

3 Disciplinare per l'uso degli strumenti informatici, di internet e della posta elettronica

Regole di condotta ed obblighi dei collaboratori in relazione all'uso degli strumenti informatici, di Internet e della Posta Elettronica redatto anche ai sensi del "Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati" (da ora in poi GDPR) e del provvedimento del Garante della Privacy (Deliberazione n. 13 del 1/3/2007 - pubblicata sulla GU n. 58 del 10 marzo 2007) comprensivo di alcuni controlli richiesti dalla ISO 27001 e note per la gestione dei dati cartacei.

Indice dei contenuti

1. SEZIONE I – AMBITO GENERALE	4
1.1. Definizioni.....	4
1.2. Premessa	4
1.3. Classificazione delle informazioni	5
1.3.1. Informazioni pubbliche (open)	5
1.3.2. Informazioni con accesso ristretto.....	5
1.3.3. Informazioni confidenziali.....	6
1.4. Esclusione all'uso degli strumenti informatici.....	6
1.5. Titolarità dei device e dei dati.....	7
1.6. Trasferimento degli Asset.....	7
1.7. Finalità nell'utilizzo dei device.....	7
1.8. Restituzione dei device.....	7
1.9. Restituzione dei dati cartacei	7
1.10. Trasferimento di dati con supporti digitali	8
2. SEZIONE II – PASSWORD	9
2.1. Le Password.....	9
2.2. Regole per la corretta gestione delle password.....	9
2.3. Divieto di uso.....	10
2.3.1. Alcuni esempi di password non ammesse.....	10
2.4. La password nei sistemi.....	10
2.5. Chiavi crittografiche	10
2.6. Audit delle password	10
3. SEZIONE III – OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO.....	12
3.1. Login e Logout	12
3.2. Obblighi	12
4. SEZIONE IV - USO DEL PERSONAL COMPUTER DELL'AZIENDA	13
4.1. Modalità d'uso del COMPUTER aziendale.....	13
4.2. Corretto utilizzo del COMPUTER aziendale.....	13
4.3. Divieti Espresi sull'utilizzo del COMPUTER	13
4.4. Uso di programmi di utilità privilegiati.....	14
4.5. Antivirus	14
5. SEZIONE V – INTERNET	16
5.1. Internet è uno strumento di lavoro.....	16
5.2. Misure preventive per ridurre navigazioni illecite	16
5.3. Divieti Espresi concernenti Internet	16
5.4. Divieti di Sabotaggio.....	17
5.5. Diritto d'autore.....	17
6. SEZIONE VI – POSTA ELETTRONICA.....	18

.

6.1.	La Posta Elettronica è uno strumento di lavoro	18
6.2.	Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica	18
6.3.	Divieti Espressi.....	18
6.4.	Posta Elettronica in caso di assenze programmate ed assenze non programmate.....	19
6.5.	Cessazione del rapporto lavorativo.....	19
6.6.	Utilizzo Illecito di Posta Elettronica	20
6.7.	Utilizzo della Posta elettronica Certificata	20
7.	SEZIONE VII – USO DI ALTRI DEVICE (PERSONAL COMPUTER PORTATILE, TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELETTRONICI)	21
7.1.	L'utilizzo del notebook, tablet o smartphone	21
7.2.	Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ...)	21
7.3.	Device personali e BYOD	22
7.4.	Utilizzo del cellulare/smartphone personale.	22
7.5.	Utilizzo delle stampanti.....	22
7.6.	Distruzione dei Device.....	22
8.	SEZIONE VIII – SISTEMI IN CLOUD.....	23
8.1.	Cloud Computing.....	23
8.2.	Utilizzo di sistemi cloud	23
9.	SEZIONE IX – GESTIONE DATI CARTACEI	24
9.1.	Clear Desk Policy	24
10.	SEZIONE X -APPLICAZIONE E CONTROLLO	25
10.1.	Il controllo	25
10.2.	Modalità di verifica	25
10.3.	Modalità di Conservazione	25
11.	SEZIONE XI – SOGGETTI PREPOSTI DEL TRATTAMENTO, INCARICATI E RESPONSABILI.....	26
11.1.	Individuazione dei Soggetti autorizzati.....	26
12.	SEZIONE XII – PROVVEDIMENTI DISCIPLINARI	27
12.1.	Conseguenze delle infrazioni disciplinari.....	27
13.	SEZIONE XIII – VALIDITA', AGGIORNAMENTO ED AFFISSIONE	28
13.1.	Validità	28
13.2.	Aggiornamento	28
13.3.	Affissione.....	28



1. SEZIONE I – AMBITO GENERALE

1.1. Definizioni

Azienda: La ragione sociale indicata in testata al presente documento.

Dipendente: personale dell'ente assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.

Disciplinare: Disciplinare per l'utilizzo degli strumenti informatici, di internet e della posta elettronica. E' il presente documento.

Device: Qualsiasi computer (workstation o laptop) smartphone, tablet o altro tipo di dispositivo elettronico (comprese chiavette usb, hard disk, smart card o altri sistemi di memorizzazione o di gestione dei dati)

GDPR: Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati

Incaricato: ogni dipendente, come sopra identificato, ed ogni altra persona fisica che sotto il controllo dell'Azienda, nell'ambito dell'attività assegnatagli, tratta dati (nell'accezione del capitolo seguente) gestiti dall'Azienda stessa.

NDA: non disclosure agreement, ovvero accordo di non divulgazione, è un negozio giuridico di natura sinallagmatica che designa informazioni confidenziali e con il quale le parti si impegnano a mantenerle segrete, pena la violazione dell'accordo stesso e il decorso di specifiche clausole penali in esso contenute.

1.2. Premessa

L'ambito lavorativo porta la nostra Azienda a gestire una serie di "informazioni", proprie e di terzi, per poter erogare i servizi che le vengono contrattualmente richiesti.

Tali informazioni possono essere considerate, ai sensi 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 adeguate misure tecniche ed organizzative atte a proteggere tali dati.

Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "informazioni riservate", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l'Azienda è chiamata a garantire la riservatezza, o per NDA, o per una più ampia tutela del patrimonio aziendale.

Ai fini di questo disciplinare si specifica, pertanto, che con il termine "dati" deve intendersi l'insieme più ampio di informazioni di cui un incaricato (dipendente, collaboratore, tirocinante, ...) 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.

Inoltre, nell'ambito della sua attività, l'Azienda tratta "dati cartacei" ovvero informazioni su supporto cartaceo e "dati digitali" ovvero informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature digitali.

In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui l'incaricato 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'Azienda stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita dell'Azienda.

Anche tra colleghi, 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.

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare l'accesso alla rete internet dal computer aziendale 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 il presente Disciplinare diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.

Il presente Disciplinare si applica agli Incaricati che si trovino ad operare con dati dell'Azienda.

Una gestione dei dati cartacei, un uso dei Device aziendali nonché dei servizi di internet e della posta elettronica difforme dalle regole contenute nel presente Disciplinare 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.

Le informazioni contenute nel presente Disciplinare vengono rilasciate anche ai sensi dell'art. 13 del Codice sulla Privacy e costituiscono, quindi, parte integrante dell'informativa rilasciata agli Incaricati.

1.3. Classificazione delle informazioni

Di seguito vengono classificate le informazioni detenute, secondo il seguente schema:

1.3.1. Informazioni pubbliche (open)

Tipo:	Informazioni che possono essere distribuite a chiunque senza causare danno all'organizzazione, ai dipendenti o agli stakeholders. La Direzione deve approvare l'attribuzione di questa classificazione su un insieme di informazioni. I documenti in questa categoria possono essere comunicati al pubblico o a persone esterne all'organizzazione.
Esempio:	Materiale del Marketing predisposto per la comunicazione al pubblico o per spot, brochures, rendicontazioni annuali, internet, annunci di lavoro, etc.
Etichettatura:	nessuna
Responsabilità utilizzatore:	nessuna
Duplicazione:	senza vincoli
Distribuzione:	senza vincoli
Distruzione e riciclaggio:	senza vincoli

1.3.2. Informazioni con accesso ristretto

Tipo:	Informazioni che possono essere divulgate ad un gruppo ristretto di soggetti esterni all'azienda.
Esempio:	Documentazione di progetto archiviata e resa disponibile a ristretti gruppi di soggetti esterni o a utenti autorizzati.
Etichettatura:	nessuna
Responsabilità utilizzatore:	Autore: responsabile di verificare che la distribuzione delle informazioni confidenziali sia limitata ai casi di effettiva necessità.
Duplicazione:	senza vincoli
Distribuzione:	Distribuzione tramite sistemi di controllo di accesso e tracciatura delle attività.

Distruzione e riciclaggio:	Cancellazione dal sistema o rimozione della condivisione esterna da parte degli utenti autorizzati.
-----------------------------------	---

1.3.3. Informazioni confidenziali

Tipo:	Informazioni aziendali, confidenziali o di valore, sia personali che sotto brevetto. Non devono assolutamente essere divulgate all'esterno dell'organizzazione senza l'esplicito permesso della Direzione.
Esempio:	Password, codici PIN, certificati di firma digitale, informazioni personali, dati relativi alla contabilità aziendale, altre informazioni altamente confidenziali o di valore.
Etichettatura:	CONFIDENZIALE
Responsabilità utilizzatore:	Autore: responsabile di verificare che la distribuzione delle informazioni confidenziali sia limitata ai casi di effettiva necessità. Utilizzatore: assicurarsi che le informazioni confidenziali siano conservate con tecniche di cifratura o tenute sotto chiave.
Duplicazione:	L'autore o i suoi delegati possono creare un numero limitato di copie.
Distribuzione:	Interna: utilizzare buste sigillate o la consegna a mano. Esterna: tramite busta sigillata anonima consegnata a mano, tramite email registrate/PEC, corrieri di fiducia, etc. Per via elettronica: utilizzando Cifratura.
Distruzione e riciclaggio:	Documento cartaceo: fatto a pezzi con trituradocumenti predisposto. Dati elettronici: cancellazione dal sistema o cancellazione tramite smagnetizzazione (degaussing). Inviare CD, DVD, Hard Disk, Portatili etc. al reparto IT per lo smaltimento.

1.4. 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 device aziendali, di internet e della posta elettronica da parte degli incaricati.

Successivamente e periodicamente l'Azienda valuta la permanenza dei presupposti per l'utilizzo dei device aziendali, di internet e della posta elettronica da parte degli incaricati.

È fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici aziendali.

I casi di esclusione possono riguardare:

1. l'utilizzo del COMPUTER o di altri DEVICE;
2. l'utilizzo della posta elettronica;
3. l'accesso a internet.

Le eventuali esclusioni sono strettamente connesse al principio della natura aziendale e lavorativa degli strumenti informatici nonché al principio di necessità di cui al GDPR.

Più specificatamente hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo gli incaricati che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.

I casi in cui le esclusioni dovranno risultare operative in forza di tali motivazioni verranno comunicati individualmente e potranno riguardare sia tutti i casi sopra descritti, sia solo uno o due degli stessi.

Si informa che tali esclusioni sono divenute necessarie alla luce del Provvedimento del Garante 1° marzo 2007 che indica di ridurre a titolo cautelativo e preventivo l'utilizzo degli strumenti informatici in considerazione dei pericoli e delle minacce indicate in questo documento.

1.5. Titolarità dei device e dei dati

L'Azienda è esclusiva titolare e proprietaria dei Device messi a disposizione degli 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 device digitali o archiviati in modo cartaceo nei propri locali.

L'incaricato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei device aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'Azienda.

1.6. Trasferimento degli Asset

Apparecchiature, informazioni o software, in linea generale, non devono essere portati all'esterno dell'Azienda senza preventiva autorizzazione.

L'incaricato che ne avesse necessità deve farne richiesta alla Direzione che provvede ad autorizzare in modo esplicito la tipologia di asset che può essere portata al di fuori dell'azienda ed i limiti di tempo per l'asportazione.

1.7. Finalità nell'utilizzo dei device

I device assegnati sono uno strumento lavorativo nelle disponibilità dell'Incaricato esclusivamente per un fine di carattere lavorativo. I device, quindi, non devono essere utilizzati per finalità private e diverse da quelle aziendali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare.

Qualsiasi eventuale tolleranza da parte di questa Azienda, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

1.8. Restituzione dei device

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

1. procedere immediatamente alla restituzione dei device in uso nello stato in cui si trova;
2. divieto assoluto di cancellare o formattare o alterare o manomettere o distruggere i device assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo, compresa la cifratura dei dati.

1.9. Restituzione dei dati cartacei

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

1. procedere immediatamente alla restituzione dei dati cartacei in loro possesso;
2. divieto assoluto di cancellare o alterare o manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili tramite qualsiasi processo.

1.10. Trasferimento di dati con supporti digitali

Il trasferimento di dati sia all'interno che all'esterno dell'Azienda attraverso i supporti digitali è generalmente ammesso a patto che siano seguite delle procedure che possano garantire di proteggere le informazioni trasferite da potenziali intercettazioni, copia, modifica errori di instradamento e/o distruzione.

Nell'invio delle e-mail gli utenti devono essere molto attenti nel controllare l'indirizzo del/i destinatario/i prima dell'invio per evitare errori di battitura o errori dovuti all'autocompilazione.

L'invio di comunicazioni deve avvenire solo da device protetti da antivirus onde proteggere le comunicazioni da eventuali malware.

Gli allegati contenenti "dati particolari" ex art. 9 del GDPR o "dati giudiziari" ex art. 10 del GDPR oppure "Informazioni confidenziali" come sopra definite, devono essere oggetto di invio come allegato criptato.

Nel caso di utilizzo di posta elettronica certificata (PEC) vanno seguite le regole stabilite nella sezione specifica del presente Disciplinary.

In caso di trasferte fuori dall'ufficio, utilizzando i device in ambito pubblico, è necessario prestare la massima attenzione che non vi siano terzi non autorizzati che possano accedere ai dati.

2. SEZIONE II – PASSWORD

2.1. Le Password

Le password possono essere un metodo di autenticazione assegnato dall'Azienda 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 dell'Azienda nel suo complesso.

Nel tempo anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza.

L'Azienda ha implementato alcuni meccanismi che permettono di aiutare e supportare gli Incaricati in una corretta gestione delle password, in particolare, per quanto riguarda le password di accesso al Dominio (ove previsto), è in funzione un sistema automatico di richiesta di aggiornamento delle stesse impostato dall'Azienda secondo il livello di sicurezza richiesto dall'Azienda stesso e, comunque, in linea con quanto richiesto dalla valutazione dei rischi effettuata dall'azienda in base alle richieste del GDPR.

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.

Le password che non vengono utilizzate da parte degli Incaricati per un periodo superiore ai sei mesi verranno disattivate dall'Azienda.

In qualsiasi momento l'Azienda si riserva il diritto di revocare all'Incaricato 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 delle password

L'Incaricato, da parte sua, per una corretta e sicura gestione delle proprie password deve rispettare le regole seguenti:

1. Le password sono assolutamente personali e non vanno mai comunicate ad altri;
2. Occorre cambiare immediatamente una password non appena si abbia alcun dubbio che sia diventata poco "sicura";
3. Le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali¹ e numeri;
4. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
5. Le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password.
6. 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 fino ad 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.

¹ Per caratteri speciali si intendono, per esempio, i seguenti: { } [] , . < > ; ! " £ \$ % & / () = ? ^ \ | ' * - + _ .

2.3. Divieto di uso

Al fine di una corretta gestione delle password, l'Azienda stabilisce il divieto di utilizzare come propria password:

1. Nome, cognome e loro parti;
2. Lo username assegnato;
3. Un indirizzo di posta elettronica (e-mail);
4. Parole comuni (in Inglese e in Italiano);
5. Date, mesi dell'anno e giorni della settimana, anche in lingua straniera;
6. Parole banali e/o di facile intuizione, ad es. pippo, security e palindromi (simmetria: radar);
7. Ripetizioni di sequenze di caratteri (es. abcabcabc);
8. Una password già impiegata in precedenza.

2.3.1. 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.: "NIMzz5DICmm!", 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.).

2.4. La password nei sistemi

Ogni Incaricato 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. Chiavi crittografiche

Eventuali chiavi crittografiche nelle disponibilità dell'azienda devono essere in possesso solo della Direzione, che potrà, di volta in volta, delegare le stesse a personale espressamente autorizzato.

2.6. 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 gli Incaricati stessi.

Nei caso in cui l'audit abbia, tra gli esiti possibili, la decodifica della password, questa viene bloccata e all'incaricato richiesto di cambiarla. Tale risultanza potrebbe dar luogo a provvedimenti disciplinari secondo quanto previsto dal CCNL adottato dall'Azienda.

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

In questa sezione vengono trattate le operazioni a carico dell'Incaricato 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 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), ognuno dei quali richiede un username e una password.

In questi casi, sebbene sia preferibile che ogni utente abbia un suo specifico user name e password, l'Azienda potrà assegnare un univoco user name e password per gruppi di incaricati per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci per l'accesso agli applicativi che contengono dati.

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 deve quindi eseguire le operazioni seguenti:

1. Se si allontana dalla propria postazione dovrà mettere in protezione il suo device affinché persone non autorizzate non abbiano accesso ai dati protetti.
2. Bloccare il suo device prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
3. Chiudere la sessione (Logout) a fine giornata;
4. Spegnerne il PC dopo il Logout;
5. Controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo device.

4. SEZIONE IV - USO DEL PERSONAL COMPUTER DELL'AZIENDA

4.1. Modalità d'uso del COMPUTER aziendale

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

I files 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.

Gli operatori del Reparto Sistemi Informativi possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la Sicurezza sia sui PC degli utenti che sulle unità di rete.

4.2. Corretto utilizzo del COMPUTER aziendale

Il computer consegnato all'incaricato 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.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Il computer che viene consegnato contiene tutti i software necessari a svolgere le attività affidate dall'Azienda. Per necessità aziendali, gli amministratori di sistema utilizzando la propria login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente documento, sia alla memoria di massa locali di rete (repository e backup) che ai server aziendali nonché, previa comunicazione al dipendente, accedere al computer, anche da remoto.

In particolare l'Incaricato deve adottare le seguenti misure:

1. utilizzare solo ed esclusivamente le aree di memoria della rete dell'Azienda ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri files fuori dalle unità di rete;
2. spegnere il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso;
3. mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), disposti dall'Azienda;
4. Non dare accesso al proprio computer ad altri utenti, a meno che siano incaricati con cui condividono l'utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

4.3. Divieti Espresi sull'utilizzo del COMPUTER

All'incaricato è vietato:

1. La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali dell'incaricato 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 alcun software di cui l'Azienda non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione dell'Azienda. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale.
5. Caricare sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate. In particolare non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
6. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (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'Azienda, quali per esempio virus, trojan horses ecc.
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'Azienda.
11. Attivare la password d'accensione del BIOS
12. Riprodurre o duplicare programmi informatici ai sensi delle Legge n.128 del 21.05.2004 ("...recante interventi per contrastare la diffusione telematica abusiva di materiale audiovisivo, nonché a sostegno delle attività cinematografiche e dello spettacolo"), vedi anche Legge n. 633 del 22.04.1941 ("Legge sul diritto d'autore").

4.4. Uso di programmi di utilità privilegiati

L'uso di programma di utilità che potrebbero essere in grado di aggirare i controlli applicativi e di sistema sono, in generale, vietati.

Tali programmi possono essere utilizzati solo se sussistono le seguenti condizioni:

- 1) I programmi in questione sono stati autorizzati esplicitamente dalla Direzione;
- 2) Gli incaricati ad utilizzare tali programmi sono stati oggetto di esplicita autorizzazione da parte della Direzione;
- 3) Ogni volta che i programmi devono essere utilizzati è necessario che l'incaricato autorizzato richieda alla direzione l'autorizzazione allo specifico utilizzo;
- 4) Ogni utilizzo di tali programmi deve essere tracciato;
- 5) I programmi di utilità devono essere disinstallati una volta terminato l'utilizzo.

4.5. Antivirus

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, via mail ...

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.

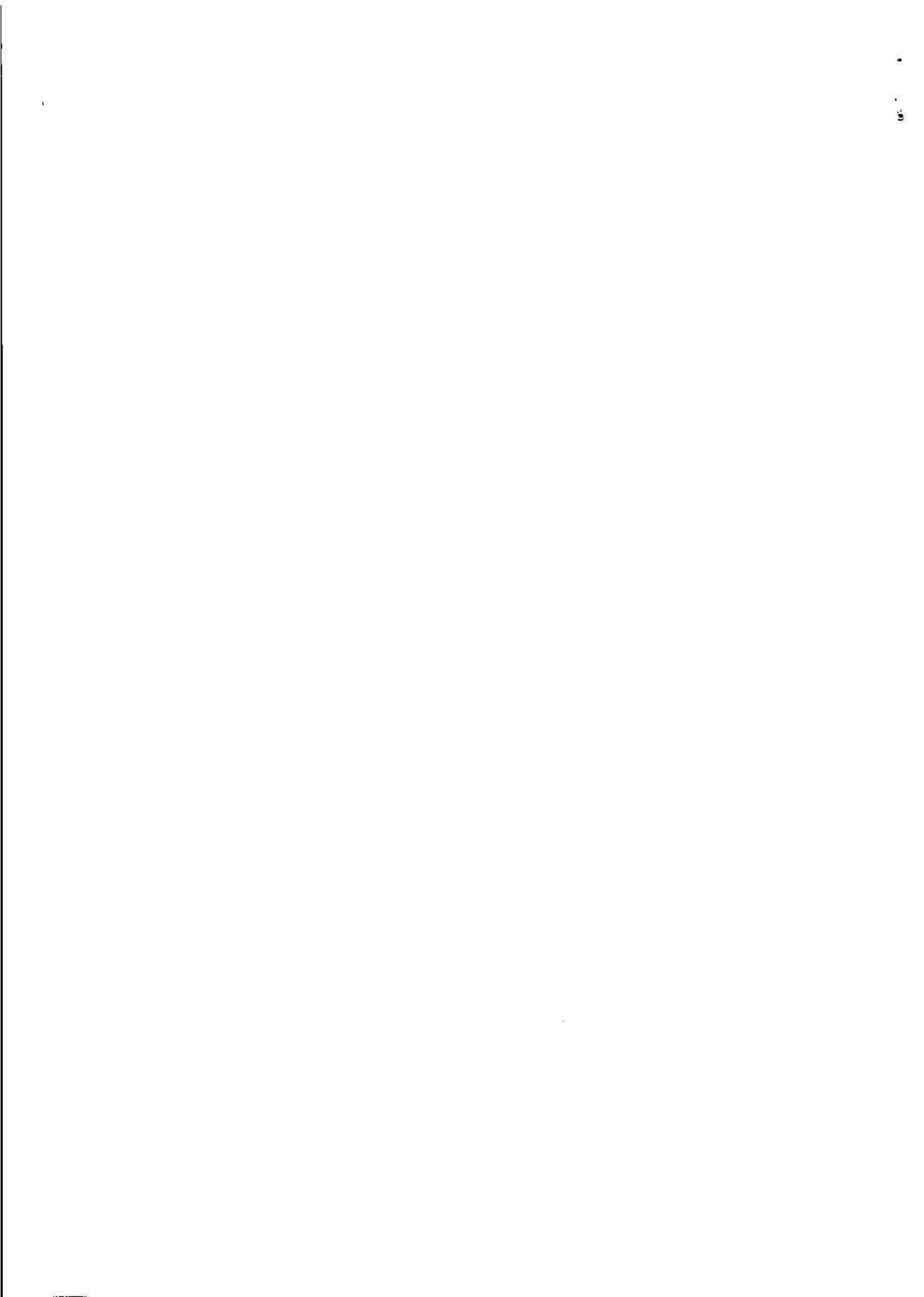
L'incaricato, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer, e, in particolare, deve rispettare le regole seguenti:

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:

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 e 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.

Contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.



5. SEZIONE V – INTERNET

5.1. Internet è uno strumento di lavoro

La connessione alla rete internet dal device avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento.

In particolare si vieta l'utilizzo dei social network, se non espressamente autorizzati.

5.2. Misure preventive per ridurre navigazioni illecite

L'Azienda potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list implementati ad esempio attraverso i sistemi di content filter dei firewall.

5.3. Divieti Espresi concernenti Internet

1. È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute dell'Incaricato poiché potenzialmente idonea a rivelare dati personali ai sensi del GDPR.
2. 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, degli handicap.
3. È vietato all'Incaricato lo scarico di software (anche gratuito) prelevato da siti Internet;
4. 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.
5. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
6. 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.
7. 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.
8. È vietato all'Incaricato di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale.
9. È vietato accedere dall'esterno alla rete interna dell'Azienda, salvo specifica autorizzazione e con le specifiche procedure previste dall'Azienda stessa.
10. È vietato, infine, creare siti web personali sui sistemi dell'Azienda nonché acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.
11. È vietato utilizzare internet per attività di file sharing.

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

dell'Incaricato inadempiente e può dar luogo a provvedimenti disciplinari secondo quanto previsto dal CCNL adottato dall'Azienda.

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, 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248 e s.m.i.). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, ...) se non espressamente autorizzato dall'Azienda:

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. L'uso per motivi personali deve essere moderato ed è tollerato esclusivamente ai sensi dell'articolo seguente.

Gli Incaricati possono avere in utilizzo caselle di posta elettronica appartenenti ai domini aziendali. Gli assegnatari dei singoli account sono responsabili del corretto utilizzo delle stesse.

Le caselle e-mail possono essere assegnate con natura impersonale (tipo info, amministrazione, fornitori, direttore, consulenza, ...) per evitare che il destinatario delle mail possa considerare l'indirizzo assegnato al dipendente "privato", ai sensi dei suggerimenti del Garante a tal proposito.

Possono altresì essere assegnati indirizzi nominativi che dovranno comunque essere considerati a pieno titolo indirizzi dedicati all'attività lavorativa.

La scelta dell'account mail da assegnare all'incaricato resta in capo all'Azienda.

6.2. Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica

L'Azienda è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte degli Incaricati e allo scopo prevede le seguenti misure:

1. In caso di ricezione sulla e-mail aziendale di posta personale si avverte di cancellare immediatamente ogni messaggio al fine di evitare ogni eventuale e possibile back up dei dati. Tutti i contenuti non cancellati possono essere soggetti a back up.
2. Avisare l'Azienda quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.

6.3. Divieti Espressi

1. È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio dell'Azienda per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'Azienda, nonché utilizzare il dominio dell'Azienda per scopi personali.
2. È vietato redigere messaggi di posta elettronica utilizzando l'indirizzo aziendale, diretti a destinatari esterni dell'Azienda, senza utilizzare il seguente disclaimer nel pedice della mail:

Il presente messaggio e gli eventuali suoi allegati sono di natura aziendale, prevalentemente confidenziale e sono visionabili solo dal destinatario di posta elettronica. La risposta o l'eventuale invio spontaneo da parte vostra di e-mail al nostro indirizzo potrebbero non assicurare la confidenzialità potendo essere viste da altri soggetti appartenenti all'Azienda oltre che al firmatario della presente, per finalità di sicurezza informatica, amministrative e allo scopo del continuo svolgimento dell'attività aziendale. Qualora questo messaggio vi fosse pervenuto per errore, vi preghiamo di cancellarlo dal vostro sistema e vi chiediamo di volercene dare cortesemente comunicazione al mittente.

La Vs. mail è in ns. possesso in quanto da Voi fornita tramite comunicazione scritta, telefonica, telematica o direttamente oralmente. Essa è utilizzata esclusivamente per fornirVi informazioni sulla ns. attività e sui servizi da noi offerti. Non sarà ceduta a terzi in nessun caso salvo approvazione da parte Vostra. Il Titolare del trattamento è l'Azienda. I ns. sistemi informativi e le ns. procedure interne sono conformi alle norme e garantiamo la presenza di adeguate misure tecniche ed organizzative costantemente aggiornate.

È possibile in qualsiasi momento richiedere la cancellazione della Vs. mail tramite la semplice risposta alla presente mail con titolo unsubscribe

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 dell'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 per messaggi con allegati di grandi dimensioni.
8. Nel caso di mittenti sconosciuti o messaggi inusuali, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.
9. Nel caso di messaggi provenienti da mittenti noti ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti ma cancellati.

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

Nel caso di assenza prolungata sarebbe buona norma attivare il servizio di risposta automatica (Auto-reply). In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, l'Incaricato deve nominare un collega fiduciario con lettera scritta che in caso di assenza inoltri i files necessari a chi ne abbia urgenza.

Qualora l'Incaricato non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, l'Azienda, mediante personale appositamente incaricato, potrà verificare il contenuto dei messaggi di posta elettronica dell'incaricato, informandone l'incaricato stesso e redigendo apposito verbale.

6.5. Cessazione del rapporto lavorativo

L'Azienda può attivare account di mail relativi sia su caselle di tipo generico (info@, amministrazione@, ufficio@ etc...) sia su caselle di tipo nominale (n.cognome@, nome.cognome@, cognome@, nome@ etc...).

In caso di cessazione del rapporto di lavoro tra l'Azienda e l'incaricato è vietato a quest'ultimo di cancellare i messaggi di mail inviati e/o ricevuti tramite l'account assegnatogli, essendo quei messaggi un patrimonio aziendale.

In caso di cessazione del rapporto di lavoro tra l'Azienda e l'incaricato la casella mail assegnata potrà essere mantenuta attiva per un periodo fino a 12 mesi o dismessa, anche prima dei 12 mesi, in base alle necessità aziendali.

Se mantenuta attiva potrà essere assegnata ad altro personale aziendale oppure le mail ricevute potranno essere inviate ad altra mail aziendale.

L'azienda potrà predisporre un messaggio di risposta automatica per avvisare il mittente che il destinatario non lavora più in azienda. Il contenuto della mail (inviato o ricevuto) resta di proprietà dell'Azienda che potrà decidere se conservarlo e archivarlo (mantenimento dei back up) oppure eliminarlo definitivamente.

6.6. Utilizzo Illecito di Posta Elettronica

1. È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
2. È vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano 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, degli handicap.
3. Qualora l'Incaricato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'Azienda.

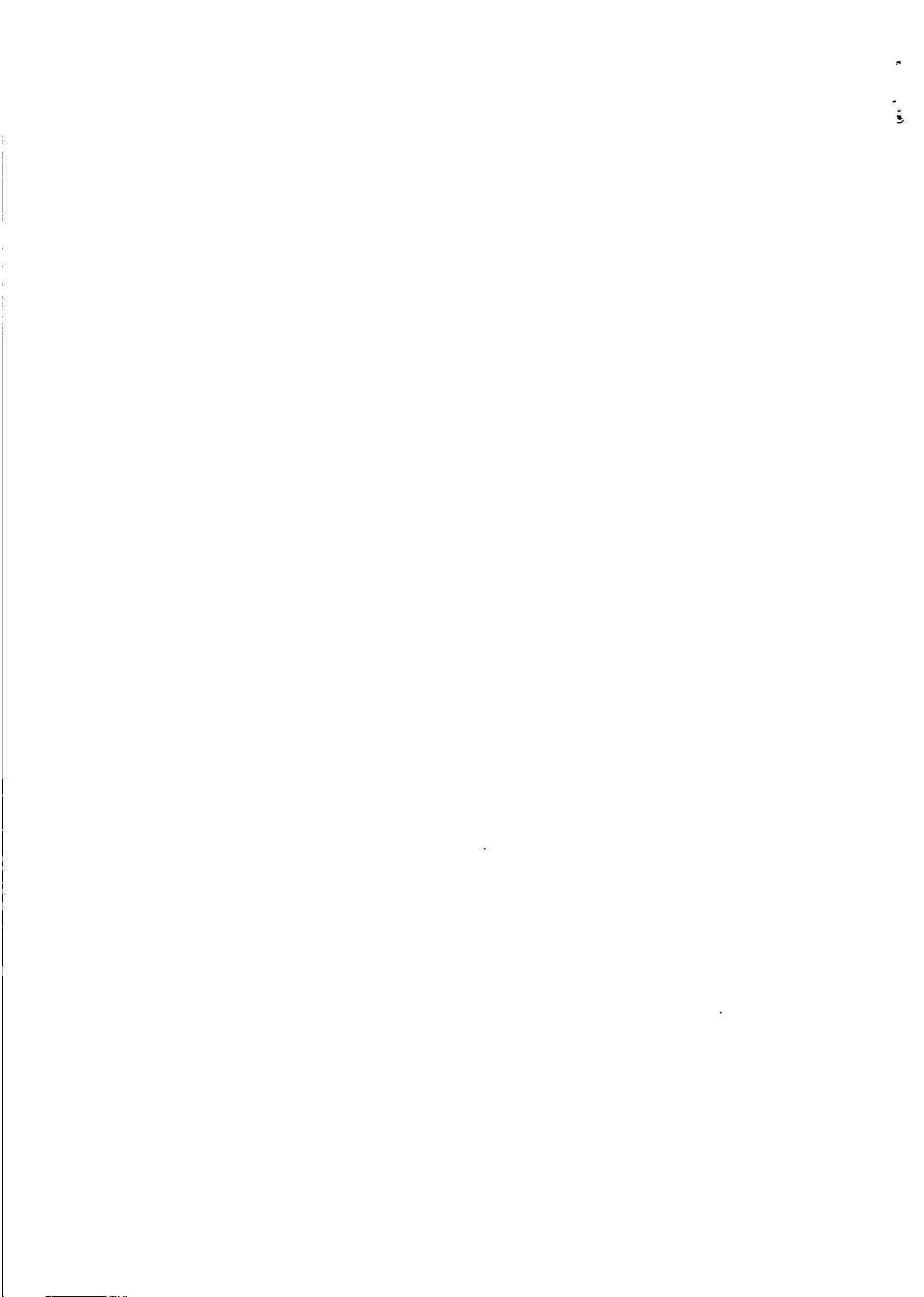
6.7. Utilizzo della Posta elettronica Certificata

La Posta Elettronica certificata (PEC) è uno strumento o servizio informatico italiano che permette di dare ad un messaggio di posta elettronica lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale, garantendo così il non ripudio, con il vantaggio che la ricevuta di consegna contiene anche il messaggio, gli allegati e le identità del mittente e del destinatario di PEC, anch'essi certificati.

Ogni PEC è registrato e collegata al nominativo di una persona fisica.

La PEC viene utilizzata principalmente per le comunicazioni istituzionali, in particolare per le comunicazioni con gli enti pubblici o in sostituzione della raccomandata anche tra privati.

Le credenziali di accesso alla PEC devono essere nella stretta disponibilità della persona fisica a cui la PEC si riferisce. La stessa può delegare, con atto formale, altri incaricati all'utilizzo della PEC sia in visione che in trasmissione.



7. SEZIONE VII – USO DI ALTRI DEVICE (PERSONAL COMPUTER PORTATILE, TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELETTRONICI)

7.1. L'utilizzo del notebook, tablet o smartphone.

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in "device mobile") possono venire concessi in uso dall'Azienda agli Incaricati che durante gli spostamenti necessitano di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'Azienda.

L'Incaricato è responsabile dei device mobili assegnatigli dall'Azienda e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai device 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 files creati o modificati sui device mobili devono essere trasferiti sulle memorie di massa aziendali al primo rientro in ufficio e cancellati in modo definitivo dai device mobili (Wiping). Sui device mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'Azienda. I device 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 device 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. Anche di giorno, durante l'orario di lavoro, all'Incaricato non è consentito lasciare incustoditi i device mobili.

All'Incaricato è vietato lasciare i device mobili incustoditi e a vista dentro l'auto o in una stanza d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

I device mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciati privi di PIN.

Laddove il device mobile sia accompagnato da un'utenza, l'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 l'Incaricato è tenuto ad informare tempestivamente e preventivamente l'Azienda.

In relazione alle utenze mobili, salvo autorizzazione dell'Azienda, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione dell'Azienda, gli utilizzi all'esterno devono essere preventivamente comunicati all'Azienda per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

Alcuni Device mobili, quali smartphone e tablet, possono essere dotati dall'azienda di particolari misure di protezione (MDM o altro).

7.2. Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ...)

Agli Incaricati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, ...) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, ...).

Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

7.3. Device personali e BYOD

Ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili, device personali.

Ai dipendenti, se espressamente autorizzati dall'Azienda, è permesso solo l'utilizzo della posta elettronica aziendale sui loro device personali.

In tal caso è necessario che il device abbia password di sicurezza stringenti approvate dall'Azienda e l'eventuale furto o smarrimento del device deve essere immediatamente segnalato anche all'Azienda per eventuali provvedimenti di sicurezza.

Al collaboratore è vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, ...).

Alcuni incaricati possono utilizzare i propri device personali per memorizzare dati dell'Azienda (Bring Your Own Device – BYOD) solo se espressamente autorizzati dall'Azienda stessa e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali device dovranno essere preventivamente valutati dall'Azienda, per la verifica della sussistenza di adeguate misure di sicurezza.

7.4. 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 all'esterno degli uffici dell'Azienda, il telefono personale può rimanere acceso, anche per facilitare la comunicazione con l'Azienda stessa ove fosse necessario.

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

7.5. Utilizzo delle stampanti

L'incaricato deve effettuare la stampa dei dati solo se necessaria all'attività lavorativa e deve ritirarla prontamente dai vassoi delle stampanti personali/comuni per evitare che sia visibile o possa essere raccolta da terzi. Al momento del ritiro dei fogli stampati, l'utente deve porre attenzione a prelevare solo le proprie pagine.

L'incaricato, qualora disponga di più dispositivi di stampa, deve utilizzare quello che garantisce un maggior controllo del documento stampato.

7.6. Distruzione dei Device

Ogni Device ed ogni memoria esterna affidati agli 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.

Possono essere utilizzate le seguenti procedure:

- Distruzione fisica del supporto
- Cancellazione Logica (Wiping)
- Smagnetizzazione (Degauss)

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.

Le risorse non vengono pienamente configurate e messe in opera dal fornitore apposta per l'utente, ma gli sono assegnate, rapidamente e convenientemente, grazie a procedure automatizzate, a partire da un insieme di risorse condivise con altri utenti lasciando all'utente parte dell'onere della configurazione. Quando l'utente rilascia la risorsa, essa viene similmente riconfigurata nello stato iniziale e rimessa a disposizione nel pool condiviso delle risorse, con altrettanta velocità ed economia per il fornitore.

Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, 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 extraeuropeo, configurando un trasferimento dei dati all'estero. 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.

Nel caso di industrie o aziende, tutti i dati memorizzati nelle memorie esterne sono seriamente esposti a eventuali casi di spionaggio industriale.

8.2. Utilizzo di sistemi cloud

È vietato agli incaricati l'utilizzo di sistemi Cloud non espressamente approvati dall'Azienda. Per essere approvati i sistemi cloud devono rispondere ad almeno i seguenti requisiti:

- Essere sistemi cloud di cui si conosce l'esatto posizionamento dei server e per i quali si è predisposto quanto richiesto dalle norme, compreso eventualmente quello che è richiesto per il trasferimento dei dati all'estero;
- L'azienda che fornisce il sistema in Cloud deve essere preventivamente nominata Responsabile al Trattamento dei dati da parte dell'Azienda;
- L'azienda che fornisce il sistema in Cloud deve comunicare all'Azienda, almeno una volta all'anno, i nominativi degli amministratori di sistema utilizzati.
- Dovranno essere verificate tutte le indicazioni e le prescrizioni previste dal Garante della Privacy nei suoi provvedimenti sugli Amministratori di Sistema e sul Cloud.

9. SEZIONE IX – GESTIONE DATI CARTACEI

9.1. Clear Desk Policy

Gli Incaricati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Gli Incaricati sono invitati dall'Azienda ad adottare una "politica della scrivania pulita". Ovvero si richiede agli incaricati di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dell'Azienda.

I principali benefici di una politica della scrivania pulita sono:

- 1) Una buona impressione a clienti e fornitori che visitano la nostra Azienda;
- 2) La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;
- 3) La riduzione che documenti confidenziali possano essere sottratti all'Azienda.

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.

Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura degli Incaricati riporre in luogo sicuro (armadio, cassetiera, archivio, ...) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti nell'Azienda.

A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra.

Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica.

Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archivarli digitalmente.

E' necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.

Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

10. SEZIONE X -APPLICAZIONE E CONTROLLO

10.1. 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:

1. Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.
2. Evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo.
3. Verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit e vulnerability assesment del sistema informatico. Per tali controlli l'Azienda si riserva di avvalersi di soggetti esterni.

Si precisa, in ogni caso, che l'Azienda 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 certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente.

10.2. Modalità di verifica

In applicazione del GDPR, l'Azienda promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili agli 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 informa di non adottare 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 degli Incaricati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche. Al contrario possono esserci verifiche programmate ai sensi del principio di Accountability ex art. 5.2 del GDPR.

Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di files pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) si effettuerà un avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

10.3. 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:

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.

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 Azienda strettamente correlate agli obblighi, compiti e finalità già esplicitati.

11. SEZIONE XI – SOGGETTI PREPOSTI DEL TRATTAMENTO, INCARICATI E RESPONSABILI

11.1. Individuazione dei Soggetti autorizzati

L'Azienda ha individuato specifiche figure cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità.

Per quanto riguarda i soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) sono stati appositamente incaricati di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità di sicurezza informatica, senza realizzare attività di controllo a distanza, neanche di propria iniziativa.

I soggetti che operano quali amministratori di sistema o le figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, svolgono un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

12. SEZIONE XII – PROVVEDIMENTI DISCIPLINARI

12.1. Conseguenze delle infrazioni disciplinari

Le infrazioni disciplinari alle norme del presente Disciplinare potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato, tra cui:

1. il biasimo inflitto verbalmente;
2. lettera di richiamo inflitto per iscritto;
3. multa;
4. la sospensione dalla retribuzione e dal servizio;
5. il 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'Azienda potrà procedere al licenziamento del dirigente autore dell'infrazione.

13. SEZIONE XIII – VALIDITA', AGGIORNAMENTO ED AFFISSIONE

13.1. Validità

Il presente Disciplinare ha validità a partire dalla data di sottoscrizione da parte del Titolare sotto riportata.

13.2. Aggiornamento

Il presente Disciplinare sarà 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 del presente Disciplinare sarà comunicata agli incaricati.

13.3. Affissione

Il presente Disciplinare verrà affisso nella bacheca aziendale e/o pubblicato sulla intranet aziendale per la maggior diffusione ed ai sensi del CCNL

Data

19 OTT. 2018

Il legale rappresentante del Titolare del trattamento

Il Sindaco

Massimiliano Giorgi



