MdP MANUALE delle PROCEDURE PRIVACY

REDATTO AI SENSI E PER GLI EFFETTI DELL'ART. 29 REL REGOLAMENTO U.E. 2016/679 AL FINE DI ISTRUIRE GLI INCARICATI DEL TRATTAMENTO CIRCA LE MODALITA' DELLO STESSO.

COMPLETO DI:

REGOLAMENTO per l'utilizzo di INTERNET e POSTA ELETTRONICA

MODELLO REV. 1.0

STUDIO TECNICO LEGALE
CORBELLINI
Studio AG.I.COM. S.r.l.

Redatto a cura e negli uffici del D.P.O. :

STUDIO AG.I.COM. S.R.L. UNIPERSONALE
Via XXV Aprile, 12 – 20070 SAN ZENONE AL LAMBRO (MI)
Tel. 02 90601324 Fax 02 700527180 info@agicomstudio.it

www.agicomstudio.it

SCOPO DEL PRESENTE MANUALE

Il Manuale delle Procedure Privacy (M.d.P.) è una raccolta delle procedure in uso all'interno dell'azienda/Ente da parte dei soggetti designati quali "Incaricati del trattamento dei dati" al fine di ottemperare all'obbligo di cui all'Art. 29 del Regolamento U.E. 2016/679: "*Il responsabile del trattamento o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali, non può trattare tali dati se non è stato istruito in tal senso dal titolare del trattamento…"*.

Il manuale viene messo nella disponibilità degli incaricati per la consultazione ed inoltre viene utilizzato come testo di riferimento in occasione dei corsi di formazione svolti all'interno dell'azienda/ente.

Gli strumenti informatici rappresentano da un lato un mezzo insostituibile di lavoro e dall'altro lato un rischio per la sicurezza del patrimonio aziendale (se utilizzati in modo non idoneo).
Si rende pertanto necessaria l'adozione di un documento finalizzato a disciplinare il regolare utilizzo dei predetti strumenti durante l'orario di lavoro e nell'ambito della struttura del titolare del trattamento (*Regolamento utilizzo di internet e della posta elettronica*).

Ogni utilizzo dei dati in possesso dell'azienda/ente diverso da finalità strettamente professionali, è espressamente vietato. Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che, anche inconsapevolmente, potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine dell'Azienda/Ente.

DESTINATARI E CAMPO DI APPLICAZIONE

I soggetti chiamati ad applicare i contenuti del Manuale delle Procedure Privacy sono:

- Il Titolare del trattamento
- Il Responsabile del trattamento (interno o esterno)
- Gli Incaricati del trattamento

Quando operano azioni di inserimento, cancellazione, modifica, elaborazione e custodia di informazioni relative a persone fisiche identificate o identificabili per finalità diverse da quelle strettamente private.
Le procedure si applicano sia ai dati detenuti in formato cartaceo sia a quelli detenuti in formato digitale.

DEFINIZIONI

Ai fini del presente manuale e secondo l'articolo 4 del Regolamento UE 2016/679 (GDPR), si definisce:

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

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

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

ADEMPIMENTI

Ciascun incaricato del trattamento deve:

- rispettare i principi generali del GDPR, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi, è vietato trattare i dati in modo diverso rispetto a quanto previsto dalle procedure interne;

- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;

- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti dell'azienda/ente;

- rispettare le misure di sicurezza adottate, atte a salvaguardare la riservatezza e l'integrità dei dati;

- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;

- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;

- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;

- mantenere riservate le proprie credenziali di autenticazione;

- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;

- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;

- informare senza ritardo il proprio responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;

- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;

- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

- eseguire le procedure riportare di seguito.

NORME LOGISTICHE PER L'ACCESSO FISICO AI LOCALI

I locali, ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro gli stessi possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue il trattamento di dati personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati.
Pertanto le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di Dati Personali.

PROCEDURA CHIAVI

DESTINATARI	ASSISTENTI AMMINISTRATIVI COLLABORATORI SCOLASTICI ALTRI INCARICATI DEL TRATTAMENTO
APPLICABILITA'	CUSTODIA DOCUMENTI CARTACEI CONTENENTI DATI PERSONALI CORRENTI
	TUTTI I DOCUMENTI CARTACEI, CONTENENTI DATI PERSONALI, DI USO CORRENTE DEVONO ESSERE CUSTODITI ALL'INTERNO DI ARMADI, CASSETTI, CASSETTIERE OD OGNI ALTRO ARREDO IDONEO CHIUDENDO A CHIAVE LA SERRATURA DEL MEDESIMO. A FINE TURNO LE CHIAVI DELL'ARREDO IN QUESTIONE DEVONO ESSERE COLLOCATE ALL'INTERNO DI UNA CASSETTINA METALLICA PORTACHIAVI COLLOCATA IN LUOGO SICURO (UFFICIO DS, UFFICIO DSGA) ED A SUA VOLTA CHIUDIBILE. I LOCALI ALL'INTERNO DEI QUALI SONO CUSTODITI GLI ARREDI ATTI ALLA CUSTODIA DEI DOCUMENTI PERSONALI, DOTATI DI PORTA CHIUDIBILE, DEVONO ESSERE A LORO VOLTA CHIUSI A CHIAVE E LA CHIAVE DEVE ESSERE COLLOCATA ALL'INTERNO DI UNA SECONDA CASSETTINA METALLICA PORTACHIAVI COLLOCATA IN LUOGO SICURO (UFFICIO DS, UFFICIO DSGA) ED A SUA VOLTA CHIUDIBILE. LA CHIAVE DELLA CASSETTINA PORTACHIAVI CONTENENTE LE CHIAVI DEGLI ARREDI (c.d. "ULTIMA CHIAVE") E' TRATTENUTA DAL TITOLARE DEL TRATTAMENTO (D.S.) O DA ALTRO INCARICATO AVENTE RUOLO DIRETTIVO E PORTATA CON SE' OPPURE COLLOCATA IN UN LUOGO SEGRETO. LA CHIAVE DELLA CASSETTINA PORTACHIAVI CONTENENTE LE CHIAVI DEI LOCALI ALL'INTERNO DEI QUALI SONO CUSTODITI GLI ARREDI ATTI ALLA CUSTODIA DEI DOCUMENTI PERSONALI, A FINE TURNO, E' COLLOCATA INSIEME ALLE CHIAVI DI TUTTI GLI ALTRI LOCALI SCOLASTICI.
PROCEDURA COLLEGATA	**PULIZIA DEI LOCALI DESTINATI AL TRATTAMENTO DEI DATI IN ASSENZA DI PERSONALE INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI**
	I COLLABORATORI SCOLASTICI CHIAMATI AD ESEGUIRE LE PULIZIE DEI LOCALI IN CUI AVVIENE IL TRATTAMENTO DEI DATI PERSONALI (SEGRETERIA, UFFICIO DI PRESIDENZA, VICEPRESIDENZA, SALA DOCENTI ED ARCHIVI) IN ASSENZA DI PERSONALE INCARICATO DEL TRATTAMENTO, AVRANNO DISPONIBILITA' DELLE SOLE CHIAVI DI ACCESSO A DETTI LOCALI E NON ANCHE DEGLI ARREDI DESTINATI ALLA CUSTODIA DEI DATI PERSONALI. LA PULIZIA DEGLI ARCHIVI DEVE AVVENIRE SOLAMENTE AD OPERA DI COLLABORATORI SCOLASTICI INCARICATI DEL TRATTAMENTO O ALLA PRESENZA DI ALTRI INCARICATI DEL TRATTAMENTO (D.S.G.A. / ASSISTENTI AMMINISTRATIVI)
PROCEDURE AFFINI	- PROCEDURA SCRIVANIE PULITE - PROCEDURA DI CUSTODIA DELLE PAROLE CHIAVE (PASSWORD)

PROCEDURA DI CUSTODIA DELLE PAROLE CHIAVE (PASSWORD)

DESTINATARI	ASSISTENTI AMMINISTRATIVI DOCENTI ALTRI INCARICATI DEL TRATTAMENTO CHE FANNO USO DI STRUMENTI INFORMATICI
APPLICABILITA'	QUANDO IL TRATTAMENTO DI DATI DIGITALI E' MANTENUTO SEGRETO MEDIANTE L'IMPIEGO DI CREDENZIALI DI ACCESSO CON PAROLA CHIAVE (PASSWORD), IL SOGGETTO INCARICATO CHE DISPONGA DI TALE PAROLA CHIAVE IN VIA ESCLUSIVA DEVE RIPORTARLA SU UN APPOSITO MODULO, SIGILLATO IN UNA BUSTA, DA APRIRE SOLAMENTE IN CASO DI ESTREMA NECESSITA' (PROLUNGATA ASSENZA DELL'INTERESSATO, MORTE, MALATTIA ETC.). TALE PROCEDURA DEVE ESSERE ATTUATA ESCLUSIVAMENTE SE VI SIANO AREE DELL'ELABORATORE IN USO ALL'INCARICATO O DI ALTRA PERIFERICA AD ACCESSO ESCLUSIVO.
	IL TITOLARE, RESPONSABILE E INCARICATO DEL TRATTAMENTO DI DATI CHE DISPONE DI UN METODO DI ACCESSO AI DATI INFORMATICI CON PASSWORD, DEVE RIPORTARE LA STESSA SU UN APPOSITO MODULO, CHE DOVRA' ESSERE COLLOCATO IN UNA BUSTA SIGILLATA. TALE PROCEDURA DEVE ESSERE ATTUATA ESCLUSIVAMENTE SE VI SIANO AREE DELL'ELABORATORE IN USO ALL'INCARICATO O DI ALTRA PERIFERICA AD ACCESSO ESCLUSIVO. LA BUSTA DEVE ESSERE CONSEGNATA NELLE MANI DEL SOGGETTO INCARICATO DAL TITOLARE DELLA CUSTODIA DELLE CREDENZIALI DI ACCESSO CHE PROVVEDERA' A POSIZIONARLA IN UN LUOGO SICURO (CASSAFORTE AD ESEMPIO). ALL'ESTERNO DELLA BUSTA DEVE ESSERE SCRITTO IL NOME UTENTE A CUI SI RIFERISCE LA PAROLA CHIAVE IN ESSA CONTENUTA ED I LEMBI DELLA STESSA DEVONO ESSERE CONTROFIRMATI DALL'INCARICATO INTERESSATO. QUALORA LA STESSA DEBBA ESSERE APERTA PER CASI DI ESTREMA NECESSITA' (PROLUNGATA ASSENZA DELL'INTERESSATO, MORTE, MALATTIA ETC.), DOVRA' ESSERE REDATTO UN BREVE PROCESSO VERBALE DA CUI SI EVINCA CHI HA ESEGUITO L'APERTURA E IN CHE GIORNO ED IN CHE ORA LA STESSA SIA AVVENUTA. QUANTO PRIMA, SE POSSIBILE, OCCORRE INFORMARE IL SOGGETTO INTERESSATO DELL'AVVENUTA APERTURA DELLA BUSTA.
PROCEDURE AFFINI	- PROCEDURA CHIAVI

PROCEDURA DISTRUZIONE DI DOCUMENTI

DESTINATARI	ASSISTENTI AMMINISTRATIVI COLLABORATORI SCOLASTICI ALTRI INCARICATI DEL TRATTAMENTO
APPLICABILITA'	TRATTAMENTO CORRENTE DI DOCUMENTI CARTACEI CONTENENTI DATI PERSONALI DA ELIMINARE IN QUANTO ECCEDENTI NEL NUMERO DI STAMPE, ERRATI O DA DISMETTERE IN SEGUITO AL RAGGIUNGIMENTO DEL TERMINE ULTIMO DI CUSTODIA O ALL'ACCOGLIMENTO DELLA DOMANDA DI OBLIO O PER OGNI ALTRO MOTIVO LEGITTIMO.
	TUTTI I DOCUMENTI IN FORMATO CARTACEO CONTENENTI DATI PERSONALI DI QUALSIASI NATURA CHE DEBBANO ESSERE ELIMINATI IN QUANTO ECCEDENTI NEL NUMERO DI STAMPE, ERRATI O DA DISMETTERE IN SEGUITO AL RAGGIUNGIMENTO DEL TERMINE ULTIMO DI CUSTODIA O ALL'ACCOGLIMENTO DELLA DOMANDA DI OBLIO O PER OGNI ALTRO MOTIVO LEGITTIMO, DEVONO ESSERE RESI COMPLETAMENTE ILLEGGIBILI MEDIANTE L'USO DI UN DISTRUGGIDOCUMENTI.
PROCEDURE AFFINI	- PROCEDURA DISTRUZONE DI DATI INFORMATICI

PROCEDURA SCRIVANIE PULITE	
DESTINATARI	ASSISTENTI AMMINISTRATIVI COLLABORATORI SCOLASTICI ALTRI INCARICATI DEL TRATTAMENTO
APPLICABILITA'	TRATTAMENTO CORRENTE DI DOCUMENTI CARTACEI CONTENENTI DATI PERSONALI
	GLI INCARICATI DEL TRATTAMENTO CHE STIANO ELABORANDO DOCUMENTI CARTACEI CONTENENTI DATI PERSONALI, QUANDO SI TROVANO A FINE TURNO OPPURE QUANDO SONO COSTRETTI AD UN ALLONTANAMENTO DALLA LORO POSTAZIONE PER LUNGO TEMPO, HANNO CURA DI RIPORRE OGNI DOCUMENTO CONTENENTE DATI PERSONALI NELL'ARMADIO, CASSETTIERA O CASSETTO LORO FORNITO CHIUDENDO LO STESSO A CHIAVE E PORTANDO CON SE LA CHIAVE DELLO STESSO O RIPONENDOLA NELLA CASSETTINA METALLICA A CIO' ADIBITA, LASCIANDO COSI' LA SCRIVANIA SGOMBRA DA QUALSIVOGLIA DOCUMENTO DI CARATTERE PERSONALE.
PROCEDURE AFFINI	- PROCEDURA CHIAVI

PROCEDURA DISTRUZIONE DI DATI INFORMATICI	
DESTINATARI	ASSISTENTI AMMINISTRATIVI COLLABORATORI SCOLASTICI ALTRI INCARICATI DEL TRATTAMENTO
APPLICABILITA'	TRATTAMENTO CORRENTE DI DOCUMENTI IN FORMATO DIGITALE CONTENENTI DATI PERSONALI DA ELIMINARE IN QUANTO ECCEDENTI NEL NUMERO DI COPIE, ERRATI O DA DISMETTERE IN SEGUITO AL RAGGIUNGIMENTO DEL TERMINE ULTIMO DI CUSTODIA O ALL'ACCOGLIMENTO DELLA DOMANDA DI OBLIO O PER OGNI ALTRO MOTIVO LEGITTIMO.
	TUTTI I DOCUMENTI IN FORMATO DIGITALE CONTENENTI DATI PERSONALI DI QUALSIASI NATURA CHE DEBBANO ESSERE ELIMINATI IN QUANTO ECCEDENTI NEL NUMERO DI COPIE, ERRATI O DA DISMETTERE IN SEGUITO AL RAGGIUNGIMENTO DEL TERMINE ULTIMO DI CUSTODIA O ALL'ACCOGLIMENTO DELLA DOMANDA DI OBLIO O PER OGNI ALTRO MOTIVO LEGITTIMO, DEVONO ESSERE RESI COMPLETAMENTE ILLEGGIBILI MEDIANTE L'USO DI UN SISTEMA DI DISTRUZIONE SICURO. IN CASO DI SOSTITUZIONE DI COMPUTER, SERVER ED ALTRI APPARECCHI INFORMATICI I DATI DEVONO ESSERE DISTRUTTI FISICAMENTE MEDIANTE SISTEMI DI SMAGNETIZZAZIONE (HARD DISK) O DI DEMOLIZIONE FISICA (PENDRIVE, SSD ETC.) IN ALTERNATIVA OCCORRE PROCEDERE CON SISTEMI SOFTWARE DI DISTRUZIONE BASATI SU RISCRITTURA PER TRE VOLTE DI TUTTI I SETTORI IN MODO CHE I DATI ORIGINALI NON SIANO PIU' RECUPERABILI.
PROCEDURE AFFINI	- PROCEDURA DISTRUZONE DI DOCUMENTI

DIFFUSIONE DEL MANUALE DELLE PROCEDURE PRIVACY

Il presente Manuale delle Procedure Privacy è a disposizione di chiunque, Titolare, Responsabile e Incaricato del trattamento dei dati personali, ne voglia prendere visione. Le procedure in esso contenute devono essere conosciute dettagliatamente da parte di tutti i soggetti che entrino in contatto con i dati personali a qualsiasi titolo.

REVISIONE

Il presente Manuale delle Procedure Privacy deve essere revisionato in ogni occasione in cui sia mutato almeno uno degli elementi essenziali presi in esame in occasione della sua redazione ed in occasione di ogni nuovo trattamento dati.

RIPE

REGOLAMENTO
per l'utilizzo di INTERNET e della POSTA ELETTRONICA

REDATTO AI SENSI E PER GLI EFFETTI DEL PROVVEDIMENTO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI PUBBLICATO SULLA GAZZETTA UFFICIALE N° 58 DEL 10 MARZO 2007.

MODELLO REV. 1.0

Redatto a cura e negli uffici del D.P.O. :

STUDIO TECNICO LEGALE
CORBELLINI
Studio AG.I.COM. S.r.l.

STUDIO AG.I.COM. S.R.L. UNIPERSONALE
Via XXV Aprile, 12 – 20070 SAN ZENONE AL LAMBRO (MI)
Tel. 02 90601324 Fax 02 700527180 info@agicomstudio.it

www.agicomstudio.it

I. ENTRATA IN VIGORE DEL REGOLAMENTO E PUBBLICITA'

Il nuovo regolamento entrerà in vigore il giorno successivo alla data di pubblicazione all'albo o della pubblicazione ai lavoratori interessati.
Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.
Copia del regolamento, oltre ad essere affisso in bacheca, verrà consegnato individualmente a ciascun utente informatico.

II. CAMPO DI APPLICAZIONE DEL REGOLAMENTO

Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori a prescindere dal rapporto contrattuale intrattenuto (lavoratori somministrati, collaboratori a progetto, in stage, ecc.).
Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente, ecc.) in possesso di specifiche credenziali di autenticazione.

III. UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.
Il Personal Computer dato in affidamento all'utente permette l'accesso alla rete solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto del presente Regolamento.

L'azienda/ente rende noto che il personale incaricato che opera presso il servizio di assistenza tecnica è stato autorizzato a compiere interventi nel sistema informatico diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware etc.).

Detti interventi potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività, si applica anche in caso di assenza prolungata od impedimento dell'utente.

Il personale incaricato del servizio di assistenza tecnica ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc.
L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità**,** a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio Tecnico, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.
L'inosservanza della presente disposizione espone l'azienda/ente a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

Salvo preventiva espressa autorizzazione del personale del Servizio Tecnico, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …).

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio Tecnico nel caso in cui siano rilevati virus ed adottando quanto previsto dal punto specifico del presente Regolamento relativo alle procedure di protezione antivirus.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso**.**

Una modalità automatica che evita di lasciare incustodito il pc, anche in caso di mancato spegnimento da parte dell'utente è quello di adottare il savescreen a tempo con obbligo di reintrodurre la password per l'accesso.

IV. GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio Tecnico, previa formale richiesta del Titolare del trattamento.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (USER-ID), assegnato dal Servizio Tecnico, associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Servizio Tecnico.

La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi (ogni tre mesi nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici).

Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del Servizio Tecnico.

V. UTILIZZO DELLA RETE

Per l'accesso alla rete ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parola chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

Le cartelle utenti presenti nei server di segreteria e di laboratorio sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del personale del Servizio Tecnico.
Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale incaricato del Servizio ICT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

In molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al custode; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'incaricato entro i termini massimi: in questi casi, vanno adattate le istruzioni contenute nel presente regolamento, eliminando, tra l'altro l'onere di comunicazione della variazione al custode delle credenziali.

Il personale del Servizio Tecnico può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Risulta opportuno 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.

VI. UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili, 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.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente potrà contattare il personale del Servizio Tecnico e seguire le istruzioni da questo impartite.

In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

E' vietato l'utilizzo di supporti rimovibili personali salvo che ciò non sia espressamente consentito dal responsabile dell'ufficio.

L'utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

VII. UTILIZZO DEI PERSONAL COMPUTER PORTATILI/TABLET/SMARTPHONE

L'utente è responsabile del PC portatile/Tablet o Smartphone assegnatogli dal Titolare del trattamento e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatile/Tablet o Smartphone si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

I PC portatile/Tablet o Smartphone utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

VIII. UTILIZZO DELLA POSTA ELETTRONICA

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica ufficiali per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del Servizio Tecnico.
  Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'azienda/ente ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Titolare del trattamento.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, …), devono essere autorizzate e firmate dal Titolare del trattamento, a seconda del loro contenuto e dei destinatari delle stesse.

È obbligatorio porre la massima attenzione nell'aprire i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

Al fine di garantire la funzionalità del servizio di posta elettronica e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) potrà essere configurato dal Servizio Tecnico in modo da inviare automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere attivata dall'utente.

In caso di assenza non programmata (ad es. per malattia) la procedura, qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni. potrà essere attivata a cura dell'azienda/ente.

Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dal Titolare del trattamento, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario.

Al fine di ribadire agli interlocutori la natura esclusivamente istituzionale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy.

IX. NAVIGAZIONE IN INTERNET

Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo che tale comportamento, durante l'orario di lavoro, sia espressamente autorizzato dal responsabile dell'ufficio.

In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Titolare del trattamento e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Titolare;

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, si rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.

Gli eventuali controlli, compiuti dal personale incaricato del Servizio Tecnico, ai sensi del precedente punto, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.

X. PROTEZIONE ANTIVIRUS

Il sistema informatico è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del Servizio Tecnico.

Ogni dispositivo magnetico di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio Tecnico.

XI. UTILIZZO DEI TELEFONI, FAX E FOTOCOPIATRICI

Il telefono 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 consentito solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso a disposizione.

Qualora venisse assegnato un cellulare all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare si applicano le medesime regole sopra previste per l'utilizzo del telefono : 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. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal personale del Servizio Tecnico.

È vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.

È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

XII. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati ai sensi del Regolamento UE 2016/679 (G.D.P.R.).

XIII. ACCESSO AI DATI TRATTATI DALL'UTENTE

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione, tramite il personale del Servizio Tecnico o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

XIV. SISTEMI DI CONTROLLO GRADUALE

In caso di anomalie, il personale incaricato del Servizio Tecnico effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
Controlli su base individuale potranno essere computi solo in caso di successive ulteriori anomalie.
In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

XV. SANZIONI

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, nonché con tutte le azioni civili e penali consentite.

In caso di abuso, a seconda della gravità del medesimo, e fatte salve le ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le seguenti sanzioni (D.Lgs 297 del 16 Aprile 1994 e Art. 2043 C.C.) :

a. Il richiamo verbale;
b. Il richiamo scritto;
c. Il risarcimento del danno provocato;

Le sanzioni sono comminate dal Datore di lavoro.

In caso abbia notizia di abuso e vi sia pericolo nel ritardo il Titolare del trattamento può ordinare l'immediata cessazione dell'attività all'origine dell'abuso adottando le necessarie misure per impedire che l'abuso venga portato ad ulteriori conseguenze.

Chiunque e con qualsiasi mezzo può segnalare al Titolare del trattamento o al Responsabile della rete violazioni di quanto previsto nel presente regolamento. Le segnalazioni anonime non vengono prese in considerazione.

Se il Titolare del trattamento ritiene infondata la segnalazione ne dà comunicazione motivata all'autore.
Se, al contrario, ritiene che la segnalazione sia fondata invita l'utente a fornire tutti i chiarimenti e i documenti che ritiene utili alla propria difesa assegnando un termine non inferiore a 10 giorni. L'utente può chiedere di essere ascoltato.

Se i chiarimenti sono ritenuti sufficienti, il Titolare del trattamento archivia il procedimento e ne dà comunicazione motivata all'autore della segnalazione.
Se invece accerta l'esistenza dell'abuso, commina le sanzioni previste ai commi precedenti motivando la decisione.

La decisione viene comunicata senza ritardo alle parti.

XVI. AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dal Titolare del trattamento.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

DATA E FIRMA PER RICEZIONE DEL REGOLAMENTO

DATA _____

TITOLARE DEL TRATTAMENTO

_____

INCARICATO DEL TRATTAMENTO

_____