asbr
Azienda Servizi Bassa Reggiana
www.asbr.it

DISPOSIZIONI ATTUATIVE PER L'UTILIZZO DEGLI STRUMENTI INFO-TELEMATICI

SOMMARIO

1. SEZIONE I: AMBITO GENERALE

1.1. Premessa

L'ambito lavorativo porta la nostra organizzazione a gestire una serie di "informazioni", proprie e di terzi, per poter erogare i servizi che le vengono istituzionalmente richiesti.
Tali informazioni possono essere considerate, ai sensi del D. Lgs. 196/2003 e s.m.i. e del GDPR, "dati personali" quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che l'Azienda adotti una serie di misure minime ed idonee previste dalle norme.
Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "informazioni riservate", ovvero informazioni tecniche, commerciali, contrattuali o di altro genere per le quali l'organizzazione è chiamata a garantire la riservatezza.
Ai fini di queste Disposizioni si specifica pertanto che con il termine "dati" deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge.
In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui l'incaricato/a viene a conoscenza nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l'organizzazione stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita dell'Azienda.
Anche tra colleghi/e, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.
L'accesso alla rete internet dal computer o dai dispositivi aziendali, espone l'Azienda a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'Azienda stessa.
Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, l'Azienda ha adottato le presenti Disposizioni Attuative, dirette ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.
Le presenti Disposizioni Attuative si applicano ai/le dipendenti e/o consulenti (di seguito anche "incaricati") che si trovino ad operare con dati dell'Azienda.
L'uso dei COMPUTER e di altre attrezzature elettroniche (di seguito DISPOSITIVI), nonché dei servizi internet e della posta elettronica difforme dalle regole contenute nelle presenti Disposizioni potrebbe esporre l'Azienda ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico, mettendo a repentaglio la sicurezza personale degli utenti.
Le informazioni contenute nelle presenti Disposizioni Attuative vengono rilasciate ai sensi dell'art. 13 del Regolamento Europeo 679/2016, e costituiscono, quindi, parte integrante dell'informativa rilasciata agli Incaricati

1.2. Esclusione all'uso degli strumenti informatici

All'inizio del rapporto lavorativo o di consulenza, l'Azienda valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari dispositivi aziendali, di internet e della posta elettronica da parte dei soggetti incaricati.
Successivamente, e periodicamente, l'Azienda valuta la permanenza dei presupposti per l'utilizzo dei dispositivi aziendali, di internet e della posta elettronica.
È fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici aziendali.
Più specificatamente, hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo i/le dipendenti incaricati/e che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.

1.3. Titolarità dei dispositivi e dei dati

L'Azienda è esclusiva titolare e proprietaria dei dispositivi messi a disposizione dei soggetti incaricati, ai soli fini dell'attività lavorativa.
L'Azienda è l'unico esclusivo titolare e proprietario di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri dispositivi digitali o archiviati in modo cartaceo nei propri locali.
Il titolare non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei dispositivi aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i *file* di immagini, i *file* di filmati o altre tipologie di *file*) siano privati o personali.

1.4. Finalità nell'utilizzo dei dispositivi

I dispositivi assegnati sono uno strumento lavorativo nelle disponibilità dell'incaricato/a esclusivamente per finalità connesse allo svolgimento del rapporto di lavoro. I dispositivi, quindi, non devono essere utilizzati per finalità private e diverse da quelle istituzionali, se non eccezionalmente e nei limiti evidenziati dalle presenti Disposizioni Attuative.
Qualsiasi eventuale tolleranza da parte di questa Azienda, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nelle presenti Disposizioni Attuative.

1.5. Restituzione dei dispositivi

A seguito di una cessazione del rapporto lavorativo o di consulenza con l'Azienda o, comunque, al venir meno, ad insindacabile giudizio dell'Azienda, della permanenza dei presupposti per l'utilizzo dei dispositivi aziendali, i soggetti Incaricati hanno i seguenti obblighi:

1. procedere immediatamente alla restituzione dei dispositivi in uso, secondo le procedure aziendali in essere.
2. divieto assoluto di formattare o alterare o manomettere o distruggere i dispositivi, assegnati o rendere inintelligibili i dati in essi contenuti, tramite qualsiasi processo.
3. divieto di esportare, copiare, inviare a terzi i dati e le informazioni contenute nel dispositivo.

2. SEZIONE II: PASSWORD

2.1. Le Password

Le password possono essere un metodo di autenticazione assegnato dall'organizzazione per garantire l'accesso protetto ad uno strumento hardware, oppure ad un applicativo software.
La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi/e e all'Azienda nel suo complesso. Nel tempo, anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle almeno ogni 3 mesi o quando richiesto dal Sistema.
L'Azienda dove possibile ha implementato degli automatismi che obbligano gli utenti a gestire le password in modo corretto, in particolare, per quanto riguarda le password di accesso ad ogni dispositivo utilizzato. Password che vengono aggiornate periodicamente secondo il livello di sicurezza richiesto dall'Azienda stessa e, comunque, in linea con quanto richiesto dalla normativa privacy.
Altra buona norma è quella di non memorizzare la password su supporti facilmente intercettabili da altre persone. Il miglior luogo in cui conservare una password è la propria memoria.
In qualsiasi momento, l'organizzazione si riserva il diritto di revocare ai soggetti Incaricati il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

2.2. Regole per la corretta gestione ed utilizzo delle password

Il soggetto cui è assegnato un dispositivo, sia esso fisso o mobile oppure l'accesso a un software e/o ad un applicazione web, per una corretta e sicura gestione delle proprie password, deve rispettare le regole seguenti:

a) la password deve essere abbastanza lunga: almeno 8 caratteri, anche se più aumenta il numero dei caratteri più la password diventa "robusta" (si suggerisce intorno ai 15 caratteri);

b) la password deve contenere caratteri di almeno 4 diverse tipologie, da scegliere tra: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (per caratteri speciali si intendono, per esempio, i seguenti: { } [ ], . < > ; : ! " £ $ % & / ( ) = ? ^ \ | ' * - + , ecc.);
c) la password non deve contenere riferimenti personali facili da indovinare (nome, cognome, data di nascita, ecc.); non deve nemmeno contenere riferimenti al nome utente (detto anche user account, alias, user id, user name);
d) meglio evitare che la password contenga parole "da dizionario", cioè parole intere di uso comune: è meglio usare parole di fantasia oppure parole "camuffate" per renderle meno comuni, magari interrompendole con caratteri speciali (ad esempio: caffè può diventare caf-f3); esistono infatti software programmati per tentare di indovinare e rubare le password provando sistematicamente tutte le parole di uso comune nelle varie lingue, e con questa accortezza si può rendere il loro funzionamento più complicato;
e) la password andrebbe periodicamente cambiata, soprattutto per i profili più importanti o quelli che usi più spesso (e-mail, e-banking, social network, ecc.);
f) occorre cambiare immediatamente una password, non appena si abbia un dubbio che sia diventata poco "sicura" o che abbia perso la necessaria segretezza;
g) utilizza password diverse per account diversi (e-mail, social network, servizi digitali di varia natura, ecc.); in caso di «furto» di una password si evita così il rischio che anche gli altri profili che ti appartengono possano essere facilmente violati;
h) non utilizzare credenziali (user-id e password) di altri utenti, nemmeno se fornite volontariamente o se pervenute casualmente a conoscenza;
i) non utilizzare per lo stesso account password già utilizzate in passato;
j) cambiare immediatamente le eventuali password temporanee rilasciate da un sistema o da un servizio informatico, scegliendone una personale;
k) non scrivere mai le password su biglietti che poi magari conservi nel portafoglio o indosso, o che puoi distrattamente lasciare in giro, oppure in file non protetti sui tuoi dispositivi personali (computer, smartphone o tablet);
l) evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'Azienda; in alcuni casi, sono implementati meccanismi che consentono all'incaricato/a un numero limitato di tentativi errati di inserimento della password, oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato per alcuni minuti. In caso di necessità, contattare il Titolare.
m) evitare sempre di condividere le password via e-mail, sms, social network, instant messaging, ecc.; anche se comunicate a persone conosciute, le credenziali potrebbero essere diffuse involontariamente a terzi o «rubate» da malintenzionati;
n) in caso di utilizzo di pc, smartphone e altri dispositivi che non appartengono all'Azienda, evitare sempre che possano conservare in memoria le password utilizzate.

2.3. Alcuni esempi di password non ammesse

La password ideale deve essere complessa, senza alcun riferimento, ma facile da ricordare. Una possibile tecnica è usare sequenze di caratteri prive di senso evidente, ma con singoli caratteri che formano una frase facile da memorizzare (es.: "NlMzz5DlCmm!", Nel Mezzo Del Cammin, più il carattere 5 e il punto esclamativo). Decifrare una parola come questa può richiedere giorni, una come "radar" meno di dieci secondi. Alcuni esempi di password assolutamente da evitare:

1. Se Username="mariorossi", password="mario", o ancora peggio, password="mariorossi".
2. Il nome della moglie/marito, fidanzato/a, figli, ecc. anche a rovescio!
3. La propria data di nascita, quella del coniuge, ecc.
4. Targa della propria auto.
5. Numero di telefono proprio, del coniuge, ecc.
6. Parole comuni tipo "Kilimangiaro", "Password", "Qwerty", "12345678" (troppo facili).
7. Qualsiasi parola del vocabolario (di qualsiasi lingua diffusa, come inglese, italiano, ecc.) che non sia stata "alterata" come negli esempi che precedono.

2.4. La password nei sistemi

Ogni Incaricato/a può variare la propria password di accesso a qualsiasi sistema aziendale in modo

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

2.5. Audit delle password

Nell'ambito delle attività riguardanti la tutela della sicurezza della infrastruttura tecnologica, l'Azienda potrebbe effettuare analisi periodiche sulle password degli Incaricati al fine di verificarne la solidità, le policy di gestione e la durata, informandone preventivamente i soggetti stessi.
Nel caso in cui l'audit abbia, tra gli esiti possibili, la decodifica della password, questa viene bloccata e richiesto all'incaricato/a di cambiarla.

3. SEZIONE III: OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

In questa sezione vengono trattate le operazioni a carico dell'Incaricato/a e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio aziendale.

3.1. Login e Logout

Il "Login" è l'operazione con la quale l'Incaricato/a si connette al sistema informativo aziendale o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'Account), aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet, ecc.), ognuno dei quali richiede uno username e una password.
Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. 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.
Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla.

3.2. Obblighi

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.
L'incaricato/a deve quindi eseguire le operazioni seguenti:

1. se si allontana dalla propria postazione, dovrà mettere in protezione (bloccare) il suo dispositivo affinché persone non autorizzate non abbiano accesso ai dati protetti ed alle informazioni aziendali;
2. chiudere la sessione (Logout) a fine giornata;
3. spegnere il PC dopo il Logout, salvo diverse e temporanee indicazioni dell'Azienda;
4. controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo dispositivo.

4. SEZIONE IV: USO DEL PERSONAL COMPUTER AZIENDALI (FISSI E PORTATILI)

4.1. Modalità d'uso del COMPUTER aziendale

Il sistema informativo aziendale è composto da un insieme di unità (server centrali e/o in cloud e client) connessi ad una rete locale (LAN e/o WAN), che utilizzano diversi sistemi operativi e applicativi.
I file creati, elaborati o modificati sul computer assegnato devono essere poi sempre salvati a fine giornata sul sistema di repository documentale centralizzato.
L'Azienda non effettua il backup dei dati memorizzati in locale.

4.2. Corretto utilizzo del COMPUTER aziendale

Il computer consegnato all'Incaricato/a è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla

sicurezza.
Per necessità aziendali, gli amministratori di sistema utilizzando il proprio login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente documento, sia alle memorie di massa locali di rete (repository e backup) che ai server aziendali nonché, previa comunicazione al/la dipendente, potranno accedere al computer, anche in remoto.
In particolare, i soggetti Incaricati devono adottare le seguenti misure:

1. utilizzare solo ed esclusivamente le aree di memoria della rete dell'Azienda indicate agli utenti dagli amministratori di sistema ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri file fuori dalle unità di rete.
2. spegnere il computer o curarsi di effettuare il Logout ogni sera prima di lasciare gli uffici, poiché lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi, senzachevisialapossibilità di provarne in seguito l'indebito uso.
3. mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), stabiliti dall'Azienda.
4. nel caso di uso condiviso di un computer aziendale con altri utenti, accedere sempre allo stesso con le proprie credenziali e al termine della propria sessione di lavoro effettuare il logout.

Risulta opportuno, inoltre che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

4.3. Divieti Espressi sull'utilizzo del COMPUTER

Al soggetto Incaricato/a è vietato:

1. la gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere;
2. modificare le configurazioni già impostate sul personal computer;
3. utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta dell'Azienda;
4. installare software senza espressa autorizzazione dell'Azienda o di cui l'Azienda non possieda la licenza. È, peraltro, vietato fare copia dei software installati sui computer aziendali al fine di farne un uso personale;
5. caricare sul disco fisso del computer o nel server documenti, giochi, file musicali o audiovisivi o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate o che violano le regole sul diritto d'autore;
6. aggiungere o collegare dispositivi hardware o periferiche (ad esempio hard disk, memorie flash, telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell'Azienda;
7. creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'organizzazione, quali per esempio virus, trojan horses e malware in genere.
8. accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte;
9. effettuare in proprio attività manutentive;
10. permettere attività manutentive da parte dei soggetti non espressamente autorizzati dell'organizzazione.

4.4. ANTIVIRUS

I virus (per essere precisi, il malware, il software malevolo) possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, ecc.…
L'Azienda impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.
L'Incaricato/a, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer e, in particolare, deve rispettare le regole seguenti:

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

Inoltre, all'Incaricato/a:

1. è vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione;
2. è vietato ostacolare l'azione dell'antivirus aziendale;
3. è vietato disattivare l'antivirus senza l'autorizzazione espressa dell'Azienda, anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer;
4. è vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani (c.d. phishing);
5. in ogni caso è necessario contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

5. SEZIONEV: INTERNET

5.1. Internet è uno strumento di lavoro

La connessione alla rete internet dal dispositivo avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. E' consentita, previa autorizzazione del Dirigente responsabile, la consultazione occasionale di siti internet per finalità non istituzionali.
È vietato l'accesso a caselle webmail di posta elettronica personale.

5.2. Misure preventive per ridurre navigazioni illecite

L'organizzazione potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.

5.3. Divieti Espressi concernenti Internet

- È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute del soggetto incaricato poiché potenzialmente idonea a rivelare dati particolari ai sensi del GDPR.
- È fatto divieto di accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, della condizione di disabilità.
- È vietato all'Incaricato/a lo scarico (download) di software (anche gratuito) prelevato da siti Internet.
- È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria, ivi 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.
- È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa con i dispositivi e le utenze aziendali.
- È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'Azienda, salvo specifica autorizzazione dell'Azienda stessa.
- È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
- È vietato al soggetto incaricato promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale.
- È vietato accedere dall'esterno alla rete interna dell'organizzazione, salvo che con le specifiche procedure previste dall'Azienda stessa.
- È vietato, infine, creare siti web personali sui sistemi dell'organizzazione, nonché acquistare beni o servizi su Internet, a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.

Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e particolari, è posta sotto la personale responsabilità del

soggetto incaricato inadempiente.

5.4. Divieti di Sabotaggio

È vietato accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'Azienda per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

5.5. Diritto d'autore

È vietato utilizzare l'accesso ad Internet, in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, D. Lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, …).
È vietato conservare nei supporti di memorizzazione aziendale materiale che violi il copyright.

5.6. Utilizzo dei Social Network

È vietato l'utilizzo di social networks riferibili agli account aziendali per la promozione e diffusione di contenuti non inerenti all'attività aziendale o che ne possano ledere l'immagine.

Al fine di assicurare il rispetto del segreto d'ufficio, del segreto professionale e della riservatezza dei dati conosciuti in ambito aziendale, è vietato l'uso, anche privato, dei social network per lo scambio di informazioni e dati inerenti all'attività istituzionale.

6. SEZIONE VI: POSTA ELETTRONICA

6.1. La Posta Elettronica è uno strumento di lavoro

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa.
È vietato l'uso per motivi personali della posta elettronica aziendale.
Le caselle e-mail possono essere nominative (es: nome.cognome) o di natura impersonale (tipo info, Azienda, segreteria, direttore, collaboratore, consulenza, …) proprio per evitare ulteriormente che il destinatario delle mail possa considerare l'indirizzo assegnato al/la dipendente "privato".
I soggetti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

6.2. Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica

In caso di ricezione sulla e-mail aziendale di posta personale (nonostante il divieto dell'uso personale della posta elettronica aziendale), è necessario cancellare immediatamente ogni messaggio, al fine di evitare ogni eventuale e possibile back up dei dati ed è necessario chiedere al mittente di non utilizzare e-mail aziendale per le future comunicazioni di carattere personale.

6.3. Divieti Espressi

1. È vietato utilizzare l'indirizzo di posta elettronica contenente il nome di dominio dell'organizzazione per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa.
2. È vietato scrivere e generare messaggi di posta elettronica utilizzando l'indirizzo aziendale, diretti a destinatari esterni all'organizzazione, senza utilizzare il disclaimer indicato ed impostato dall'azienda afferente gli avvisi in caso di invio a destinatario errato.
3. È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.
4. È vietato trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un'intera divisione) senza l'autorizzazione necessaria.
5. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.
6. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni alll'Azienda informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia

necessario in ragione delle mansioni svolte.

7. È vietato utilizzare la posta elettronica o altri servizi internet (gratuiti o a pagamento) per il trasferimento di file di grandi dimensioni: in questi casi dovranno essere utilizzati gli strumenti di condivisione indicati dall'azienda.
8. È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico, che abbia contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, della disabilità. Qualora il soggetto Incaricato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'Azienda.

6.4. Utilizzo della Posta elettronica aziendale e scambio di dati particolari e/o informazioni riservate

È vietato riportare dati particolari ed informazioni riservate nel corpo di testo della e-mail.
L'invio di documenti contenti dati particolari e/o informazioni riservate deve avvenire esclusivamente mediante condivisione sicura con l'impiego degli strumenti messi a disposizione dall'Azienda che permettano la lettura al destinatario tramite autenticazione.

6.5. Posta Elettronica in caso di assenze programmate ed assenze non programmate

Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di adeguatezza, pertinenza e di proporzionalità, l'assegnatario/a della casella di posta elettronica aziendale, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede), deve impostare il messaggio di risposta automatica contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura/servizio ed attivare, eventualmente, l'inoltro del messaggio verso i predetti contatti.
In alternativa, e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, il soggetto incaricato deve nominare un/a collega fiduciario con lettera scritta che in caso di assenza inoltri i file necessari a chi ne abbia urgenza.
Qualora il soggetto assegnatario non abbia provveduto ad individuare un/a collega fiduciario o questi sia assente o irreperibile, o l'assenza non sia programmata, l'organizzazione, mediante personale appositamente responsabile, potrà verificare il contenuto dei messaggi di posta elettronica dell'assegnatario, informandolo e redigendo apposito verbale.

7. SEZIONE VII: USO DI ALTRI DISPOSITIVI (TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELETTRONICI)

7.1. L'utilizzo del tablet o smartphone.

Il tablet e/o lo smartphone (di seguito generalizzati in "dispositivi mobili") possono venire concessi in uso dall'organizzazione ai soggetti incaricati che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'organizzazione.
Il soggetto incaricato è responsabile dei dispositivi mobili assegnatigli dall'organizzazione e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai dispositivi mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare, i file creati o modificati sui dispositivi mobili, devono essere trasferiti sulle memorie di massa aziendali al primo rientro in ufficio.
Sui dispositivi mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'Azienda. I dispositivi mobili utilizzati all'esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto dei dispositivi mobili, deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente l'Azienda che provvederà – se del caso – ad occuparsi delle procedure connesse alla

privacy (gestione Data Breach).
Ai soggetti incaricati non è consentito lasciare incustoditi i dispositivi mobili.
I dispositivi mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso o altro sistema di identificazione biometrica e non possono essere lasciati privi di PIN.
Laddove il dispositivo mobile sia accompagnato da un'utenza con contratto di servizi a consumo, il soggetto incaricato è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, …) e a rispettarli. Qualora esigenze lavorative richiedessero requirements differenti, il soggetto incaricato è tenuto ad informare tempestivamente e preventivamente l'Azienda.
In relazione alle utenze mobili, salvo autorizzazione dell'organizzazione, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione dell'organizzazione, gli utilizzi all'estero devono essere preventivamente comunicati all'organizzazione per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

7.2. Utilizzo e conservazione dei supporti rimovibili (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc.)

Ai soggetti Incaricati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, cd-rom, ecc.…) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, schede dati …).
Esaurite le esigenze che hanno permesso un utilizzo temporaneo del supporto removibile, l'incaricato/a deve trasferire i contenuti aggiornati sui sistemi aziendali e cancellare in modo irreversibile i dati dal supporto medesimo
Al fine di assicurare la effettiva cancellazione dei dati contenuti nei supporti aziendali, ciascun utente dovrà seguire le procedure ed indicazioni fornite dal Servizio Informatico.
Tutti i supporti rimovibili forniti dall'Azienda, contenenti dati personali e particolari nonché informazioni costituenti patrimonio aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.
Al fine di assicurare la effettiva distruzione e/o inutilizzabilità di supporti magnetici rimovibili aziendali, l'incaricato/a deve essere autorizzato dal proprio responsabile a contattare il personale del Servizio Informatico e seguire le istruzioni da questo ultimo impartite.

7.3. Utilizzo di telefoni, fax, scanner e fotocopiatrici

Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di necessità ed urgenza. Qualora venisse assegnato un cellulare aziendale all'Interessato, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo degli altri supporti aziendali: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa.
È vietato l'utilizzo dei fax aziendali, delle fotocopiatrici aziendali, di scanner aziendali per fini personali. Il controllo sul corretto utilizzo degli strumenti in parola è affidato al Coordinatore del soggetto incaricato a cui detti strumenti sono stati assegnati.
L'utilizzo del telefono o di altro strumento di comunicazione personale in orario di servizio deve essere limitato ai casi di urgenza ed indifferibilità, che non consentono di effettuare la comunicazione dopo la fine dell'orario di lavoro.

7.4. Dispositivi personali (BYOD - Bring Your Own Device).

Ai/le dipendenti non è permesso svolgere la loro attività su PC fissi, portatili ed altri dispositivi personali, fatte salve specifiche autorizzazioni dell'Azienda rilasciate in occasione e per lo svolgimento del lavoro agile e/o di prestazioni lavorative flessibili.
E' vietata la connessione dei propri dispositivi personali alla rete Wi-Fi dell'Azienda. E' consentita la

connessione alla rete dedicata agli "ospiti", ove sia disponibile.
I soggetti non dipendenti (ovvero i/le consulenti e collaboratori esterni), possono utilizzare la rete aziendale per collegare i propri dispositivi personali solo se espressamente autorizzati dall'Azienda e secondo le disposizioni da questa indicate.

7.5. Distruzione dei dispositivi

Ogni dispositivo ed ogni memoria esterna affidati ai soggetti incaricati (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all'Azienda, che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.
In particolare, l'Azienda provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

8. SEZIONE VIII: SISTEMI IN CLOUD

8.1. Cloud Computing

In informatica con il termine inglese "cloud computing" (in italiano "nuvola informatica") si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on demand attraverso Internet a partire da un insieme di risorse preesistenti e configurabili.
Utilizzare un servizio di cloud computing per memorizzare dati personali o particolari, espone l'Azienda a potenziali problemi di violazione della privacy. I dati personali vengono memorizzati nelle server farms di aziende che spesso risiedono in uno stato diverso da quello dell'Azienda. Il cloud provider, in caso di comportamento scorretto o malevolo, potrebbe accedere ai dati personali per eseguire ricerche di mercato e profilazione degli utenti. Con i collegamenti wireless, il rischio sicurezza aumenta e si è maggiormente esposti ai casi di pirateria informatica a causa della minore sicurezza offerta dalle reti senza fili. In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per l'Azienda, con difficoltà di raggiungere soluzioni giuridiche e/o rimborsi se il fornitore risiede in uno stato diverso da paese dell'utente.

8.2. Utilizzo di sistemi cloud

È vietato ai dipendenti l'utilizzo di sistemi cloud non espressamente approvati dall'Azienda.

9. SEZIONE IX: CONTROLLO E VERIFICA

9.1. Il controllo

L'Azienda, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

- tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.
- evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo.
- verificare la funzionalità del sistema e degli strumenti informatici.
- tutelare il patrimonio aziendale.

Le attività di controllo potranno avvenire anche con audit e 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) dirette a controllare la produttività e l'efficienza nello svolgimento dell'attività lavorativa, tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente.
Sono legittime, invece, le attività di controllo attinenti a condotte estranee alla prestazione lavorativa o dirette all'accertamento di comportamenti illeciti diversi dal mero inadempimento della prestazione

lavorativa.

9.2. Modalità di verifica

ASBR, in ossequio ai principi di cui all'art. 5 del GDPR, promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili ai soggetti incaricati e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.
L'Azienda non adotta sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.
In particolare, eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte dei soggetti incaricati avvengono nel rispetto del principio di pertinenza e adeguatezza, con esclusione di registrazioni o verifiche con modalità sistematiche.
Resta ferma in ogni caso la necessaria esplicazione delle attività di accertamento posta in essere dal datore di lavoro (o da personale da questi autorizzato), mediante modalità non eccessivamente invasive, oltre che rispettose delle garanzie di libertà e dignità dei dipendenti, con le quali deve contemperarsi l'interesse del datore di lavoro al controllo ed alla difesa dell'organizzazione produttiva aziendale.

9.3. Modalità di Conservazione

I sistemi software sono stati programmati e 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 alle seguenti finalità:

- esigenze tecniche o di sicurezza del tutto particolari;
- indispensabilità del dato per esercizio del potere disciplinare previsto dalla legge e dal CCNL applicabile;
- indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria e stragiudiziale;
- obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

Il datore di lavoro, nell'effettuare i controlli sui lavoratori, è obbligato a rispettare i principi in materia di tutela dei dati personali:

- principio di necessità: il controllo deve risultare necessario o indispensabile rispetto ad uno scopo determinato ed avere il carattere dell'eccezionalità, limitato nel tempo e nell'oggetto, mirato e mai massivo;
- principio di finalità: il controllo deve essere finalizzato a garantire la sicurezza o la continuità aziendale, o a prevenire e reprimere illeciti;
- principio di trasparenza: il datore di lavoro deve informare preventivamente i/le dipendenti sui limiti di utilizzo degli strumenti e delle sanzioni previste nel caso di violazione di tali limiti;
- principio di proporzionalità: il datore di lavoro deve adottare forme di controllo strettamente proporzionate e non eccedenti lo scopo della verifica;
- principio di sicurezza: i dati raccolti devono essere protetti in modo adeguato.

Il trattamento dei dati del/la lavoratore/rice per le predette finalità avviene pertanto nel rispetto dei diritti fondamentali dei lavoratori e delle lavoratrici e la base giuridica di tale trattamento è rappresentata da:

- adempimento di obblighi derivanti da un contratto di lavoro;
- adempimento di obbligazioni previste dalla legge.

10. SEZIONE X: PROVVEDIMENTI DISCIPLINARI

10.1. Conseguenze delle infrazioni disciplinari

Il mancato rispetto o la violazione delle regole contenute nelle presenti disposizioni è perseguibile con provvedimenti disciplinari nonché con azioni civili e penali e fatto salvo in ogni caso il diritto dell'Azienda al risarcimento dei danni eventualmente patiti a causa della condotta del lavoratore e della lavoratrice.

La presente disposizione disciplinare integra e non sostituisce il sistema più generale delle sanzioni relative ai rapporti tra datore di lavoro e dipendente, in base alle normative vigenti.

La tipologia di sanzioni irrogabili nei confronti dei dipendenti, nel rispetto di quanto indicato dall'articolo 7 della legge 20 maggio 1970 n. 300 (Statuto dei Lavoratori) e successive modifiche, è quella prevista dal contratto collettivo di riferimento, cui si rinvia.

10.2. Modalità di Esercizio dei diritti

Il lavoratore interessato del trattamento dei dati effettuato mediante strumenti informatici ha diritto di accedere, ai sensi dell'art. 15 del Regolamento, alle informazioni che lo riguardano scrivendo al Titolare dell'azienda ed al Responsabile per la protezione dei dati (RPD) ed esercitare i diritti previsti dagli artt. 15 e seguenti del GDPR.

11. SEZIONE XI: VALIDITA', AGGIORNAMENTO ED AFFISSIONE

11.1. Validità

Le presenti Disposizioni Attuative sono adottate con Disposizione del/la Direttore/rice Generale ed entrano in vigore a decorrere dal trentesimo giorno successivo alla sua approvazione.

11.2. Aggiornamento

Le presenti Disposizioni Attuative saranno oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'Azienda o in caso di mutazioni legislative.

Ogni variazione delle presenti Disposizioni Attuative sarà comunicata a tutti i soggetti Incaricati.

11.3. Rinvio

Per quanto non espressamente richiamato nelle presenti Disposizioni Attuative, si rinvia alle disposizioni civili e penali vigenti in materia.

11.4. Affissione

Le Disposizioni Attuative e gli eventuali aggiornamenti delle stesse verranno affisse nelle apposite bacheche presenti in ogni sede ai sensi dell'art. 7 della legge 300/70 e del CCNL, e/o inviati alle caselle di posta elettronica di dipendenti e collaboratori, e ove previsto pubblicate sul sito internet aziendale.