Regolamento sulla protezione e sicurezza dei dati

FOGLIANI Spa – FUTURTEC Srl
FOGLIANI ROMANIA

CONTROLLO DEL DOCUMENTO

CODICE DOCUMENTO	LIVELLO DI REVISIONE	DATA DI EMISSIONE	TIPO DOCUMENTO
	1.0	7 marzo 2019	POLICY

Sommario

1 INTRODUZIONE

Il presente documento rappresenta il regolamento di Fogliani e delle società collegate/controllate sulla privacy e sicurezza dei dati personali.

Per Fogliani la sicurezza delle informazioni è una condizione necessaria al fine di raggiungere gli obiettivi istituzionali: la salvaguardia dei dati aziendali e dei relativi sistemi informativi consente infatti a Fogliani di erogare servizi di qualità garantendo l'affidabilità del servizio offerto.

Attraverso i sistemi informativi aziendali vengono trattati numerosi dati personali relativamente ai quali le normative italiana ed europea sulla Privacy richiedono l'implementazione di misure di sicurezza tecniche ed organizzative ed il coinvolgimento attivo degli incaricati al trattamento, al fine di garantire un'adeguata protezione degli stessi.

La protezione dei dati aziendali dipende sostanzialmente dall'osservanza di norme comportamentali che consentano di preservare la Riservatezza, l'Integrità e la Disponibilità degli stessi nel tempo (criterio RID).

1.1 SCOPO

Trattandosi di una policy e non di una procedura, non sono riportate specifiche attività e flussi di operazioni.

L'obiettivo primario della presente policy è far sì che tutti gli utenti adeguino il proprio comportamento secondo le indicazioni dettagliate di seguito.

Questo contribuirà al raggiungimento degli obiettivi della sicurezza, riassumibili nei tre aspetti distinti:

- **Riservatezza**, ovvero garantire la prevenzione di accessi abusivi o non autorizzati alle informazioni, ai servizi e ai sistemi;
- **Integrità**, ovvero garantire che le informazioni non siano state alterate da incidenti o abusi.
- **Disponibilità**, ovvero garantire l'accesso alle informazioni e ai servizi di rete da parte del personale incaricato in relazione alle esigenze lavorative;

1.2 DESTINATARI

Il presente documento è destinato a tutti i dipendenti e collaboratori interni di FOGLIANI Spa, FUTURTEC Srl, FOGLIANI ROMANIA Srl

1.3 REVISIONE E AGGIORNAMENTO DEL DOCUMENTO

La revisione e l'aggiornamento del presente documento sono in carico alle Direzione Amministrativa e alla funzione IT, che si avvalgono del supporto di tutte le altre strutture aziendali relativamente alle aree di competenza.

2 RIFERIMENTI LEGISLATIVI

La legislazione italiana negli ultimi anni si è dotata di un complesso di norme volte a guidare le aziende nel raggiungimento di un equilibrio tra quanto le tecnologie consentono di realizzare e la necessità di proteggere dati che spesso non appartengono ai singoli soggetti che li gestiscono.

Adempiere alla normativa in materia di sicurezza delle informazioni significa, quindi, evitare il rischio legale ovvero di incorrere in sanzioni penali/amministrative a seguito del mancato adempimento di leggi o regolamenti.

Relativamente al tema della sicurezza dei dati in azienda è possibile sintetizzare la normativa italiana ed europea di riferimento nelle seguenti voci:

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali del 27 aprile 2016
- Codice in materia di protezione dei dati personali (D.Lgs. 196 del 30 giugno 2003), abrogato parzialmente e modificato dal decreto 101/2018
- Provvedimenti del Garante Privacy
- Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica, Legge n. 547 del 1993
- Normativa sul diritto d'autore (Legge 633/41)
- D.Lgs. 231 del 08/06/2001 sulla Responsabilità Amministrativa degli Enti

2.1 Normative in materia di protezione dei dati personali (Regolamento Europeo 2016/679)

Il **General Data Protection Regulation (GDPR)**, ovvero il Regolamento UE n. 679/2016 sulla protezione dei dati personali (o Regolamento sulla privacy), è entrato in vigore Il 24 maggio 2016, e diventa pienamente applicabile dal 25 maggio 2018, abrogando la Direttiva 95/46/CE da cui sono nate negli scorsi anni le diverse normative nazionali (tra cui l'italiano Testo Unico sulla Privacy - D.Lgs 196/2003).

Il Regolamento è relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che sono da intendere come "qualsiasi informazione concernente una persona fisica identificata o identificabile".

Non si tratta più di una norma esclusivamente giuridica, ma c'è un impatto anche economico perché il legislatore ha voluto introdurre le regole necessarie per mettere ordine nell'economica digitale, dominata dai colossi del web.

Principi generali

Come in sostanza già sancito dal D.Lgs 196/2003, il Regolamento garantisce che "*la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale*".

Il legislatore si propone di uniformare l'applicazione della protezione dei dati personali nel territorio dell'Unione, di assicurare un livello coerente ed elevato di protezione dei diritti e delle libertà fondamentali delle persone fisiche, e di rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione.

Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o trattati i dati personali che li riguardano, nonché la misura in cui i dati personali sono o saranno trattati.

Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro

Il Regolamento Europeo prevede fra i suoi pilastri il principio di **Accountability** (che potrebbe essere tradotto in "responsabilizzazione e obbligo di rendicontazione") che riguarda tutti i soggetti.

Il Titolare del trattamento dei dati deve essere in grado di dimostrare di avere adottato un processo complessivo di misure giuridiche, organizzative e tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi: deve dimostrare in modo positivo e proattivo che i trattamenti di dati effettuati sono adeguati e conformi.

Novità dall'Europa

Oltre al già citato e fondamentale principio di Accountability, con il Regolamento Europeo sono state introdotte alcune interessanti novità a tutela dei dati personali:

- Il "**Privacy Impact Assessment**" (valutazioni preventive di impatto sulla tutela dei dati) in caso di trattamenti rischiosi; vale a dire torna obbligatoria una puntuale analisi dei rischi. Il testo del Regolamento cita espressamente i parametri di gravità e probabilità dell'evento
- La nomina di un "**Data Protection Officer**" (responsabile della protezione dei dati personali), che dovrà essere competente, indipendente e non necessariamente interno all'ente/impresa. La nomina è obbligatoria in alcuni casi (es. trattamenti a rischio dei dati personali) ma tutte le organizzazioni hanno la facoltà di nominarlo per una corretta ed efficace gestione di un sistema privacy
- Le figure dei "**joint controllers**" (Contitolari), che potranno dividersi o condividere le responsabilità privacy in un apposito contratto, di cui si dovrà tenere conto in caso di controlli o contenziosi. Questa novità potrebbe essere utile, in particolare, nel settore del cloud computing (fino ad oggi difficilmente inquadrabile nei vecchi schemi titolare/responsabile).
- Il concetto di "stabilimento principale" del titolare, per evitare che un'impresa attiva in più Stati UE debba fronteggiare gli adempimenti nazionali di ogni singolo Stato.
- Il ruolo di "Lead Authority", per far sì che vi sia un solo Garante di volta in volta responsabile dei procedimenti con impatti multi-Stato
- **Sanzioni** molto più pesanti che in passato: fino al 4% del volume d'affari globale di un'impresa. Lo scopo è chiaramente far diventare la protezione dei dati un tema sensibile anche e soprattutto per le grandi multinazionali (ad esempio Google, Facebook, Microsoft)
- L'obbligo di attenersi, nell'ideazione di nuovi prodotti o servizi, ai principi "**Data Protection by Design**" e "**Data Protection by Default**", cioè l'applicazione della protezione dati fin dalla fase di progettazione di qualsiasi trattamento
- Il diritto all'oblio, per cui ogni interessato potrà richiedere la rimozione di propri dati personali per motivi legittimi (per esempio, potremo chiedere di essere "dimenticati" on line).
- I ***Data Breach***, ovvero la notifica di una violazione all'autorità, se possibile entro 72 ore, e la comunicazione agli interessati.

Impatto sulla sicurezza del trattamento

A livello comunitario la disciplina sul tema della sicurezza del trattamento dei dati viene mantenuta nel suo impianto generale; si introduce però una maggiore attenzione al cosiddetto *risk-based approach* e si specificano in modo più descrittivo ed esemplificativo alcune delle principiali tipologie di misure tecniche ed organizzative.

Inoltre, assume grande rilievo la rilevazione di efficacia delle misure di sicurezza adottate (Art. 32, lettera d) e soprattutto la valutazione di impatto (nota come *DPIA - Data Protection Impact Assessment*) quale strumento fondamentale per conoscere lo stato attuale ed il margine di miglioramento del proprio sistema privacy.

In generale, si ribadisce uno dei concetti fondamentali della sicurezza delle informazioni: garantire la riservatezza, integrità e disponibilità (noti con l'acronimo RID).

Come tenere traccia di tutto questo? Il Regolamento UE prevede a carico dei titolari del trattamento o dei responsabili l'obbligo di adottare e mantenere della documentazione simile al Documento Programmatico sulla Sicurezza previsto dal D.Lgs 196/2003.

Per esempio, c'è l'obbligo di tenere un registro delle attività del trattamento dei dati personali, comprensivo di una descrizione generale delle misure di sicurezza tecniche e organizzative adottate. Formalmente, le piccole aziende che non presentano trattamenti a rischio possono essere esonerate da tale obbligo; si ne consiglia comunque l'adozione di tale registro, che permette in ogni situazione di dimostrare chiaramente la tipologia di dati personali gestiti.

Riassumendo il titolare ed i responsabili del trattamento sono tenuti ad adottare delle misure di sicurezza organizzative e tecniche volte a mitigare il rischio secondo un approccio proattivo (accountabilty), identificando i rischi connessi al trattamento (c.d. risk-based approach) e adottando misure adeguate che tengano in conto dei principi di trasparenza oltre ai principi di privacy by design (privacy sin dalla progettazione) e by default.

2.2 Modifiche ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica, Legge n. 547 del 1993

La Legge 547/93 ha introdotto il concetto di criminalità informatica all'interno delle norme del codice penale e del codice di procedura penale. In tal senso ha reso possibile perseguire i reati informatici in modo del tutto simile a quelli tradizionali prevedendo a carico del reo l'irrogazione di pene variabili fino ad un massimo di cinque anni di reclusione. I crimini informatici considerati e gli articoli del codice penale che sono stati sostituiti sono elencati qui di seguito:

- Attentato a impianti informatici di pubblica utilità (art. 420)
- Falsificazione di documenti informatici (art. 491 bis)
- Accesso abusivo ad un sistema informatico o telematico (art. 615 ter)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quarter)
- Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 quinquies)
- Violazione di corrispondenza telematica (artt. 616-617 sexies)
- Intercettazione di e-mail (art. 617 quarter)
- Danneggiamento di sistemi informatici e telematici (art. 635 bis)
- Frode informatica (alterazione dell'integrità dei dati allo scopo di procurarsi un ingiusto profitto (art. 640 ter)

La conoscenza delle figure di reato sopra elencate consente agli utenti di prevenire eventuali comportamenti criminosi durante l'utilizzo degli strumenti informatici e di comprendere maggiormente la necessità di applicare alcune delle regole di seguito descritte.

2.3 Normativa sul diritto d'autore (Legge 633/41)

La Legge 22 aprile 1941 n. 633 che disciplina la "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio", revisionata con la legge 18 agosto 2000 n. 248 e con il successivo Decreto legislativo n. 68 del 9 aprile del 2003, configura sanzioni penali e amministrative per chi viola il copyright. Secondo tale norma, in caso di constatazione dell'uso illecito di prodotti software in azienda, può essere ritenuto responsabile il rappresentante legale e l'eventuale responsabile del settore informatico, qualora venga accertato che l'illecito sia stato effettuato direttamente dall'azienda, mentre verrà ritenuto responsabile l'utente finale, qualora venga accertato che quest'ultimo ha introdotto copie illegali nell'ambiente di lavoro all'insaputa dell'azienda ovvero in contrasto con i regolamenti vigenti in azienda. L'utilizzo abusivo di software comporta quindi due tipi di rischi, uno di natura tecnica e uno di natura giuridica:

- Rischi di natura tecnica: l'utilizzo di programmi contraffatti all'interno della rete aziendale può comportare la diffusione di virus e il malfunzionamento dei sistemi dell'azienda (perdita di dati e di operatività) dovuti a copie incomplete e incompatibili tra loro;
- Rischi di natura giuridica: nella loro qualità di opere di intelletto, i prodotti software sono protetti dal regime giuridico dei diritti d'autore. La copia e l'utilizzo di prodotti software senza aver ottenuto la necessaria autorizzazione dal titolare dei diritti costituiscono un reato. I rischi di natura giuridica cui ci si espone comprendono sanzioni civili e sanzioni penali.

Per quanto riguarda, invece, la duplicazione abusiva dei programmi per elaboratore, chi commette tale reato rischia sanzioni penali a cui si può aggiungere una sanzione amministrativa pecuniaria, ovvero una multa che può arrivare al doppio del prezzo di mercato dei programmi copiati illegalmente.

FOGLIANI mette a disposizione dei propri utenti tutti gli strumenti software necessari allo svolgimento dell'attività lavorativa e garantisce la conformità degli stessi alla normativa sul diritto d'autore. È pertanto necessario che gli utenti si attengano scrupolosamente alle regole inerenti il software aziendale al fine di scongiurare i rischi connessi all'introduzione di programmi non autorizzati o dannosi.

2.4 Responsabilità Amministrativa degli Enti (D.lgs. 231/2001)

Il decreto 231/2001 ha introdotto nell'ordinamento italiano la responsabilità amministrativa degli enti per taluni reati ed illeciti che, pur compiuti materialmente da soggetti in posizione apicale o dipendenti dell'ente, si possono considerare direttamente ricollegabili allo stesso qualora "commessi nel suo interesse o vantaggio".

Fattispecie di reati perseguiti dal D.Lgs. 231/2001:

- reati nei confronti della pubblica amministrazione
- reati societari
- reati di falsità in monete, carte di pubblico credito e valori di bollo
- reati di insider trading e market abuse
- reati con finalità di terrorismo

Per i reati previsti dal decreto, l'ente è responsabile solo qualora la commissione del reato sia stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. E' esclusa l'omissione di tali obblighi se, prima della commissione del reato, l'ente ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della fattispecie di quello verificatosi.

2.5 Mancata osservanza delle presenti norme di comportamento.

FOGLIANI si riserva la facoltà, nei limiti consentiti dalla legge, di verificare l'adesione alle presenti norme per attività di verifica del corretto funzionamento dei sistemi.

FOGLIANI si riserva la facoltà di revocare l'autorizzazione all'accesso agli strumenti di Internet e di posta elettronica in caso di mancata osservanza delle norme sopra elencate.

Si fa altresì presente che, sulla base di specifiche norme di legge, sia l'accesso al sistema informativo aziendale per finalità non consentite dall'azienda sia - una volta ottenuto l'accesso - il mantenersi collegati al predetto sistema per finalità parimenti non consentite può costituire illecito penale (art. 615 ter Cod.Pen.) oltre che costituire inadempimento degli obblighi contrattuali rilevante sul piano disciplinare.

Inoltre, si fa presente che il Codice Penale (art. 615 quater) ipotizza espressamente la reclusione nei confronti di chi "al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo".

3 ACCEPTABLE USE POLICY

La sicurezza del sistema informativo di FOGLIANI è un requisito fondamentale per garantire l'affidabilità delle informazioni trattate, nonché l'efficacia ed efficienza dei servizi erogati dall'azienda. La sicurezza del sistema informativo ha come obiettivo primario la protezione dei dati e degli elementi attraverso i quali i dati stessi sono gestiti.

La protezione dei dati e degli elementi associati è garantita se viene preservata:

- **la riservatezza:** assicura che i dati siano accessibili solamente a coloro che sono autorizzati ad averne accesso;
- **l'integrità:** salvaguarda la completezza dei dati e dei metodi di trasferimento;
- **la disponibilità:** assicura che gli utenti autorizzati abbiano accesso ai dati e agli elementi che li trattano quando necessario;

La mancanza di un adeguato livello di sicurezza dei dati, in termini di Riservatezza, Disponibilità e Integrità, può avere come conseguenze la perdita di vantaggio competitivo, di immagine, di clienti, di fatturato ed una conseguente significativa perdita finanziaria. A tutto questo bisogna, inoltre, aggiungere il rischio di incorrere in sanzioni legate a violazioni delle normative vigenti.

Pertanto, la sicurezza del sistema informativo viene ottenuta implementando una serie di misure di sicurezza adeguate, ovvero procedure, meccanismi tecnici o pratiche che riducano i rischi cui risulta esposto il patrimonio informativo nel suo complesso.

FOGLIANI orienta la propria attività al rispetto della normativa vigente, con particolare riferimento al Codice in materia di protezione dei dati personali, non solo al fine di evitare il rischio di un coinvolgimento dell'azienda, ma sopratutto per garantire un adeguato livello di sicurezza dei dati personali dell'azienda e del relativo sistema informativo.

3.1 Politiche generali di sicurezza dei dati

Nel presente paragrafo vengono indicati i principi fondamentali che ispirano le norme per la sicurezza dei dati di FOGLIANI.

3.1.1 Sistemi informativi aziendali

Il sistema informativo aziendale è composto da un insieme di unità server centrali e PC client connessi ad una rete locale (LAN), che utilizzano diversi sistemi operativi e applicativi.

FOGLIANI fornisce ai propri dipendenti e collaboratori interni tutti gli strumenti necessari allo svolgimento delle mansioni assegnate. Gli strumenti e gli applicativi software forniti dall'azienda sono strumenti di lavoro e devono essere utilizzati per tali finalità. I dati presenti all'interno degli strumenti di lavoro sono considerati dati aziendali e come tali di proprietà dell'azienda. Di conseguenza su di essi l'azienda può disporre in modo completo e gli utenti non potranno avere aspettative di privacy rispetto alle informazioni inviate, ricevute o memorizzate.

Si ricorda inoltre che gli usi impropri dei sistemi aziendali includono l'elaborazione, la trasmissione, il recupero, l'accesso, la visualizzazione, l'immagazzinamento, la stampa ed in generale la diffusione di materiali e dati fraudolenti, vessatori, minacciosi, illegali, razzisti, di orientamento sessuale, osceni, intimidatori, diffamatori o comunque non congrui ad un comportamento professionale.

Pertanto, nessun dato di questo genere dovrà essere presente sulla rete FOGLIANI, sui Personal Computer, all'interno degli applicativi (come ad esempio la posta elettronica, i portali intranet, ecc.) e nelle cartelle di rete personali o condivise.

Inoltre, gli utilizzatori dei sistemi aziendali non devono utilizzare le infrastrutture per fare business, vendere prodotti, o per qualsiasi altra attività commerciale diverse da quelle espressamente previste dalla direzione aziendale.

3.1.2 Accesso alle informazioni

L'accesso alle informazioni da parte di ogni singolo utente deve essere limitato alle sole informazioni di cui necessita per lo svolgimento dei propri compiti (principio del *need to know*). La divulgazione e trasmissione di informazioni all'interno, così come verso l'esterno, deve fondarsi sullo stesso principio.

3.1.3 Personale e sicurezza

L'azienda programma ed esegue attività formative ed informative dirette al personale, con particolare attenzione alla sicurezza delle informazioni e al corretto uso della strumentazione aziendale.

Deve essere richiesto al personale di garantire un livello minimo di sicurezza alle apparecchiature assegnate. Il furto, il danneggiamento o lo smarrimento degli strumenti di lavoro devono essere prontamente segnalati.

Il personale (compresi i consulenti ed i collaboratori esterni) deve sottoscrivere clausole di riservatezza che dovranno essere ribadite al momento della cessazione del rapporto di lavoro.

Il mancato rispetto di quanto indicato in questo documento e in tutti gli altri che da esso discendono costituisce "incuria del materiale aziendale" e sarà pertanto oggetto di sanzioni disciplinari secondo quando indicato dall'articolo 7 della legge 300/70 e dal contratto Collettivo Nazionale di Lavoro.

3.1.4 Incidenti e anomalie

Tutti i dipendenti sono tenuti a rilevare e notificare al personale IT eventuali problematiche legate alla sicurezza aziendale.

3.1.5 Sicurezza fisica

L'accesso agli edifici ed ai locali rilevanti per la protezione dei beni e dei dati deve avvenire solo previa identificazione dei soggetti autorizzati. L'individuazione e la progettazione delle contromisure di sicurezza fisica deve tenere conto sia della possibilità del concretizzarsi di minacce di tipo fisico, sia della normativa e legislazione in vigore.

La manutenzione degli apparati deve essere eseguita in conformità con le indicazioni del costruttore o con procedure documentate per assicurare la disponibilità del servizio e l'integrità.

3.1.6 Sicurezza Informatica

La progettazione e l'implementazione del piano di sicurezza informatica deve tenere conto sia della possibilità del concretizzarsi di tentativi di accesso non autorizzati interni ed esterni, sia della normativa e legislazione in vigore e di altri vincoli legati a processi aziendali, certificazioni di settore, regolamenti.

Gli utenti non devono sfruttare le eventuali debolezze o le mancanze del sistema di sicurezza informatico per danneggiare sistemi o dati, ottenere risorse per le quali non si è autorizzati, sottrarre risorse ad altri utenti o avere accesso a sistemi per i quali non si hanno le necessarie autorizzazioni.

3.1.7 Verifiche

I sistemi informativi devono essere periodicamente controllati così come l'applicazione delle procedure operative.

I principi espressi nelle politiche generali di sicurezza trovano specifica applicazione all'interno delle norme di sicurezza generali e in quelle specifiche per il trattamento dei dati illustrate nei seguenti capitoli.

Il personale incaricato che opera presso la funzione IT è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi

tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.).

Detti interventi, in considerazione delle regole successivamente dettagliate sull'uso della posta elettronica e Internet, potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna.

La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'azienda, si applica anche in caso di assenza prolungata od impedimento dell'utente.

Il personale IT incaricato ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc.

L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

4 REGOLE SPECIFICHE

4.1 Accesso fisico e logico

4.1.1 Accesso alle sedi

L'accesso alle sedi è consentito previa identificazione dei collaboratori interni e dei visitatori. È necessario che il referente interno del visitatore lo accompagni sempre durante la sua permanenza nella sede FOGLIANI.

4.1.2 Accesso ai locali tecnici e alle sale CED

L'accesso a questi locali è ristretto ai soli autorizzati. In caso di manutenzione tecnica nel locale CED il personale esterno deve essere accompagnato da un referente interno FOGLIANI.

4.1.3 Gestione delle credenziali di accesso fisico a sedi, locali ed archivi

Tali credenziali di accesso sono attribuite dalla Direzione e/o da funzioni appositamente delegate in relazione ai diritti di accesso del personale. La consegna viene annotata in modo da conoscere sempre le abilitazioni di ogni singolo dipendente o collaboratore interno e in modo da gestire l'eventuale restituzione delle medesime (per esempio nel caso di chiavi fisiche) una volta terminata la relativa autorizzazione.

Periodicamente viene verificata la sussistenza delle condizioni relative ai diritti di accesso.

4.1.4 Gestione delle credenziali di accesso ai sistemi informatici

Tali credenziali di accesso vengono attribuite dagli incaricati IT su richiesta delle singole divisioni aziendali e dell'Ufficio Personale. Ciascun utente accede ai sistemi informatici con diritti definiti in relazione alla mansione svolta (es. utilizzo di specifiche risorse come applicazioni e cartelle di rete). Tali diritti vengono rivisti in occasione di cambiamento di mansione ovvero di cessazione del rapporto di lavoro.

Al fine di mantenere aggiornati i profili autorizzativi degli utenti l'Ufficio Personale ha il compito di comunicare ogni variazione organizzativa alle funzioni IT.

In caso un'utenza non debba essere più utilizzata, gli operatori IT provvedono ad avviare la procedura di cessazione che include la disattivazione dell'utenza, al fine di evitare di attribuire nuovamente tale utenza a soggetti diversi. In caso di inutilizzo per un periodo superiore a 6 mesi, le credenziali di accesso sono disabilitate automaticamente dove il sistema informatico lo consente o manualmente dal personale IT.

Quando l'inutilizzo di lunga durata è noto in anticipo (per esempio in caso di lungo infortunio o maternità), sarà cura dell'Ufficio Personale effettuare apposita comunicazione all'IT.

4.1.5 Manutenzione correttiva e preventiva dei sistemi

I sistemi devono essere sempre aggiornati per prevenire eventuali vulnerabilità.

A tal fine, le funzioni IT monitorano lo stato delle vulnerabilità note e degli aggiornamenti da installare, effettuano dove possibile in modo automatico o manuale gli aggiornamenti oppure notificano agli utenti quali attività intraprendere per mantenere i sistemi sempre allineati e in efficienza.

4.1.6 Fornitori

Qualora FOGLIANI si avvalga di società esterne per la gestione della sicurezza informatica e/ la manutenzione dei sistemi, tali soggetti saranno formalmente autorizzati ed incaricati ed assumeranno il ruolo, se applicabile, di Amministratore di Sistema o Responsabile Esterno del Trattamento.

4.1.7 Uso dei sistemi ad opera di terze parti

Gli agenti/consulenti/venditori esterni che, per la durata del rapporto di collaborazione devono accedere ai sistemi aziendali, sono autorizzati in modo formale dal Responsabile dell'area di competenza. Gli operatori IT si occupano della predisposizione delle credenziali e del profilo di accesso ai sistemi sulla base del ruolo che il consulente dovrà ricoprire e seguendo le indicazioni dell'Ufficio Personale e/o del Responsabile interno prima citato.

Oltre alla documentazione contrattuale, tutti i soggetti esterni abilitati all'accesso alla rete aziendale, devono ricevere e sottoscrivere il presente regolamento informatico aziendale.

Inoltre, se un soggetto esterno utilizza il proprio PC per collegarsi alla rete Guest aziendale, deve garantire di avere installato la versione più aggiornata del software antivirus e un sistema di protezione delle comunicazioni (es. VPN) qualora debba collegarsi a propria rete aziendale o comunque applicazione esterna.

I PC non di proprietà FOGLIANI non possono connettersi alle risorse di rete aziendali, sia via cavo che in WiFi.

Le persone che non sono dipendenti, collaboratori a tempo determinato, consulenti o agenti non devono essere a conoscenza e/o possedere user-id degli utenti interni e, allo stesso modo, non devono usufruire dei privilegi concessi dal sistema aziendale, salvo specifiche situazioni appositamente autorizzate, legate alle attività di manutenzione degli applicativi gestionali o di altri sistemi informatici.

4.2 Sicurezza degli strumenti

4.2.1 Protezione della postazione di lavoro

- Gli utenti devono evitare di lasciare incustodite postazioni di lavoro con la sessione di lavoro aperta ed attiva (login effettuato) o con videate contenenti dati riservati.
- Ciascun utente deve inserire il blocco del sistema (con CTRL-ALT-CANC + Blocca) quando si allontana dalla postazione di lavoro; la riattivazione è regolata da password (uguale a quella di accesso al sistema aziendale).
- Inoltre, ciascun utente dovrà assicurarsi che la postazione sia protetta dal salva schermo o blocco del sistema che entra in funzione automaticamente dopo un tempo definito di inattività (10-15 minuti); non è consentito modificare tale configurazione o disattivarla. Questo tipo di misure serve ad evitare che la postazione (e quindi gli applicativi aperti) possa essere utilizzata da altri in propria assenza
- Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.
- Spegnere il PC a fine giornata (salvo specifiche indicazioni da parte dell'IT per attività manutentive) o in caso di assenze prolungate, perché lasciare un elaboratore incustodito e connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'uso illecito

4.2.2 Corretto utilizzo degli strumenti elettronici

- È vietata l'installazione di programmi provenienti dall'esterno che non siano stati espressamente autorizzati dall'IT
- Non è consentito l'uso di programmi per i quali l'azienda non abbia acquisito idonea licenza
- Non è consentito l'utilizzo degli strumenti elettronici aziendali per duplicare e/o divulgare materiale protetto dal diritto d'autore o da brevetti

- Non è consentito modificare le configurazioni impostate sul proprio computer
- Non è consentito installare ed utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici
- Non è consentita l'installazione sul proprio computer di mezzi di comunicazione diversi da quelli messi a disposizione dall'azienda.
- Evitare di lasciare incustoditi supporti rimovibili (CD, DVD, nastri, chiavette usb) contenenti dati aziendali, sulle scrivanie o in altri luoghi dove potrebbero essere facilmente asportati da terze persone non autorizzate. Tutti i supporti, e tutto ciò che sia facilmente copiabile, asportabile ed occultabile, quando non utilizzati, devono essere riposti in armadi, scaffali o cassetti chiusi a chiave.

4.2.3 Maggiore attenzione ai computer portatili e altri strumenti di tipo "Mobile"

- Il computer portatile, il tablet e il cellulare possono venire concessi in uso dall'organizzazione agli Incaricati che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'organizzazione.
- A causa della vulnerabilità delle informazioni contenute sui device mobili, dovrà essere prestata particolare attenzione a questi tipi di sistemi e limitarne al massimo gli usi a rischio.
- Non lasciare mai il dispositivo incustodito; se siete presso altre aziende, potete utilizzare sistemi di protezione quali cavi di sicurezza per PC portatili.
- Durante i viaggi tenete sempre gli strumenti con voi. Non lasciate mai il PC portatile dentro l'auto, anche se riposto nel bagagliaio, oppure a vista in una stanza d'albergo, nell'atrio degli hotel e nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.
- Qualora non sia possibile una connessione sicura al sistema aziendale, eseguire il backup giornaliero degli eventuali dati riservati presenti sul device portatile utilizzando dispositivi esterni quali chiavette Usb che il personale IT può mettere a disposizione (su richiesta).
- In caso di furto o perdita, effettuare denuncia alle autorità competenti ed avvisare prontamente l'azienda (funzioni Ufficio Personale e IT) che effettuerà, se del caso, quanto necessario per impedire un utilizzo illecito delle utenze configurate sul device

4.2.4 Utilizzo del cellulare/smartphone personale

Durante l'orario di lavoro, comprese le eventuali pause, agli Incaricati è concesso l'utilizzo del telefono cellulare personale ma solo per comunicazioni di emergenza o strettamente collegate all'ambito lavorativo.

In caso di trasferte lavorative fuori ufficio, il telefono personale può rimanere acceso, anche per facilitare la comunicazione con l'azienda ove fosse necessario.

In questo caso si invita, comunque, a non utilizzarlo per fini personali, in modo particolare alla presenza di clienti o fornitori.

Gli Incaricati non dipendenti (consulenti, agenti, collaboratori esterni), possono utilizzare i propri cellulari/smartphone per memorizzare dati dell'azienda solo se espressamente autorizzati e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali cellulari/smartphone dovranno essere preventivamente valutati dal Titolare, per la verifica della sussistenza di misure di sicurezza adeguate.

4.2.5 Attenzione ai sistemi di comunicazione!

Le comunicazioni in rete viaggiano sempre più spesso con mezzi diversi dalla posta elettronica: software di instant messaging, social network e altri sistemi.

Si ricorda che spesso questi strumenti non sono in grado di proteggere le comunicazioni che veicolano.

Per esempio, è molto semplice vestire i panni di un altro utente con tanto di nome completo; spesso il mancato utilizzo del protocollo HTTPS agevola gli attacchi malware o l'assenza di tecnologie avanzate per la cifratura delle comunicazioni consente l'identificazione delle frasi con un'accuratezza straordinaria.

È sconsigliato quindi trasmettere documenti aziendali attraverso questo tipo di sistemi, a meno che non si tratti di applicazioni verificate ed autorizzate dall'azienda.

4.2.6 Antivirus

La presenza di un software antivirus è una misura di sicurezza essenziale ed un utile strumento di protezione. La sua efficacia dipende in modo fondamentale dall'aggiornamento che, per quanto riguarda i computer degli utenti, avviene in modo automatico durante l'attività lavorativa.

I titolari di computer portatili devono assicurarsi che l'antivirus sia sempre aggiornato, a tal fine è sufficiente connettersi frequentemente alla rete aziendale o al sito del produttore, usufruendo questo modo del servizio di aggiornamento automatico. Istruzioni di dettaglio sono disponibili presso l'IT.

Data la notevole complessità raggiunta dai virus, gli utenti non devono cercare di eliminarli senza l'aiuto di una persona esperta. Il sistema antivirus è impostato automaticamente per eliminare i virus trovati.

Se si sospetta una situazione più complessa o se il virus viene messo in quarantena perché impossibile da eliminare, l'utente deve immediatamente disconnettere il computer dalla rete, spegnerlo e contattare gli operatori IT.

Questo comportamento aiuterà a contenere i danni provocati ai file ed ai software e al tempo stesso garantirà che le informazioni necessarie per individuare una nuova infezione siano registrate.

4.2.7 Restituzione degli strumenti

A seguito della cessazione del rapporto lavorativo o di consulenza dell'utente con l'azienda o comunque al venir meno, ad insindacabile giudizio dell'organizzazione, della validità dei presupposti per l'utilizzo degli strumenti assegnati, gli incaricati hanno i seguenti obblighi:

a. Procedere immediatamente alla restituzione dei device in uso;
b. Divieto assoluto di formattare o alterare o manomettere o distruggere i device assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo manuale o automatizzato.

4.3 Memorizzazione e disponibilità dei dati

- I dati necessari per lo svolgimento della propria attività lavorativa (documenti, immagini inerenti al business, e-mail) devono essere salvati sulle risorse di rete messe a disposizione dall'azienda, al fine di consentirne il backup automatico centralizzato. Gli incaricati che operano all'esterno dell'azienda e che non hanno la possibilità di utilizzare le risorse di rete, devono richiedere alla funzione IT l'assegnazione di una memoria esterna qualora abbiano la necessità di effettuare backup di dati presenti sul PC locale (maggiori dettagli di seguito).

- Si raccomanda di:
    - salvare i dati nella cartella di rete più idonea in funzione della tipologia di documento e delle modalità utilizzate dal gruppo di lavoro di cui l'utente fa parte
    - non conservare in rete numerose versioni dello stesso documento e soprattutto, una volta consolidato il medesimo, eliminare le versioni precedenti, in modo da non occupare inutilmente risorse disco
    - evitare di spostare o eliminare dalle cartelle documenti non propri o non conosciuti; in ogni caso avvisare prontamente l'IT in caso di operazioni errate o non andate a buon fine

- Gli utenti non devono memorizzare in rete, nelle cartelle comuni e sul PC aziendale assegnato file e documenti a carattere personale o che comunque non siano attinenti all'attività professionale, sia per tutelare la privacy di ciascuno sia per non occupare inutilmente risorse disco.

  Pertanto, qualunque file che non sia legato all'attività lavorativa (es. fotografie personali, file musicali, video) NON può essere salvato sulle risorse aziendali (dischi di rete, storage condivisi, PC dell'utente), nemmeno per brevi periodi. L'azienda si riserva la facoltà di procedere immediatamente alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza dei propri sistemi ovvero nel caso in cui risulti che tali applicazioni siano state acquisite o installate in violazione del presente Regolamento.

- Non è consentita la memorizzazione o la diffusione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

- Non è consentita l'archiviazione di documenti aziendali presso servizi cloud NON autorizzati dalla funzione IT (es. Apple iCloud, Dropbox, Google Drive personale, One Drive personale, ecc.)

- Gli incaricati che operano all'esterno dell'azienda e che non hanno la possibilità di utilizzare le risorse di rete, devono richiedere alla funzione IT l'assegnazione di una memoria esterna (chiavetta usb, hard disk esterno, memory card) su cui copiare temporaneamente dei dati oppure da utilizzare per effettuare il backup dei dati presenti in locale sul PC portatile o fisso. La funzione IT valuterà le necessità dell'utente ed eventualmente assegnerà il tipo di dotazione che riterrà più idonea. L'utente dovrà seguire le istruzioni fornite dall'IT per l'utilizzo della memoria ed in particolare per le operazioni di backup. Questi dispostivi dovranno inoltre essere custoditi con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro; dovranno essere utilizzati esclusivamente dalle persone a cui sono stati assegnati e, in nessun caso, devono essere consegnati a terzi. Eventuali perdite di dati legate alla mancata esecuzione del backup saranno di responsabilità dell'utente a cui è stato assegnato il dispositivo.

4.4 Gestione dei dati cartacei

4.4.1 Gestione corretta dei documenti cartacei

Gli incaricati del trattamento, cui sono stati affidati documenti contenenti dati personali, devono conservare tali documenti con le necessarie accortezze e riporli in archivio (comprese eventuali copie) al termine delle operazioni di trattamento.

Si raccomanda di:

- Verificare il funzionamento delle chiusure tramite chiave degli armadi e dei contenitori contenenti i dati di natura sensibile o comunque riservati (anche per la custodia temporanea di documenti)
- Assegnare le chiavi degli armadi/contenitori ai soli incaricati autorizzati, che dovranno conservarle con cura
- Non lasciare documenti all'interno di stampanti, fotocopiatrici o fax
- Non lasciare documenti visibili sulla scrivania (*clean desk policy*) quando ci si allontana dalla stanza o si riceve qualcuno per una riunione
- Se si beneficia di un ufficio personale, chiudere a chiave la stanza quando ci si allontana per pause, riunioni, impegni all'esterno dell'azienda; in alternativa chiudere gli archivi, le cassettiere, ecc.

4.4.2 Documenti particolarmente riservati

I documenti cartacei contenenti dati personali sensibili, giudiziari o ritenuti importanti devono essere protetti e la loro circolazione deve essere ristretta.

Gli utenti autorizzati alla gestione di documenti cartacei contenenti dati personali di categorie particolari (*ex dati sensibili*), giudiziari o ritenuti importanti devono garantire che tali documenti non possano essere visionati da soggetti non autorizzati anche durante l'attività lavorativa avendo cura di non lasciare incustoditi tali documenti presso stampanti, fotocopiatrici o fax e di archiviarli in armadi chiusi a chiave. La circolazione di detta documentazione deve essere ristretta ai soli autorizzati.

4.4.3 Consigli pratici

Qualche esempio e suggerimento pratico per gli utenti di tutte le sedi. Si raccomanda una particolare attenzione a chi opera nelle Filiali, dove gli ambienti sono più piccoli e utilizzati in modo condiviso per esigenze diverse.

- Utilizzare la sala riunioni, laddove presente, per ricevere i clienti e i fornitori
- Se devono essere ricevute persone esterne al proprio tavolo per utilizzare il PC, assicurarsi di non lasciare in vista documenti riservati (offerte, listini, contratti, capitolati di gara, ecc.)
- In generale, riporre le pratiche commerciali alla fine del lavoro negli armadi, cassettiere, archivi
- Attenzione ai dati personali che si annotano sui pacchi (recapiti telefonici, ecc.); inserire solo le informazioni necessarie a gestire la consegna
- Sui banchi vendita non devono essere lasciati documenti con elenchi di contatti, e-mailing, ecc.
- Custodire con la necessaria riservatezza eventuali proposte, capitolati, documenti lasciati dagli installatori per la preparazione di un progetto e preventivo

5 PASSWORD POLICY – USER ACCESSES

5.1 Autenticazione

5.1.1 Composizione delle credenziali di accesso.

Ogni utente, per accedere ai sistemi informatici aziendali deve essere preventivamente identificato ed autenticato, attraverso la verifica delle proprie credenziali. Le credenziali sono costituite da:

- identificativo univoco dell'utente (user-id)
- parola chiave segreta (password).

Le credenziali sono riservate e strettamente personali e vengono assegnate ad ogni dipendente che deve utilizzare una postazione, collegata alla rete informatica aziendale, come strumento di lavoro. Le parole chiave (password) costituiscono 'misure di sicurezza' predisposte in ottemperanza a precisi obblighi di legge. Per questa ragione è vietata la comunicazione a chiunque e a qualunque titolo della stessa; non esistono deroghe a tale previsione, nemmeno nei confronti dei propri diretti responsabili. Il divieto è riferibile a ogni possibile forma di comunicazione delle credenziali di autenticazione, sia di tipo orale che scritta (telefono, e-mail ecc.).

Si ricorda che l'utilizzo del sistema informativo aziendale e di conseguenza l'accesso ai dati, ai programmi ed alle risorse informatiche aziendali è consentito al fine di permettere l'espletamento delle mansioni e/o degli incarichi assegnati e per il tempo occorrente a svolgere tali compiti e mansioni.

5.1.2 Regole di composizione della parola chiave

Entro il termine di scadenza della propria parola chiave, in alcuni casi segnalato in automatico, ogni utente dovrà provvedere, secondo le modalità in uso, all'aggiornamento della parola chiave medesima rispettando le seguenti regole:

- adottare una combinazione di numeri e lettere (alfanumerica) con una lunghezza di almeno 8 caratteri; si consiglia anche l'utilizzo combinato di maiuscole e minuscole e un carattere speciale
- non dovrebbe basarsi su informazioni di carattere personale (nome di familiari, targa dell'auto, data di nascita, parte del proprio nome/cognome, luogo geografico di appartenenza, ecc.)
- non usare un acronimo, un modo di dire comune, un vocabolo dialettale o di slang
- non deve essere una sequenza comune di caratteri come 123456, aaabbb, qwerty, ecc.
- non deve basarsi su terminologie aziendali facilmente individuabili quali il nome dell'azienda e le sue derivazioni o i codici/nomi dei prodotti

In generale, la password deve essere sufficientemente complessa in termini di combinazione di caratteri ma deve essere facilmente ricordabile dall'utente.

Una possibile tecnica è utilizzare sequenze di caratteri prive di senso evidente, ma con singoli caratteri che formano una frase facile da memorizzare, come il titolo di un film, di un libro o di una canzone. Es: I7N0m3de88aR%sa = Il nome della rosa.

5.1.3 Riservatezza della parola chiave

Tutti gli utenti devono assicurare la massima riservatezza della parola chiave; tutte le parole d'accesso devono essere trattate come informazioni sensibili e confidenziali d'impresa, e pertanto si dovranno rispettare le seguenti indicazioni:

- non comunicarla ad alcun altro;
- non rivelare le password nei messaggi e-mail o in altre forme elettroniche di comunicazione
- non rivelare la propria password al telefono a nessuno

- evitare di tenerne traccia scritta;
- digitarla facendo sempre attenzione di non essere osservati da alcuno;
- provvedere immediatamente al suo aggiornamento in caso di violazione della riservatezza, anche solo sospettata

5.1.4 Aggiornamento della parola chiave.

È necessario effettuare l'aggiornamento della parola chiave nei seguenti casi:

- al momento del primo collegamento al sistema informatico (es. rete e server aziendali, applicazioni) per la sostituzione della parola chiave 'iniziale' assegnata, che è solitamente temporanea;
- quando segnalato automaticamente dal sistema (o almeno ogni 90 giorni se gestito manualmente dall'utente);
- tutte le volte si abbia il sospetto o comunque si ritenga che la parola chiave abbia perso i requisiti di riservatezza

Si rammenta che, nell'effettuare l'operazione di aggiornamento della parola chiave, quella nuova dovrà essere composta nel rispetto delle regole definite precedentemente.

L'aggiornamento della parola chiave dovrà essere effettuato su tutti i sistemi operativi o gli applicativi che richiedono l'utilizzo delle credenziali indipendentemente dalla presenza di un sistema di scadenza automatica delle stesse.

5.1.5 Disattivazione delle credenziali utente

Le credenziali di accesso al dominio o agli applicativi saranno disattivate in caso di mancato utilizzo delle stesse per un periodo superiore a sei mesi. Qualora il mancato utilizzo sia legato ad assenze note (per maternità o lungo infortunio), sarà l'Ufficio Personale a darne informazione all'IT.

L'utente dovrà poi chiedere, secondo le modalità attualmente in vigore, la riattivazione delle proprie credenziali alla divisione IT.

5.1.6 Disabilitazione delle autorizzazioni di un utente

Le autorizzazioni di accesso al sistema informatico vengono disabilitate nel caso in cui l'utente non abbia più necessità di accedere a determinate informazioni o servizi in modo da garantire la corrispondenza tra mansione organizzativa svolta e diritti di accesso ai dati.

5.1.7 Accesso ai dati in caso di necessità

In caso di necessità (per esempio assenza improvvisa e prolungata), è previsto che le parole chiave dell'utente vengano resettate e sostituite per consentire l'accesso ai dati da parte di una figura organizzativa autorizzata. Tale necessità viene comunicata all'utente titolare delle credenziali di accesso che dovrà successivamente provvedere, secondo le modalità attualmente in vigore, all'aggiornamento delle medesime.

5.1.8 Gestione della chiusura del rapporto di lavoro

L'Ufficio Personale deve comunicare tutte le variazioni significative degli incarichi dell'utente e/o dello stato di impiego alle funzioni IT, affinché gli operatori preposti possano effettuare le operazioni necessarie sulle utenze.

In seguito alla fine del rapporto di lavoro, si procede con le seguenti attività:

- la user-id viene disabilitata dai Sistemi Informativi aziendali
- la casella di posta elettronica (se nominativa) viene disattivata e cancellato il suo contenuto al massimo entro quindici giorni dalla chiusura del rapporto di lavoro; sarà opportuno quindi effettuare preventivamente i necessari passaggi di consegne e le comunicazioni all'esterno dell'azienda (se del caso) con i riferimenti dei nuovi interlocutori

- se l’utente in uscita utilizzava una casella di posta di tipo funzionale/generico, tale casella sarà resa disponibile al nuovo incaricato
- il contenuto degli strumenti di lavoro può essere valutato dal responsabile dell’utente, che in breve tempo decide se deve essere riutilizzato e quindi riassegnato oppure cancellato, comunicando la scelta a tutti gli uffici di competenza

Si raccomanda all’utente in uscita dall’azienda di non eliminare i dati di proprietà aziendale dal personal computer, mentre è necessario che eventuali dati personali (di natura non lavorativa) non siano presenti sulla strumentazione aziendale che deve essere restituita.

5.1.9 Controlli di sicurezza

Nell'ambito delle attività riguardanti la tutela della sicurezza della infrastruttura tecnologica, l'azienda potrebbe effettuare analisi periodiche sulle password degli utenti al fine di verificarne la solidità, le policy di gestione e la durata, informandone preventivamente gli utenti stessi.

Nel caso in cui l'audit abbia, tra gli esiti possibili, la decodifica della password, questa viene bloccata e all'Incaricato sarà richiesto di sostituirla con una più sicura.

5.2 E-MAIL POLICY

5.2.1 Posta elettronica – Regole Generali

- La posta elettronica è un mezzo di comunicazione di proprietà dell'azienda, assegnato all'incaricato per lo svolgimento delle proprie mansioni.
- In generale un messaggio di posta elettronica inviato da un indirizzo di posta qualificato da nome.cognome@nomeazienda, oppure funzione@nomeazienda viene percepito come contenente informazioni, notizie, opinioni di carattere ufficiale proveniente dall'azienda. Di conseguenza l'uso della posta elettronica dovrà essere considerato alla pari dell'uso della carta intestata aziendale.
- Ciascuno è responsabile del contenuto delle proprie comunicazioni, anche per quanto riguarda la riservatezza dei dati in esse trattati: una diffusione impropria potrebbe configurarsi come violazione di segreto aziendale o trasgressione di normative vigenti.
- L'uso personale della casella di posta elettronica aziendale non è consentito. Qualsiasi informazione di natura personale non deve transitare dai server di posta della società, che possono essere soggetti a controlli durante le attività di manutenzione o in caso di anomalie, guasti o interventi legati alla sicurezza; gli utenti non potranno quindi avere aspettative di privacy rispetto alle informazioni inviate, ricevute o memorizzate. In caso di ricezione di posta personale sulla casella aziendale, l'utente dovrà cancellare immediatamente ogni messaggio.
- Si ricorda che l'azienda mette a disposizione degli indirizzi di posta "di funzione" condivisi tra più lavoratori, affiancandoli a quelli individuali. Se ne consiglia l'utilizzo per gestire tutte quelle comunicazioni che devono essere condivise all'interno del gruppo di lavoro.

5.2.2 Posta elettronica – Sicurezza

- Non è autorizzata la configurazione sul computer aziendale del proprio account di posta personale (es. sul proprio client Outlook, Mozilla, ecc.,). È possibile invece consultare la propria casella di posta personale attraverso applicazioni Webmail (es. Gmail, Yahoo, Libero, Fastweb, ecc.) rispettando comunque le modalità di utilizzo della rete definite con la presente procedura. È altresì permesso accedere al proprio account di posta attraverso lo smartphone (o analogo device) aziendale, sempre nei limiti di un minimo impegno che non impatti sull'attività lavorativa e sulla propria efficienza e produttività. Si ricorda che l'email personale NON dovrà MAI essere utilizzata per trattare dati aziendali.
- L'azienda ha adottato numerosi sistemi di protezione della posta elettronica dai virus e dalle attività di spamming. Si coglie comunque l'occasione per ribadire alcuni fondamentali norme per un corretto uso della posta elettronica:
    a. Gli utenti non devono aprire allegati di posta elettronica di cui non si conosca con certezza il mittente o sulla sicurezza dei quali si nutrono anche minimi dubbi.
    b. Non inoltrare ad alcuno i messaggi contenenti notizie false di allarmi o appelli di cui si chiede la diffusione.
    c. Non creare, archiviare e spedire, all'interno e all'esterno del dominio aziendale, messaggi pubblicitari o promozionali non connessi con lo svolgimento dell'attività lavorativa
    d. Non effettuare comunicazioni massive attraverso il proprio client di posta elettronica, ma utilizzare unicamente gli appositi strumenti dedicati all'e-mail marketing (rivolgersi alla funzione IT in caso di necessità)
    e. Non rispondere a messaggi apparentemente provenienti da mittenti considerati "sicuri" (es. banca, posta, spedizionieri, ecc.) e soprattutto non fornire alcun dato personale richiesto all'interno di queste e-mail **né collegarsi ad eventuali link proposti nel messaggio**.
- In tutte le situazioni sopra descritte, nel caso sussista qualche dubbio su come gestire il messaggio, si ricorda di non aprire né il messaggio né l'eventuale allegato, e contattare le funzioni IT.

- È necessario archiviare in modo sicuro i messaggi di posta elettronica che possono impegnare l'azienda con terze parti ovvero che abbiano un qualunque valore legale. Si ricorda che è possibile mantenere tali messaggi sul server di posta, ma tale pratica non ne garantisce le caratteristiche di autenticità, integrità, affidabilità. Si consiglia in questi casi di contattare le funzioni IT per valutare l'eventuale necessità di sistemi più idonei alla conservazione sicura, quali quelli di gestione documentale.

5.2.3 Posta elettronica – Gestione delle assenze

Sulla base di quanto esplicitato in precedenza, si precisa che:

a. Il contenuto dei messaggi di posta in entrata/uscita potrebbe essere visionato dal Titolare (attraverso apposito personale incaricato), in caso di assenza imprevista e prolungata del lavoratore, se questo fosse necessario per la continuità dell'attività lavorativa.
b. In caso di assenza prolungata e prevista, sarebbe buona norma attivare il servizio di risposta automatica. L'azienda ha messo a disposizione di ciascun lavoratore apposite funzionalità (i cosiddetti avvisi "out of office" o "regola fuori sede") attraverso le quali si possono spedire automaticamente le coordinate (telefoniche o elettroniche) di un collega o di una struttura alternativa a cui rivolgersi. Si sollecitano quindi tutti gli utenti ad usufruire di tali servizi, prevenendo quindi la possibilità che la propria posta elettronica debba essere consultata da altri soggetti.
c. In alternativa e in tutti i casi in cui sia necessario un presidio della casella di posta per particolari ragioni di operatività aziendale, l'utente potrà identificare un "fiduciario" che in sua assenza possa verificare i messaggi di posta ed inoltri eventualmente i contenuti necessari a chi ne avesse urgenza.
d. In caso di mancata identificazione del fiduciario, il responsabile gerarchico è autorizzato ad accedere al contenuto dei messaggi o a far impostare il risponditore automatico, attraverso apposito personale incaricato. L'utente sarà informato dell'avvenuto accesso alla sua casella di posta, alla prima occasione utile.
e. Nel caso in cui la propria posta sia stata consultata da terzi durante la propria assenza (secondo quanto illustrato in precedenza), la password di accesso dovrà essere modificata dall'utente al rientro in azienda.

6 INTERNET POLICY

6.1.1 Internet – Regole Generali

La connettività dei sistemi verso le reti pubbliche è fornita al fine di svolgere al meglio la propria attività lavorativa.

Uno sporadico utilizzo personale è accettato esclusivamente durante gli orari non lavorativi (es. in pausa pranzo), entro limiti di tempo ridotti al minimo, paragonabili ad altre consuetudini di comunicazione all'interno del posto di lavoro, e nel rispetto delle presenti linee guida, di tutte le altre procedure e policy aziendali e della normativa vigente.

6.1.2 Internet – Regole di navigazione sicura

Come richiesto dalla normativa sulla protezione dei dati personali, l'azienda deve promuovere ogni opportuna misura organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri dei sistemi aziendali. In generale, prevenire gli abusi deve essere considerato più importante che individuarli, e quindi devono essere preferite le misure PREVENTIVE rispetto a seguenti azioni REPRESSIVE.

Considerando questi principi, l'azienda ha adottato alcune misure di sicurezza sia organizzative che tecnologiche, ed ha in particolare:

1) Individuato le tipologie di utenti ai quali, per necessità legate alla propria professione, è concesso l'uso della posta elettronica e/o di Internet.
2) Installato da tempo alcuni dispositivi informatici che permettono di ridurre il rischio di violazione della propria rete dall'esterno
3) Installato dispositivi che limitano e contrastano eventuali usi impropri o pericolosi della "navigazione" in Internet. In particolare, sono sempre bloccati i siti pericolosi, con riferimento a black list che si aggiornano costantemente e includono categorie quali pornografia, pedofilia, violenza, pirateria informatica, violazione diritto d'autore, hacking e cracking, peer-to-peer, ecc. Inoltre, durante l'orario lavorativo può essere inibito l'accesso anche ad alcune categorie di siti non pertinenti all'attività professionale, e che possono influire significativamente sull'efficienza della banda (web mail, social network, shopping, instant messaging).

I sistemi utilizzati garantiscono un buon livello di protezione della rete aziendale rispetto a comportamenti illeciti; si ricordano in ogni caso alcune fondamentali regole:

a) È vietato collegarsi a siti quali le WebChat, i siti che propongono software protetto da copyright e attività illecite in generale.
b) È vietato scaricare e/o installare autonomamente sulla propria postazione software di qualunque genere.
c) È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute dell'utente poiché potenzialmente idonea a rivelare dati di natura sensibile.
d) Non è consentita ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa; non è consentita la partecipazione, per motivi non professionali, a forum, chat o gruppi di discussione.
e) È vietato effettuare ogni genere di transazione finanziaria di tipo personale, comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dal Titolare e con il rispetto delle normali procedure di acquisto.

Gli utenti che usufruiscono del servizio di connettività e navigazione Internet aziendale sono comunque informati del fatto che Fogliani dispone di strumenti, necessari per la sicurezza dei sistemi informatici, dei dati e del know-how, che registrano gli indirizzi dei siti visitati e l'indirizzo della postazione (IP) e che quindi potrebbero essere impiegati per accertare eventuali comportamenti contrari alle politiche di utilizzo di Internet e degli strumenti aziendali.

7 VERIFICHE E CONTROLLI

Fogliani e le altre società controllate, in qualità di Titolare dei dati e degli strumenti informatici utilizzati nei trattamenti, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

1. Tutelare la sicurezza della rete aziendale e l'integrità degli strumenti informatici e dei dati.
2. Evitare la commissione di illeciti, mettere in atto misure preventive o difensive
3. Verificare la funzionalità del sistema e degli strumenti informatici

Le attività di controllo potranno avvenire anche attraverso appositi audit tecnici o di processo, oppure a mezzo di Vulnerability Assesment del sistema informatico. Per tali controlli l'organizzazione si riserva di avvalersi di soggetti esterni.

Si precisa, in ogni caso, che l'organizzazione non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1970), tra cui sono comprese le strumentazioni hardware e software mirate al controllo dell'utente.

7.1 Modalità di verifica

Nel caso in cui un evento dannoso o una situazione di pericolo per la sicurezza aziendale non sia stato bloccato dagli accorgimenti tecnici adottati, l'azienda può adottare eventuali misure che consentano la verifica di comportamenti anomali.

Le verifiche saranno comunque rispettose dei principi fondamentali di pertinenza e non eccedenza, e saranno effettuate di regola in questo modo:

1. rilevazione dell'evento dannoso → verifica anonima su dati aggregati → avviso generalizzato (aziendale o a gruppi di lavoro)
2. ripetersi dell'evento dannoso → verifica su gruppi di postazioni/nominativi → avviso/richiamo al gruppo controllato
3. ripetersi dell'evento dannoso → verifica individuale → avviso/richiamo nominativo

Le informazioni registrate o registrabili automaticamente dai sistemi (log di navigazione Internet o del server di posta elettronica) sono accessibili solo dalle funzioni IT di Fogliani, formalmente autorizzate.

Tali incaricati svolgeranno solo le operazioni strettamente necessarie al perseguimento delle finalità tecniche e di sicurezza.

7.2 Informativa art. 13 Regolamento UE

Eventuali dati personali o appartenenti a categorie particolari, rinvenuti su strumenti elettronici di proprietà aziendale, anche se detenuti o conservati in violazione al presente regolamento, saranno comunque trattati secondo i criteri di confidenzialità previsti dalla legge, unicamente per le finalità legate all'attività di controllo e/o di eventuale tutela giudiziaria dell'azienda.

I sistemi software sono configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.
Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione:

1. Ad esigenze tecniche o di sicurezza del tutto particolari;
2. All'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
3. All'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

7.3 Sanzioni

Ognuno sarà ritenuto personalmente responsabile in caso di deliberata trasgressione delle suddette regole, secondo le norme di legge e contratto applicabili, anche di natura disciplinare.

Eventuali sanzioni:

1. Biasimo verbale
2. Lettera di richiamo inflitto per iscritto;
3. Multa;
4. Sospensione dalla retribuzione e dal servizio;
5. Licenziamento disciplinare e con le altre conseguenze di ragioni e di legge;

Per i dirigenti valgono le vigenti norme di legge e/o di contrattazione collettiva, fermo restando che, per le violazioni di maggior gravità l'ente potrà procedere al licenziamento del dirigente autore dell'infrazione.