungata dalla postazione. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. È responsabilità di ogni ***Utente*** non lasciare in nessuna occasione incustodito ed accessibile il device in uso durante una sessione di trattamento dati. A tal fine è necessario utilizzare lo Screen Saver abilitando la richiesta della propria password dopo una inattività di alcuni minuti.

9. CRITERI PER INTERNET

a) Generalità

Internet è uno strumento messo a disposizione degli ***Utenti*** per uso professionale. Ciascun ***Utente***, pertanto, deve usare la rete Internet in maniera appropriata.

La quantità di informazioni che possono essere trasmesse tramite il canale di comunicazione con Internet dovrà essere, ovviamente, limitata. Poiché tramite questo canale "passano" tutte le comunicazioni di posta elettronica, tutti gli accessi diretti ad internet e i collegamenti virtuali è necessario non "sprecare" questo canale di comunicazione per usi non lavorativi.

Colui che si connette ad internet deve verificare la veridicità e la sicurezza dei siti che intende visitare e in caso di dubbi o sospetti deve immediatamente abbandonare la connessione al sito e comunicare, tramite la ***Società***, l'evento all' ***IT Manager***.

Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:

- L'utilizzo è consentito esclusivamente per scopi aziendali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative.
- È fatto divieto comunicare su canali aperti (protocolli non criptati e siti non conosciuti) qualsiasi informazioni riservata.
- È fatto divieto di scaricare software gratuiti (freeware) e shareware prelevati da siti Internet, se non espressamente autorizzato dalla ***Società***.
- Non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi espressamente autorizzati dalla ***Società***.
- È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa, salvo quando ciò sia necessario per le specifiche competenze del reparto di appartenenza e previa autorizzazione della ***Società***.
- Non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in guest-book (sistema di registrazione che consente ai visitatori di un sito Web di lasciare un commento pubblico senza creare uno specifico account), anche utilizzando pseudonimi (o nicknames).
- Non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
- È consentito l'utilizzo di soluzioni di Instant Messaging e/o chat esclusivamente per scopi professionali ed attraverso gli strumenti ed i software messi a disposizione o indicati dalla ***Società***.

- Non è consentito l'utilizzo di sistemi di social networking durante l'attività lavorativa.
- Non è consentito lo scambio e/o la condivisione (es. sistemi di Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, etc., protetto da copyright.
- Non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà della ***Società*** in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata approvata espressamente.
- Non è consentito lo screenshot di pagine relative alla piattaforma utilizzata e/o comunque inerenti all'attività lavorativa.

È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere nociva all'immagine della *Società*.

b) Uso della rete internet

Il device abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.

L'utilizzo di Internet da parte degli ***Utenti*** potrebbe formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni.

Per evitare che questa attività possa ledere i diritti alla privacy dell' ***Utente***:

- È proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
- È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
- È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in siti anche utilizzando pseudonimi.

c) Prevenzione dell'accesso a determinati siti

Nella prospettiva della prevenzione di cui al presente documento, la ***Società*** si riserva la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti ivi non consentiti (con esclusione dei siti istituzionali) e che prevengono operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di file o software).

L'intervento sulle strutture aziendali con modalità automatiche di filtro e inibizione non comporta un controllo diretto o indiretto sulla posizione individuale, ma semplicemente può impedire l'accesso a determinati siti non funzionali all'attività aziendale, può impedire il downloading di materiale, funge da filtro per il virus detecting, impedisce l'invio o la ricezione di mail contenenti determinate parole (a sfondo sessuale o razzista) o di determinate dimensioni.

d) Internet ed infezioni da virus

Internet è il principale canale di contaminazione.

Per nessun motivo gli utenti devono scaricare programmi senza l'autorizzazione della ***Società***.

A volte viene richiesto di scaricare programmi al fine di poter visionare immagini. Anche in questo caso è necessario prima consultare la ***Società***.

e) Accessi alternativi ad internet

È proibito a tutti gli ***Utenti*** collegati ad una rete locale connettersi ad internet con modalità differenti da quelle previste (ad esempio con collegamenti a cellulari non aziendali o con appositi apparati USB) per evitare che, inconsapevolmente, si aprono falle nel sistema di sicurezza evitando i controlli previsti.

10. CRITERI PER LA POSTA ELETTRONICA

a) Generalità

Data l'importanza dell'e-mail per la normale conduzione del lavoro (consente comunicazioni asincrone e multiple ed inoltre lascia una traccia scritta), è essenziale un corretto utilizzo di questa risorsa, per ridurre eventuali rischi di carattere intenzionale o involontario e per assicurare la corretta gestione delle registrazioni ufficiali.

Se la posta elettronica contiene dati personali ed eventualmente sensibili relativi agli ***Utenti*** stessi o terzi identificati o identificabili, può violare la privacy, dato che i messaggi sono suscettibili (anche attraverso la tenuta di log file di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza del contenuto della corrispondenza.

Per evitare di violare la privacy degli *Utenti* è quindi necessario che essi si limitino ad un uso strettamente aziendale della posta elettronica.

Inviare una mail da un indirizzo con dominio aziendale corrisponde a scrivere sulla carta intestata aziendale e comporta la responsabilità della ***Società*** nei confronti dei terzi per tutto quanto è contenuto nella medesima. È quindi proibito un uso a fini privati anche delle caselle con indirizzo aziendale che, anche se contengono riferimenti al nome e cognome del lavoratore che non devono essere confuse con le caselle personali del tipo nome.cognome@gmail.com.

Gli ***Utenti*** non possono essere e non sono titolari di un diritto all'uso esclusivo della posta elettronica con dominio aziendale.

In caso di assenza dell'***Utente*** assegnatario, altri utenti potranno, per motivi di lavoro e su autorizzazione della ***Società***, entrare nella sua casella e leggere i messaggi in entrata e in uscita.

La ***Società*** comunque potrà accedere alla casella di posta elettronica – di cui sia titolare la medesima – utilizzata dall' ***Utente*** solamente per motivi connessi con lo svolgimento del lavoro.

Gli Utenti sono responsabile del corretto utilizzo delle caselle di posta elettronica aziendale e sono tenuti ad utilizzarla in modo conforme alle presenti regole:

- Non diffondere il proprio indirizzo e-mail aziendale al di fuori dei casi in cui questo sia necessario o opportuno.

- Conservare la password nella massima riservatezza e con la massima diligenza.
- Mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti.
- Utilizzare, quando necessario o opportuno, la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.
- Prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura nonché alla posta ricevuta. Gli allegati provenienti da mittenti sconosciuti non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (es. virus).
- Inviare preferibilmente e, se possibile, files in formato PDF non editabile.
- Non utilizzare la casella di posta elettronica aziendale per inviare, ricevere o scaricare allegati contenenti video, brani musicali, etc., salvo che questo non sia funzionale all'attività prestata in favore della Società (es: presentazioni o materiali video aziendali).
- Accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i files attachment di posta elettronica prima del loro utilizzo.
- Rispondere ad e-mail pervenute solo da mittenti conosciuti e cancellare preventivamente le altre.
- Collegarsi a siti internet contenuti all'interno di messaggi solo quando vi sia comprovata sicurezza sul contenuto degli stessi.

Si ricorda che, salvo l'utilizzo degli appositi strumenti di cifratura, i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto, si richiede agli ***Utenti*** di valutare con attenzione l'invio di informazioni classificabili come riservate o aventi comunque carattere confidenziale senza l'attivazione della cifratura.

Occorre inoltre che i messaggi di posta elettronica contengano un avvertimento ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi e precisato che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.

b) Organizzazione delle proprie caselle di posta

È necessario che ogni ***Utente*** provveda alla manutenzione periodica delle caselle di posta ad uso esclusivo per la catalogazione in apposite sottocartelle dei messaggi o la loro cancellazione.

In caso di accesso a caselle condivise con altri ***Utenti*** è necessario attenersi alle disposizioni del preposto alla casella per l'uso (responsabilità di chi legge il messaggio, modalità di smistamento dei messaggi, manutenzione periodica, ecc.).

Si ricorda che quando si ELIMINA un messaggio di posta questo viene spostato nella cartella POSTA ELIMINATA. È necessario svuotare periodicamente la cartella di POSTA ELIMINATA per cancellare fisicamente il messaggio (soprattutto per quelli con grossi allegati) e liberare spazio.

c) Regole per la posta (FUORI SEDE)

Il programma di posta consente di definire il testo che si desidera venga inviato in risposta ad ogni messaggio che verrà inviato quando si è FUORI SEDE. Chiunque invierà una e-mail riceverà automaticamente il messaggio che lo informerà della impossibilità di leggere la posta in tempi brevi (nel messaggio "FUORI SEDE" è opportuno indicare la data di rientro prevista) e quindi potrà comportarsi di conseguenza.

Ovviamente la funzione è particolarmente utile per il periodo di ferie o di assenza prolungata.

È quindi necessario attivarsi in tal senso per evitare che possa arrivare una comunicazione esterna urgente senza che nessuno la possa leggere ed attivarsi di conseguenza.

d) Costo della posta su internet

Anche se il costo della posta su internet è molto basso va tenuto conto che in realtà non è nullo. La posta occupa, infatti, il tempo di chi la riceve, spazio sui server della posta e rappresenta comunque uno spreco di banda di trasmissione.

Anche se nel singolo caso queste spese assommano a pochi centesimi di euro, nell'aggregato le somme coinvolte possono essere rilevanti. Va soprattutto tenuto conto che i costi della posta elettronica sono asimmetrici, nel senso che gravano maggiormente sul destinatario che sul mittente.

È quindi opportuno cancellare le parti dei messaggi non significativi (nel caso di inoltra o rispondi) per evitare di far perdere tempo o di trasmettere informazioni non necessarie a chi riceve la comunicazione ed è da evitare di inviare mail a persone non strettamente coinvolte nella gestione del messaggio.

e) Spam

Sempre più spesso su internet circolano e-mail indesiderate (*spam*).

È stato calcolato che le e-mail indesiderate rappresentano il 97% di tutte le e-mail che circolano su internet.

La ***Società*** è dotata di sistemi Antispam che riducono il numero di questi messaggi ma non possono annullarli per non rischiare di eliminare messaggi validi.

Quando si ricevono tali e-mail indesiderate, che oltretutto costituiscono una violazione della privacy ed un reato per la legge italiana, le cose da evitare sono le seguenti:

- rispondere al messaggio;
- seguire le istruzioni contenute nel messaggio, anche quando queste indicano come farsi rimuovere dalla lista o, ancora meno, quando danno dei link ipertestuali a siti di qualunque genere.

È comunque importante evitare di lasciare indirizzi in giro per la rete, soprattutto su siti che non si conoscono.

f) Gli hoax

Gli hoax (termine inglese che significa "imbroglio", "truffa", "bidone") sono messaggi diffusi in rete col metodo della catena di S. Antonio recanti contenuti falsi riconducibili sostanzialmente a due categorie:

- falsi allarmi relativi a virus informatici;
- false catene di solidarietà a beneficio di individui bisognosi (nella configurazione tipica si tratta di bambini affetti da gravissime malattie).

Gli hoax sono uno spreco di risorse e di tempo. In caso di dubbio è necessario inviare il messaggio all' ***IT Manager***, per il tramite della ***Società***, che provvederà a controllarlo anche utilizzando le apposite liste presenti su internet.

g) Phishing

PHISHING (termine coniato dalla storpiatura del vocabolo inglese "fishing" - pescare) è una tecnica fraudolenta che punta ad ottenere i dati personali (codici, password, dati della carta di credito, ecc) convincendo l' ***Utente*** a fornirli con falsi pretesti.

Un servizio di home banking, e-commerce, ecc. non chiederà mai i codici di accesso, numeri di carta di credito, codici bancomat o password inviando e-mail o lettere o telefonicamente e quindi è necessario NON rispondere a tali richieste di informazioni personali eventualmente pervenute.

Per "non abboccare" non accedere mai al sito di un servizio di home banking, e-commerce, ecc. che chiede di autenticarsi da un link inserito in un messaggio (e-mail, istant messaging …). Anche se il link nella e-mail o la barra degli indirizzi Web risulta (apparentemente) corretto, esistono delle tecniche per mascherare l'indirizzo fasullo con uno corretto. Entrare nella pagina digitando l'indirizzo direttamente nel browser (Explorer) o comunque controllare sempre l'indirizzo sulla barra.

h) Ransomware o Cryptovirus

Negli ultimi anni assistiamo ad una grande ondata di infezioni da criptovirus. Questi tipi di virus sfruttano prevalentemente il servizio di posta elettronica per entrare nel sistema del computer. Camuffato da banale documento allegato ad una e-mail come, ad esempio, una fattura di pagamento, una bolletta Enel, Tim, o e-mail provenienti da commercialisti e altre amministrazioni pubbliche, il programma viene inconsapevolmente avviato da parte dell'***Utente*** quando egli tenta di aprire il documento stesso. Purtroppo, il riconoscimento del programma malevolo all'interno dell'allegato è reso ancora più arduo dal fatto che in ambiente Windows l'estensione dei file non è direttamente leggibile.

Una volta insediato, il Cryptovirus individua rapidamente le risorse presenti nel device e, mediante la mappatura della rete, anche eventuali altri device connessi. Se il device viene lasciato accesso, il Cryptovirus ha la possibilità di svolgere con calma la sua azione, criptando il codice dei file. Questi virus sono stati studiati per colpire maggiormente i sistemi aziendali, in modo da poter rendere più efficacie il ricatto ed ottenere il pagamento.

Una volta che il virus ha criptato ogni tipologia di file, mostra un avviso sul desktop dell' ***Utente*** (a questo punto il danno è fatto), in cui descrive il problema e come risolverlo entro un determinato tempo che solitamente si aggira attorno alle 72 ore. Infatti, indica tutta una serie di istruzioni per effettuare il pagamento (illegale) in BitCoin (sistema di trasferimento denaro non tracciabile), e quindi ricevere la chiave per ripristinare tutti i nostri file.

L'unica soluzione è recuperare i dati dalle copie di backup.

i) Protezione da attacchi esterni

Dalla posta internet giungono ormai i maggiori "attacchi".

L'antivirus che protegge il sistema informatico provvede a controllare tutti gli allegati ripulendo o eliminando quelli ritenuti sospetti (all' ***Utente*** arriva come allegato, al posto dell'allegato originale, un messaggio dell'antivirus che segnala la rimozione dell'allegato precedente).

In ogni caso è opportuno:

- non aprire messaggi di posta di cui non si conosce il mittente;
- non aprire messaggi di posta contengono un oggetto non chiaro, pur provenendo da mittenti noti (alcuni virus, infatti, si propagano utilizzando le agende dei device infettati per rinviare messaggi infetti);
- non aprire allegati a messaggi "dubbi" (oggi ci sono dei professionisti del crimine che possono dedicare del tempo a leggere il contenuto di posta, di cui si sono impossessati illegalmente, per individuare elementi specifici – es. nome dei familiari o di comuni amici – per inserirli in un messaggio per renderlo più credibile).

l) Tutela della Privacy

Il Garante per la Privacy ha affermato che gli indirizzi e-mail non sono "pubblici" come possono essere quelli presenti sugli elenchi telefonici.

La vasta conoscibilità degli indirizzi e-mail che Internet consente, non rende lecito l'uso di questi dati personali per scopi diversi da quelli per i quali sono presenti on line. L'eventuale disponibilità in Internet di indirizzi di posta elettronica va "rapportata alle finalità per cui essi sono pubblicati sulla rete".

Per poter inviare una e-mail che non ha per oggetto la normale attività lavorativa senza violare la privacy degli utenti web è obbligatorio, dunque, ottenere prima il loro consenso.

m) Modalita di invio dei messaggi

Un messaggio può essere inviato ad uno o più destinatari indicati nel campo: "A".

Lo stesso messaggio potrà essere inviato sempre ad uno o più destinatari, con significato, "Per conoscenze" usando il campo "Cc".

È importante usare il campo "A" per indicare l'effettivo destinatario (chi deve prendere decisioni od eseguire le indicazioni presenti nel messaggio) distinguendo attraverso l'apposito campo, i destinatari solo per conoscenza (che non sono tenuti a compiere nessuna azione diretta in relazione al messaggio).

Tutti i proprietari delle caselle postali indicate sia nel campo "A" che nel campo "Cc" vedranno a chi è stato inviato lo stesso messaggio.

Se si desidera è possibile utilizzare il campo "Ccn" (per conoscenza nascosto) che consente di far giungere il messaggio anche ad altre persone senza che nessun altro lo possa sapere.

Il campo "Ccn" viene utilizzato anche per la difesa della privacy in quanto, in questo modo, non si diffondono gli indirizzi quando non è strettamente necessario.

Se un ***Utente*** che riceve un messaggio preme "Rispondi a tutti" la sua risposta verrà inviata solo agli indirizzi presenti nei campi "A" e "Cc" (escluso il proprio) e non a quelli presenti nel campo "Ccn".

È importantissimo riempire sempre il campo "Oggetto" oltre che per la comodità di chi riceve il messaggio che avrà maggiore facilità ad archiviarlo ed a ritrovarlo anche per la sicurezza.

Come già detto, alcuni virus sono in grado di replicarsi rinviando automaticamente posta a tutti gli indirizzi dell'agenda del device infettato. È quindi possibile ricevere posta "infetta" anche da persone note. Più difficile è che l'oggetto della posta infetta sia coerente (spesso è in inglese o comunque generico).

NOTA: Si consiglia di scrivere i destinatari solo dopo aver scritto e controllato il messaggio per evitare l'invio per errore di bozze incomplete.

Si consiglia di controllare gli eventuali allegati o link, il testo inserito nell'oggetto (è l'unica cosa che viene presentata e permette di evidenziare il messaggio anche su dispositivi mobili quindi deve essere chiaro e conciso) e dopo aver riletto e controllato, anche immaginando di invertire le parti, il testo del messaggio (la percezione di una email è asimmetrica: viene spontaneo scriverla di getto, come se parlassimo, ma viene ricevuta e rimane con l'ufficialità di un documento scritto).

n) Accesso alla posta aziendale da dispositivi privati

Se viene richiesto espressamente dall' ***Utente*** la ***Società*** può configurare i dispositivi personali (computer, tablet e smartphone) per accedere alla posta aziendale.

È possibile richiedere la configurazione solo per dispositivi ad uso strettamente personale ai quali non accedono, ad esempio, famigliari o amici.

È necessario che i dispositivi siano protetti da password o da rilevazioni biometriche ed è necessario prestare attenzione nell'impiego dei dispositivi in aree pubbliche, sale riunioni, reti domestiche e altre zone non protette.

o) Accesso alla posta personale da dispositivi aziendali.

L'accesso alla posta personale tramite web utilizzando i dispositivi aziendali e attraverso la connessione aziendale è espressamente vietata anche per evitare che dati personali possano essere trattati dai meccanismi automatici preposti alla sicurezza della rete.

11. CRITERI PER I DATI ELETTRONICI

a) Memorizzazione delle informazioni

Qualora l' ***Utente*** si trovi nelle condizioni di dover memorizzare informazioni che richiedono di essere protette in modo particolare perché potrebbero essere oggetto di "attacco dall'esterno" o perché una loro diffusione non autorizzata potrebbe portare a ripercussioni legali dovrà avvisare l'***IT Manager*** per il tramite della ***Società***.

b) Dati sui portatili o su supporti removibili

È necessario tenere presente che i dispositivi mobili potrebbero non essere collegati alla rete (o collegati con limitazioni di banda) durante le normali operazioni di aggiornamento automatico del software, per evitare vulnerabilità, o durante le operazioni di backup. L' ***Utente*** che ne fa uso dovrà quindi verificare periodicamente, eventualmente chiedendo il supporto all' ***IT Manager***, il corretto svolgimento di queste operazioni soprattutto dopo periodi nei quali l'apparecchiatura non è collegata alla rete aziendale direttamente o con una banda adeguata.

Gli ***Utenti*** che adoperano connessioni WiFi devono tener presente che alcuni protocolli di comunicazione sono immaturi e hanno debolezze note mettendo quindi, soprattutto in aree pubbliche, a rischio la riservatezza delle informazioni.

Nel caso di utilizzo di device portatili è necessario tener presente la possibilità di furto fisico dell'apparato e quindi la possibilità di rimuovere il disco per leggerne le informazioni da parte di terzi.

Qualora si intenda conservare sul disco del device portatile informazioni riservate è necessario salvarli in modalità protetta con opportune password e crittografie.

Analoghe accortezze devono essere rivolte nel caso di memorizzazione di informazioni riservate su supporti removibili.

Se i supporti contengono dati riservati è cura di chi li produce provvedere alla loro conservazione adottando misure idonee ad evitare la loro divulgazione. Analoga cura dovrà essere posta alla loro distruzione o alla cancellazione dei dati una volta cessato il motivo della duplicazione.

Qualora venga smarrito o rubato un device portatile o un supporto di memorizzazione è fatto obbligo all' ***Utente*** di presentare una tempestiva denuncia formale alle autorità competenti e farne pervenire una copia alla ***Società*** entro il primo giorno lavorativo successivo alla suddetta denuncia.

c) Smaltimento delle apparecchiature

La ***Società***, anche al fine di prevenire la produzione di rifiuti di apparecchiature elettroniche, ne promuove il reimpiego, il riciclaggio e altre forme di recupero di tali rifiuti in modo da ridurne la quantità da avviare allo smaltimento.

Questo comporta un rischio elevato di "circolazione" di componenti elettroniche che potrebbero contenere dati personali, anche sensibili, che non siano stati cancellati in modo idoneo, e di conseguente accesso ad essi da parte di terzi non autorizzati (la ***Società*** ha infatti deciso di non ricorrere alla cifratura di tutti i dati per facilitare il recupero dei dati a fronte di malfunzionamenti).

L'*Utente* che restituisce un'apparecchiatura (anche se non funzionante) dovrà informare circa la presenza di dati personali (normalmente non ammessi) per attivare le operazioni di cancellazione altrimenti non applicate ai singoli device.

d) Cartelle su server remoti

È proibito creare aree di memorizzazione delle informazioni aziendali presso fornitori di servizi Cloud (Dropbox, Drive, ecc.) senza la preventiva autorizzazione della ***Società*** che identificherà i fornitori di servizi Cloud utilizzabili e il tipo di dati memorizzabili e le eventuali misure di sicurezza aggiuntive da applicare.

Qualora si desideri memorizzare dati riservati su server remoti (Cloud) è necessario salvarli in modalità protetta poiché detti dati sono esposti ad accessi non autorizzati.

e) Protezione delle informazioni

Per proteggere delle informazioni (singoli file o intere cartelle) è possibile utilizzare i programmi di compressione aggiungendo una password.

È necessario che la password utilizzata sia adeguatamente lunga per evitare che essa possa essere scoperta con un numero di tentativi troppo bassi (effettuati da appositi programmi in automatico).

f) Telelavoro.

La ***Società*** non prevede contratti di telelavoro anche se viene consentito, in condizioni di eccezionalità (es: 2020 pandemia), l'accesso ai servizi operativi sempre e soltanto nelle modalità previste dalla ***Società***.

g) Rapporti con terze parti.

Nei rapporti con terze parti è necessario assicurare la sicurezza delle informazioni.

h) Copie di dati Riservati

La documentazione che costituisce per la ***Società*** *"know how" aziendale tecnico o commerciale non può essere comunicata all'esterno senza preventiva autorizzazione della stessa.*

La copia di dati riservati su cartelle diverse da quelle originali o su supporti removibili (FD, CD, MicroDriver USB, ecc.) o l'invio degli stessi dati tramite posta elettronica o lo scambio di dati tramite VPN, ecc. deve avvenire con le seguenti modalità in base all'uso:

- Per copie personali sarà cura dell' ***Utente*** garantire il mantenimento delle misure idonee anche sui dati copiati.
- Per invio ad altro personale della ***Società*** (che potrà avvenire unicamente per necessità) sarà cura di chi ha effettuato la copia concordare con il destinatario le modalità per il mantenimento di misure idonee alla riservatezza dei dati.
- Per invio all'esterno della ***Società*** sarà necessario concordare con la stessa le modalità per la trasmissione che comunque potrà avvenire solo a seguito di impegno scritto da parte del destinatario sulle modalità di trattamento dei dati per il mantenimento di misure idonee.

l) Misure di Sicurezza

I documenti contenenti dati riservati o contenenti dati personali non devono essere condivisi, comunicati o inviati a soggetti o istituzioni che non ne abbiano bisogno per lo svolgimento delle funzioni lavorative.

In base al supporto utilizzato è necessario adottare differenti misure per garantire la riservatezza dei dati copiati:

- ***Copia su cartelle***

  - Assicurarsi che abbiano criteri di sicurezza idonei ai dati che vi vengono copiati.
  - Provvedere all'eliminazione della copia quando non più necessaria.
  - Se i dati vengono copiati sul disco di un device portatile è necessario che l' ***Utente***, qualora questi siano sensibili o comunque riservati, provveda preventivamente a proteggerli.

- ***Copia su supporti removibili***

  - Indicare il contenuto del supporto non in chiaro.
  - Conservare il supporto con cura per evitarne lo smarrimento o il furto.
  - Utilizzare aree protette da password (MicroDriver USB).
  - Provvedere alla cancellazione dei dati (con formattazione o con sovrascrittura) o alla distruzione del supporto quando la copia non è più necessaria.

- ***Invio tramite posta elettronica***

  - L'indirizzo di posta deve essere accessibile solo a ***Utenti*** autorizzati al trattamento ed alla consultazione dei dati inviati.
  - I dati ricevuti tramite posta elettronica devono essere copiati solo su cartelle con le misure di riservatezza adeguate.
  - Il messaggio di posta deve essere eliminato in modo completo quando non più necessario.

- ***Invio tramite posta o fax***

  - I dati devono essere indirizzati all'attenzione del responsabile.
  - Nel caso in cui la consegna degli originali o delle fotocopie di documenti riservati avvenga per posta, si deve utilizzare la spedizione per assicurata convenzionale, che è l'unica che da garanzia di un continuo tracciamento del movimento del documento ed offre ben più elevate garanzie di sicura consegna al destinatario, rispetto alla più tradizionale raccomandata.
  - Quale che sia il tipo di spedizione adottato, in caso di dati riservati, è opportuno accertarsi che esso consenta di avere prova certa del fatto che il destinatario abbia effettivamente ricevuto i documenti inviati e che essi siano giunti integri, e quindi non manomessi o alterati in fase di trasporto.
  - I documenti riservati o contenenti dati personali devono essere inviati in busta chiusa e devono essere sigillati con colla, nastro adesivo o pinzatrice. Sulla busta deve essere indicata la dicitura riservato.
  - L'invio tramite fax è possibile solo se si ha la certezza che il fax ricevente sia accessibile solo dal destinatario che deve essere preventivamente avvisato, in modo

da ridurre il rischio che persone non autorizzate possano venirne a conoscenza, e successivamente è opportuno chiedere la conferma telefonica di avvenuta ricezione.

12. CRITERI PER IL TRATTAMENTO DEI DATI NON ELETTRONICI

a) Comunicazioni telefoniche

È proibito discutere, comunicare o comunque trattare dati riservati per telefono, se non si è certi che il corrispondente sia un utente, il cui profilo di autorizzazione sia tale da potere trattare i dati in questione.

È opportuno evitare di parlare ad alta voce trattando dati riservati per telefono, soprattutto utilizzando cellulari all'esterno della ***Società*** o anche all'interno, in presenza di terzi non autorizzati, onde evitare che dati riservati possano venire a conoscenza di terzi non autorizzati, anche accidentalmente.

Le suddette precauzioni diventano particolarmente importanti quando il telefono è utilizzato in luogo pubblico od aperto al pubblico.

b) Documenti cartacei

L' ***Utente*** che ha il compito di redigere documenti riservati o contenenti dati personali dovrà avere cura di rendere partecipe alla redazione del documento il minor numero possibile di persone, onde minimizzare la potenziale divulgazione non autorizzata delle informazioni trattate. È consigliabile, pertanto, non redigere documenti riservati o contenenti dati personali alla presenza di persone non appartenenti alla ***Società*** mittente o che, comunque, non sia necessario mettere al corrente del contenuto del documento stesso.

La ***Società***, al suo interno, ha individuato luoghi e arredi sicuri ove sono di norma custoditi i documenti contenenti dati riservati; come regola generale, tali documenti non devono essere asportati da tali luoghi sicuri e, ove ciò avvenga, la asportazione deve essere ridotta al minimo tempo necessario per effettuare le operazioni di trattamento. Dal luogo sicuro devono essere asportati solo i documenti strettamente necessari per le operazioni di trattamento e non intere pratiche, se ciò non è necessario.

Al termine delle operazioni di trattamento, i documenti devono essere immediatamente riposti nel luogo sicuro. Per tutto il periodo in cui i documenti sono all'esterno del luogo sicuro, l' ***Utente*** non deve mai perderli di vista, adempiendo ad un preciso obbligo di custodia dei documenti stessi.

Tutti i documenti cartacei contenenti informazioni personali o riservate prodotti o comunque trattati devono essere idoneamente custoditi dall'***Utente*** e conservati in locali, scrivanie o armadi il cui accesso sia limitato ai soli ***Utenti*** autorizzati. Nei periodi di assenza dell'***Utente*** i documenti devono essere riposti in modo da non essere consultabili da persone che hanno accesso ai locali per altre funzioni (es. pulizie).

Particolare cautela deve essere presa ove i documenti in questione vengano consegnati in originale a un ***Utente*** o responsabile debitamente autorizzato, onde evitare possibili perdite o distruzione accidentale.

Non è ammesso l'uso di fotocopiatrici e di altre tecnologie di riproduzione (per esempio scanner, fotocamere digitali) da parte di ***Utenti*** non autorizzati e le stampe contenenti informazioni riservate devono essere rimosse immediatamente dalle stampanti (o inviate alle stampanti non presidiate con un codice noto solo a chi ha inviato il documento in stampa).

Lo smaltimento dei documenti contenenti informazioni riservate viene effettuato tramite distruggi documenti o tramite l'inserimento in sacchi di plastica chiusi. È proibito il riutilizzo di carta contenente informazioni riservate.

c) Posta

Gli ***Utenti*** addetti allo smistamento della posta devono provvedere a non lasciare incustoditi i documenti prima della consegna al destinatario. In caso di documenti contenenti informazioni personali sarà necessario inserirli in busta chiusa qualora lo smistamento non avvenga direttamente.

d) Stampanti, Fotocopiatrici, Scanner e FAX

L'utilizzo dei suddetti strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte della ***Società***.

È richiesta una particolare attenzione quando si invia su una stampante condivisa documenti aventi ad oggetto dati personali o informazioni riservate; ciò al fine di evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di evitare di lasciare le stampe incustodite e ritirare immediatamente le copie non appena uscite dalla stampa.
È necessario ritirare anche gli originali nel caso di utilizzo della fotocopiatrice o scanner.

I documenti prodotti dagli scanner devono essere, se possibile, indirizzati direttamente a cartelle adeguate alla conservazione dei dati in oggetto o, dove non possibile, immediatamente rimossi da cartelle alle quali possono avere accesso altri utenti.

L'accesso ai FAX deve essere limitato ai soli Utenti incaricati al trattamento dei dati. Ogni documento pervenuto per fax deve essere consegnato immediatamente all'interessato o, se assente, custodito in luogo sicuro e non accessibile.

L'utilizzo dei fax per l'invio di documenti riservati è generalmente da evitare. Nei casi in cui questo sia necessario, si devono utilizzare le accortezze per la trasmissione delle informazioni riservate sopra riportate.

13. SEGNALAZIONE DEI PROBLEMI

a) Gestione assistenza agli Utenti

Ogni ***Utente***, in caso di problemi nell'uso dei Sistemi Informativi, può richiedere il supporto dell'***IT Manager*** tramite la ***Società***.

b) Rilevazione problematiche

Ogni ***Utente*** è invitato a segnalare tempestivamente problemi effettivi o potenziali relativi al sistema di sicurezza delle informazioni all'***IT Manager*** tramite la ***Società***, comunicando una

precisa individuazione del funzionamento anomalo. Si provvederà alla verifica ed alla gestione della eventuale Non Conformità rilevata o all'attuazione di opportune Azioni Preventive o Correttive.

Esempi di problemi legati alla sicurezza delle informazioni sono:

- Malfunzionamenti o comportamenti anomali di software o hardware (Messaggi di errore del sistema messaggi inusuali sullo schermo, tempi di caricamento o esecuzione maggiori del consueto, scomparsa non motivabile di files, ecc.).
- Funzionalità dell'ambiente operativo non disponibili.
- Funzionalità applicative non disponibili.
- Informazioni sull'ultimo LOGIN effettuato non corrispondenti all'ultima connessione realizzata dall'***Utente***.
- Violazioni delle aspettative di integrità, riservatezza o disponibilità delle informazioni.
- Errori umani.
- Violazioni alla sicurezza fisica.
- Non conformità rispetto a politiche, procedure o alla presente Policy.

In nessun caso l'***Utente*** dovrà tentare di verificare in autonomia le sospette debolezze del sistema mentre è opportuno che annoti immediatamente tutti i dettagli come il tipo di non conformità o violazione, il malfunzionamento avvenuto, i messaggi sullo schermo ecc.

L'***IT Manager***, in caso di problematiche non risolubili internamente, provvederà a coinvolgere consulenti esterni di supporto.

c) Segnalazioni ("whistleblowing").

Ogni ***Utente*** può presentare, a tutela dell'integrità della ***Società***, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi della sicurezza delle informazioni e fondate su elementi di fatto precisi e concordanti, o di violazioni delle procedure aziendali e della presente Policy, di cui siano venuti a conoscenza in ragione delle funzioni svolte direttamente.

La segnalazione dovrà essere fatta all'***IT Manager*** tramite la ***Società*** che garantisce la riservatezza dell'identità del segnalante (si ricorda che è fatto divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione e che sono previste sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate).

14. STRUMENTI DI FONIA MOBILE E/O DI CONNETTIVITA' IN MOBILITA'

La ***Società*** può mettere a disposizione, a seconda del ruolo o della funzione del singolo ***Utente***, impianti di telefonia fissa e mobile, nonché dispositivi – quali smartphone e tablet – che consentono di usufruire della navigazione in internet tramite rete dati e/o del servizio di telefonica tramite rete cellulare.

Come per qualsiasi altra dotazione aziendale, i dispositivi di cui sopra rappresentano beni aziendali dati in uso per scopi esclusivamente lavorativi. È tuttavia concesso un utilizzo personale sporadico e moderato dei telefoni aziendali utilizzando la c.d. "diligenza del buon padre di famiglia" e comunque tale da non ledere il rapporto fiduciario instaurato con la ***Società***.

A tal fine si informano gli utilizzatori dei servizi di fonia aziendale, che la ***Società*** potrà richiedere ai provider di telefonia i dettagli necessari ad effettuare controlli sull'utilizzo ed i relativi costi di traffico effettuato nel tempo. Previa comunicazione scritta all'***Utente***, la ***Società*** si riserva la facoltà, qualora dall'esame del traffico di una singola utenza rilevi uno scostamento significativo rispetto alla media del consumo, di richiedere un tabulato analitico delle chiamate effettuate dalla SIM in incarico all'***Utente*** per il periodo interessato.

L'utilizzo dei dispositivi ivi disciplinati risponde alle regole che di seguito si riportano:

- Ogni ***Utente*** assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e, conseguentemente, anche della sua diligente conservazione.
- I dispositivi devono essere dotati di password di sicurezza e/o rilevazione biometrica che ne impedisca l'utilizzo da parte di soggetti non autorizzati.
- In caso di furto, danneggiamento o smarrimento del dispositivo mobile in oggetto, è fatto obbligo all'***Utente*** di presentare una tempestiva denuncia formale alle autorità competenti e farne pervenire una copia alla ***Società*** entro il primo giorno lavorativo successivo alla suddetta denuncia. Ove detti eventi siano riconducibili ad un comportamento negligente, imprudente dell'***Utente*** e/o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti. In caso di furto o smarrimento la ***Società*** si riserva la facoltà di attuare la procedura di cancellazione da remoto di tutti i dati sul dispositivo, rendendo il dispositivo inutilizzabile e i dati in esso contenuti irrecuperabili.
- Non è consentito all'***Utente*** caricare o inserire all'interno del dispositivo qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli assegnatari di cancellare tutti i dati eventualmente presenti prima di consegnare il cellulare agli uffici competenti per la restituzione o la riparazione.
- Sugli strumenti di telefonia mobile eventualmente messi a disposizione, non è consentito all'***Utente*** effettuare procedure di Ijailbreak (letteralmente: evasione – è una procedura che rimuove le restrizioni software imposte ad esempio da Apple nei dispositivi iOS), modifiche del firmware o procedure di sblocco a vario titolo, tali da permettere l'illegittima installazione di software e/o applicazioni coperte da copyright.
- L'eventuale installazione di applicazioni, sia gratuite che a pagamento, sugli smartphone e tablet deve essere espressamente autorizzata, rimanendo, diversamente, a carico dell'***Utente*** le responsabilità derivanti dall'installazione non autorizzata.
- Salvo diversi specifici accordi, al momento della consegna del tablet o smartphone l'***Utente*** è tenuto a verificare, se lo ritiene opportuno, la disattivazione del sistema di geolocalizzazione potenzialmente attivabile sugli smartphone e tablet, consapevole che, in caso contrario, la ***Società***, e non solo, potrebbe venire a conoscenza, seppur incidentalmente, dei dati relativi alla posizione del dispositivo stesso e del suo assegnatario.

15. UTILIZZO DI APPARECCHI PERSONALI SUL LUOGO DI LAVORO

Gli apparecchi di proprietà personale dell'*Utente* quali computer portatili, telefoni cellulari, agende palmari (PDA), tablet, hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali, ecc., non potranno essere collegati ai device o alle reti informatiche aziendali, salvo preventiva autorizzazione della *Società*.

16. CESSAZIONE DEL RAPPORTO O MODIFICA DI FUNZIONE

A seguito della cessazione del rapporto o di modifica di funzione l'***Utente*** dovrà restituire tutte le apparecchiature concesse in uso dalla **Società** e l'***IT Manager*** potrà modificare la password assegnata all'***Utente*** senza più comunicarla allo stesso.

Per tutte le caselle che fanno riferimento al nome e cognome dell'U***tente*** valgono le seguenti regole: per un anno la casella di posta precedentemente assegnata all'***Utente*** rimarrà attiva per la ricezione dei messaggi di interesse aziendale. Entro 2 mesi dalla modifica di funzione o cessazione del rapporto un messaggio di risposta automatica indicherà il nuovo indirizzo da utilizzare per raggiungere la funzione aziendale.

Il contenuto dei dati della casella della posta aziendale dell'***Utente*** rimarranno a disposizione della ***Società*** che potrà darne l'accesso ad altri utenti per lo svolgimento delle attività aziendali per un periodo non superiore ai 10 anni dalla cessazione del rapporto (visto che potrebbero contenere dati aziendali necessari in caso contestazioni).

Qualora fra i dati trattati dall'***Utente*** possano rientrare informazioni che possono servire alla difesa della ***Società*** i dati potranno essere conservati per un tempo indeterminato ma non verranno utilizzati se non per la ricerca di informazioni utili per la difesa della ***Società*** eseguita direttamente dall'***IT Manager***.

Si ricorda che gli accordi di riservatezza permangono anche dopo la conclusione, per qualunque motivo, del rapporto o variazione di funzione.

17. RIFERIMENTI

Di seguito i riferimenti della Società:

- **TITOLARE DEL TRATTAMENTO**
  Opra – Organismo Paritetico Regionale dell'Artigianato - Via Vittorio Veneto 16/A – 20124 Milano (MI)

- **AMMINISTRATORE DI SISTEMA**
  EPiNet **SRL** (email: paolo.toniolo@epinet.it

- **RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO – DATA PROTECTION OFFICER)**
  Pietro Storti (email: dpo@opra.it)