Regolamento per la sicurezza e Privacy policy

Ultima revisione: gennaio 2023

Policy Aziendale

La presente Policy viene redatta da **AltaVita-Istituzioni Riunite di Assistenza- IRA,** con sede in Padova 35137 – Piazzale Mazzini, 14 - P.IVA 00558060281 - Tel. 049.8241511 Fax 049.8241531 Mail: segreteriagenerale@altavita.org PEC: altavita@legalmail.it WEB: www.altavita.org, di seguito definito Titolare.

Tale Policy si prefigge di pianificare un uso corretto delle risorse informatiche del Titolare.
Le finalità sono di natura operativa e di rispetto della sicurezza informatica.
La natura della presente Policy è obbligatoria, vincolante e informativa.
Il suo fine è regolamentare l'utilizzo delle risorse informatiche del Titolare da parte del personale dipendente e non dipendente, comunque ad essa legato da un contratto di lavoro subordinato, di prestazione d'opera occasionale, di prestazione di lavoro autonomo-libero professionale, di lavoro interinale.
Una copia della presente Policy viene consegnata ad ogni dipendente o collaboratore, che restituisce al Titolare una copia sottoscritta, così facendone integralmente proprio il contenuto.
L'inosservanza delle regole di comportamento contenute nella presente Policy configura illeciti disciplinari ai sensi di legge e di contratto, ferme restando le altre responsabilità civili, amministrative, penali.
La legge impone all'Ente di controllare il corretto impiego degli strumenti e attrezzature e di dettare le disposizioni per il corretto utilizzo degli stessi.
La presente Policy si pone l'obiettivo di creare una "buona pratica" nelle relazioni di lavoro improntate alla trasparenza, all'accordo e all'uniformità dei comportamenti.
Essa intende, pertanto, garantire il datore di lavoro, il quale ha diritto di richiedere una corretta esecuzione della prestazione lavorativa; ma anche i lavoratori che vengono, in tal modo, resi edotti della politica dell'Ente in materia di utilizzo di risorse informatiche.

Rispetto dello Statuto dei Lavoratori e della Disciplina della Privacy, del codice di comportamento e di quanto previsto nel D.lgs. 165/2001
La presente Policy intende regolamentare l'esercizio del potere di controllo, direttivo e disciplinare del Titolare nei confronti dei lavoratori nei limiti di legge e di contratto.
Il Titolare garantisce, in ogni caso, che non esistono presso il Titolare né intende adottare impianti audiovisivi e altre apparecchiature per finalità di controllo a distanza dei lavoratori; e garantisce in ogni caso di uniformare la propria attività a tutte le disposizioni di legge, regolamentari nonché di contratto vigenti.

Controllo del corretto utilizzo delle strutture aziendali
Gli artt. 2086 e 2104 C.C. riconoscono al Titolare il diritto di controllare il corretto utilizzo delle strutture dell'Ente.
L'art. 2087 C.C. impone al Titolare un generale obbligo di tutela dell'ambiente di lavoro e delle sue turbative.
Il Titolare è pertanto tenuto a controllare il corretto impiego degli strumenti dell'Ente e dettare le disposizioni per il corretto utilizzo degli stessi, di cui il Titolare assume la piena responsabilità nei confronti dei lavoratori e dei terzi.

Responsabilità nell'utilizzo delle risorse informatiche
I lavoratori sono tenuti ad un uso corretto delle risorse e attrezzature messe a loro disposizione per l'esecuzione dell'attività lavorativa. Essi rispondono dei danni eventualmente occorsi sia durante l'esecuzione della prestazione lavorativa sia al di fuori della medesima, fintanto che risorse e attrezzature rientrino nella loro disponibilità.

Obbligo di segretezza e responsabilità dei dati
I lavoratori si impegnano a non divulgare a terzi estranei al Titolare del Trattamento dati e informazioni di cui vengano a conoscenza per motivi di lavoro.
In particolare, essi si impegnano a mantenere il segreto e la massima riservatezza sui dati degli ospiti/utenti, fornitori, contratti, documenti, progetti. Essi sono responsabili dell'uso non corretto di tali dati e informazioni.
E' vietata altresì ogni tipo di ripresa audio e/o video all'interno della proprietà del Titolare senza l'autorizzazione del medesimo.

REGOLAMENTO PER L'USO DI INTERNET, DEI SOCIAL MEDIA E DEGLI STRUMENTI INFORMATICI

Principi generali.
La progressiva diffusione delle nuove tecnologie informatiche espone il Titolare ad un duplice rischio: da un lato, che il suo sistema informatico subisca danneggiamenti e/o sia sottoposto ad illecite interferenze o sottrazione di dati; dall'altro, che il Titolare venga ritenuto responsabile, anche sotto il profilo civile e/o penale e/o amministrativo, per la illecita diffusione e/o la illecita gestione o trattamenti di dati informatici. Tali rischi risultano particolarmente alti in quanto attengono da un lato alla sicurezza dei dati e dall'altro all'immagine del Titolare.
In tale quadro il Titolare ha adottato il presente Regolamento interno (di seguito anche "Regolamento") diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.
Le prescrizioni del Regolamento integrano le specifiche istruzioni già contenute nell'atto di nomina dei soggetti autorizzati in materia di trattamento dei dati personali, nonché le informative sul trattamento dei dati personali e le circolari di volta in volta inviate per l'aggiornamento in materia.
Il presente Regolamento si applica a tutti gli Autorizzati, Collaboratori del Titolare (di seguito anche "Autorizzati "o "Collaboratori").

Utilizzo del Personal Computer fisso di proprietà del Titolare.
I PC del Titolare (con tale espressione intendendosi, salvo diversa indicazione, sia le postazioni fisse che quelle portatili) sono forniti in dotazione per lo svolgimento di attività connesse allo svolgimento dell'attività lavorativa e professionale.
Il Titolare definisce per ogni postazione adeguate *policies* di sicurezza e provvede all'installazione degli applicativi necessari allo svolgimento delle attività proprie degli autorizzati ai quali sono assegnati i PC.
È vietato ogni utilizzo dei PC che contrasti con le politiche di sicurezza definite dal Titolare o che possa compromettere la sicurezza dei sistemi informatici del Titolare o esporre i dati al rischio di violazioni.
L'autorizzato è responsabile del PC assegnatogli e deve custodirlo con diligenza durante l'utilizzo nel luogo di lavoro.
Non è consentito modificare le impostazioni di rete, di sicurezza e di gestione dell'account autorizzato del proprio PC, se non previa autorizzazione esplicita del Titolare.
Non è consentita l'installazione sul proprio PC di alcuna periferica, interna od esterna, (come ad esempio masterizzatori, modem, schede grafiche, lettori di dispositivi di memoria), se non con l'autorizzazione espressa del Titolare.
Non è consentito installare autonomamente applicativi software diversi da quelli preinstallati, se non previa autorizzazione espressa del Titolare, in quanto sussiste il grave pericolo di importare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore e esporre il Titolare a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software.
Ad ogni Autorizzato è assegnato un account protetto da password per l'accesso al sistema operativo.
Non è consentita l'attivazione della password di accensione (c.d. Bios "Basic input/output system"), senza preventiva autorizzazione da parte del Titolare.
Non è consentito l'accesso contemporaneo di più persone con lo stesso account.
L'Autorizzato deve custodire la password con la massima diligenza e non deve divulgarla.
La *password* di accesso al sistema operativo deve essere cambiata con la cadenza periodica prevista nel rispetto delle misure di sicurezza adeguate al trattamento dei dati personali anche aventi natura c.d. particolare. A tal proposito, l'Autorizzato dovrà attenersi alle istruzioni fornite dal Titolare sulle modalità di scelta della *password*.
In tutti i casi in cui l'autorizzato deve assentarsi dalla propria postazione di lavoro (es. pausa pranzo, riunioni, fine orario di lavoro), il PC deve essere bloccato con password in quanto 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. In ogni caso deve essere attivata la funzionalità di blocco automatico con password con un tempo di attesa massimo di 10 minuti.
Su ogni PC è installato un applicativo antivirus/antimalware. L'Autorizzato non può interferire con il funzionamento dell'antivirus, disattivando la protezione o impedendone gli aggiornamenti. Nel caso che il software antivirus rilevi la presenza di un virus, l'Autorizzato dovrà immediatamente:
(a) sospendere ogni elaborazione in corso senza spegnere il computer;
(b) segnalare l'accaduto al Titolare.

Utilizzo di PC portatili e smartphone di proprietà del Titolare.
Il Titolare compila il MODELLO per la consegna dello strumento che viene sottoscritto da parte dell'Autorizzato.
Ai PC portatili, assegnati agli Autorizzati per lo svolgimento degli incarichi a loro affidati, si applicano le stesse disposizioni previste per le postazioni fisse. In caso di smarrimento o furto gli autorizzati sono tenuti ad informare il personale di segreteria del Titolare affinché il dispositivo sia bloccato, allegando nella comunicazione la denuncia presentata all'autorità di pubblica sicurezza.
L'utilizzo del device mobile fornito dal Titolare è disciplinato da apposite procedure e istruzioni d'uso che vengono accettate dall'Autorizzato mediante sottoscrizione di verbale di consegna del dispositivo.
Il numero di telefono autorizzato alla SIM fornita con il telefono mobile del Titolare non può essere mantenuto a titolo personale dall'Autorizzato, salvo diverso accordo o salvo che la numerazione sia stata autorizzata ad una SIM intestata al Titolare per portabilità del numero personale dell'Autorizzato.
Gli Autorizzati possono installare sui dispositivi mobili solo le applicazioni (c.d. *app*) che, in virtù dell'utilità ai fini professionali, vengono rese disponibili dal Titolare.
Gli Autorizzati sono tenuti a inserire un codice di blocco/sblocco del dispositivo se lo stesso risulta inutilizzato per periodi superiori a 30", oppure a utilizzare le equivalenti funzioni avanzate se disponibili (esempio sblocco con impronta digitale).
Al fine di garantire la sicurezza del dispositivo il Titolare può disporre, anche attraverso strumenti informatici *ad hoc*, misure quali:
a) obbligo di attivare un codice di accesso;
b) blocco degli applicativi aziendali da remoto;
c) blocco o ripristino alle impostazioni di fabbrica del dispositivo da remoto.
È vietato da parte del Titolare qualsiasi tipo di rilevazione, sistematica o puntuale, della posizione attraverso i sistemi di geo-localizzazione di cui i dispositivi sono eventualmente dotati. A ogni modo, sempre in sede di consegna, l'autorizzato dovrà essere informato delle modalità con cui potrà in qualsiasi momento disabilitare dal dispositivo la funzione di geolocalizzazione

Utilizzo di Personal Computer e Terminali mobili non di proprietà del Titolare in rete (BYOD: notebook, tablet e/o smartphone)
Tutto ciò che costituisce la dotazione delle risorse informatiche, l'accesso ad internet e la casella di posta elettronica con dominio aziendale appartengono al patrimonio aziendale tranne il device (BYOD: notebook, tablet e/o smartphone) di proprietà del collaboratore a cui è acconsentito utilizzare la rete con specifica deroga scritta.
I collaboratori autorizzati con specifica deroga scritta, pertanto, utilizzeranno le proprie risorse informatiche per fini professionali per il perseguimento degli obiettivi fissati dal Titolare.
Potrebbe essere prevista la creazione di account diverso a cura dell'Amministratore di Sistema individuato dal Titolare.
Il Titolare nel caso di concessione di utilizzo di device non di proprietà stabilisce quali sistemi di sicurezza adottare e potrà agire in remoto per rimuovere rischi per i dati aziendali. Per la sicurezza della rete i dispositivi potrebbero essere sottoposti a controlli da parte del Titolare del trattamento dei dati e dall'Operatore di Sistema-Tecnico incaricato minimo ogni 3 (tre) mesi.
E' vietato l'uso di device mobili personali durante l'orario di servizio per la gestione della comunicazione e altre attività per conto dell'Ente anche verso l'esterno.
È vietato qualsiasi tipo di rilevazione, sistematica o puntuale, della posizione attraverso i sistemi di geo-localizzazione di cui i dispositivi possono essere eventualmente dotati a seguito di settaggio da parte del Titolare.

Gestione delle credenziali di accesso.
Le credenziali di accesso alla rete locale, degli *account* autorizzato relativi a servizi del Titolare (ad esempio e-mail o servizi cloud), di accesso alla rete locale ed al sistema operativo, degli account del Titolare relativi a piattaforme ed applicativi, devono essere custodite con la massima cura da parte dell'Autorizzato.
Tutte le *password* personali devono essere cambiate a cura dell'Autorizzato con la cadenza periodica prevista nel rispetto delle misure di sicurezza adeguate al trattamento dei dati personali anche aventi natura c.d. particolare nonché in base alle istruzioni che verranno di volta in volta fornite dal Titolare.
Le *password* possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'Autorizzato. Non possono essere utilizzate *password* già impiegate per usi personali.
La *password* deve contenere almeno un carattere alfabetico ed uno numerico, non deve contenere più di due caratteri identici consecutivi, non deve contenere il nome dell'autorizzato come parte della password e non deve essere simile alle ultime 5 password precedenti.

La password deve essere immediatamente sostituita nel caso si sospetti che la stessa abbia perso la segretezza o sia stata persa.
Qualora l'autorizzato venisse a conoscenza delle *password* di altro autorizzato, è tenuto a darne immediata notizia al Titolare.
È vietata la creazione di credenziali di accesso per account o servizi di uso personale utilizzando l'indirizzo e-mail sul dominio o il numero di cellulare assegnato dal Titolare e destinato a ritornare nella sua disponibilità al termine della collaborazione. È vietato utilizzare per account o servizi di uso personale le stesse *password* utilizzate per account o servizi del Titolare.

Utilizzo di dispositivi di memorizzazione esterni. Scambio di documenti e informazioni. Utilizzo Social Media
Tutti i supporti magnetici riutilizzabili (es. hard disk esterni, schede di memoria, chiavette USB) devono essere trattati con particolare cautela onde evitare che il loro contenuto – una volta cancellato – possa essere recuperato.
I supporti magnetici contenenti dati particolari (vale a dire sensibili) e giudiziari devono essere custoditi in archivi chiusi a chiave. La loro cancellazione deve essere effettuata per mezzo di appositi programmi che verranno installati a cura del Titolare.
Non è in nessun caso consentito collegare al proprio PC dispositivi di memorizzazione esterni per scopi non strettamente connessi alla propria collaborazione professionale.
È sconsigliato l'utilizzo di supporti di memorizzazione esterni per lo scambio di documenti, all'interno della struttura o con terzi.
In ogni caso, devono essere utilizzati esclusivamente dispositivi di memorizzazione esterni approvati dal Titolare, utilizzando adeguate forme di sicurezza (es. cifratura del disco).
Ove possibile, deve essere preferito lo scambio attraverso servizi di condivisione documentale affidabili (es. Cloud, servizi OneDrive e SharePoint del Titolare).
È vietata la condivisione di documenti contenenti dati personali trattati dal Titolare attraverso servizi pubblici o account con licenza per uso privato (es. WeTransfer, account Dropbox o Google Drive personali).
È vietata la comunicazione di dati personali o documenti attraverso servizi di messaggistica istantanea diversi da quelli approvati.
In particolare, è vietato l'uso per la condivisione di comunicazioni professionali o dati del Titolare con servizi WhatsApp, Telegram e Facebook Messenger mediante dispositivi personali.
Tutti i file di provenienza incerta, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo ed alla relativa autorizzazione da parte del Titolare e dell'Operatore di Sistema – Tecnico incaricato.
Ogni dispositivo magnetico di provenienza esterna al Titolare dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e nel caso venga rilevato un virus, dovrà essere consegnato al Titolare.

Utilizzo della posta elettronica.
Ad ogni Autorizzato è attribuita una casella di posta elettronica attestata sul dominio del Titolare (@**altavita.org**). La casella di posta elettronica è attivata per lo scambio di comunicazioni a carattere professionale. Non è pertanto consentito utilizzare le caselle di posta elettronica di dominio @**altavita.org** per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione del Titolare o comunque per inviare messaggi estranei al rapporto di lavoro.
Le caselle di posta condivise tra più autorizzati devono essere utilizzate esclusivamente per le finalità per le quali sono state create. Le comunicazioni a carattere riservato devono essere archiviate separatamente e rimosse dalla casella condivisa.
Prima dell'invio di un messaggio di posta elettronica, l'Autorizzato deve verificare la correttezza dell'indirizzo del destinatario e la correttezza degli eventuali allegati. Qualora si accorga che è stato inviato un messaggio di posta elettronica contenente dati personali al destinatario sbagliato il Collaboratore è tenuto a richiedere immediatamente al destinatario di cancellare il messaggio e a segnalare l'evento al Titolare.
Ciascun autorizzato è tenuto a verificare periodicamente il contenuto della propria casella di posta elettronica ed a eliminare i messaggi non necessari.
Ciascun autorizzato è tenuto verificare con la massima cura la provenienza ed il contenuto dei messaggi di posta elettronica, accertandosi che il messaggio provenga effettivamente dal mittente indicato e che non contenga comunicazioni od allegati sospetti. Ciascun Autorizzato dovrà segnalare al Titolare ogni situazione anomala rappresentata da: ricevimento di messaggi indesiderati in numero manifestamente superiore all'ordinario, ricevimento di messaggi di posta con mittente non coerente con il testo/oggetto della mail, ricevimento di messaggi di posta elettronica non attesi che richiedono l'inserimento di credenziali.

L'Autorizzato non deve aprire allegati a messaggi di posta elettronica in formato eseguibile (.exe) ed, in genere, documenti allegati a messaggi di provenienza sospetta.
La condivisione di documenti informatici e *files* all'interno del Titolare e con terzi dovrebbe avvenire, per quanto possibile, attraverso le piattaforme di condivisione documentale gestite dal Titolare (es. cartelle di rete, cloud interno, servizio Onedrive e Sharepoint) limitando la condivisione di copie a mezzo e-mail.
In relazione al carattere strettamente professionale e non personale dalla casella di posta elettronica gli Autorizzati della stessa sono tenuti a verificare che in calce ad ogni e-mail vi sia il seguente testo:
"Ai sensi dell'art. 13 Regolamento UE n. 679/2016, si comunica che le informazioni del presente messaggio sono riservate e specificatamente indirizzate al destinatario indicato (oppure alla persona responsabile di rimetterlo al destinatario). E' necessario tener presente che è vietato qualsiasi uso, riproduzione o divulgazione di questo messaggio. Nel caso in cui aveste ricevuto questo messaggio per errore, vogliate cortesemente avvertire il mittente e di seguito distruggerlo. Il messaggio di cui alla presente comunicazione non riveste carattere personale e può essere trattato all'interno dell'Istituto AltaVita-Istituzioni Riunite di Assistenza-IRA di Padova.
I dati personali trattati con l'invio della presente e-mail (oggetto, contenuto, destinatari ed eventuali allegati) sono trattati nel rispetto del Regolamento generale sulla protezione dei dati UE n. 679/2016 e della normativa vigente in materia di privacy. Informativa completa sul sito: www.altavita.org"

Utilizzo della rete Internet.
Il Titolare adotta una politica di sicurezza volta a limitare l'accesso a risorse della rete pubblica attraverso le connessioni del Titolare. Ciascun autorizzato è tenuto ad osservare le *policies* e ad evitare condotte che possano esporre i sistemi informatici del Titolare ed i dati da esso trattati al pericolo di violazioni. In particolare, è vietato:

- scaricare qualsiasi tipo di software anche se freeware (gratuito), shareware (di modico costo) o trial (di prova) da siti Internet, se non espressamente autorizzato dal Titolare;
- scaricare qualsiasi tipo di file non attinente all'attività professionale ed in particolare lo scaricamento di file musicali, immagini e video se non con espressa autorizzazione del Titolare;
- accedere a siti internet non consentiti dalle *policies* di sicurezza o eludere i blocchi alla navigazione;
- partecipare a Forum non professionali, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames);
- utilizzare qualsiasi tipo di applicazione di messaggistica istantanea e/o chat line per fini non attinenti all'attività lavorativa;
- utilizzare, salva espressa autorizzazione dal Titolare, programmi di: streaming (audio, video o altro), condivisioni internet di file o altre risorse;
- registrarsi a siti i cui contenuti non siano legati all'attività professionale.

Verifiche sulla navigazione Internet.
La navigazione internet deve essere effettuata con i programmi Microsoft Edge, Mozilla Firefox e Google Chrome od Opera; è vietato l'utilizzo di altri programmi di navigazione salvo diversa ed esplicita autorizzazione scritta del Titolare.
L'utilizzo del browser comporta la registrazione temporanea di file nel PC che non è configurato per cancellarli automaticamente alla fine della sessione di lavoro.
Gli autorizzati possono cancellare autonomamente tali files mediante gli apposti comandi "Elimina Cookie ..." ed "Elimina file ..." del programma.
L'accesso ad Internet è protetto da un firewall che registra in modo centralizzato le attività degli ultimi 30 giorni.
Le apparecchiature di rete preposte al collegamento verso internet memorizzano un giornale (file di log) contenente le informazioni relative ai siti che le postazioni di lavoro hanno visitato, nei limiti dei tempi di registrazione sopra indicati.
Tale archivio memorizza l'indirizzo fisico delle postazioni di lavoro e non i riferimenti dell'autorizzato, garantendo in tal modo il suo anonimato.
Il controllo verrà effettuato rispettando il principio della gradualità ed i principi di pertinenza e non eccedenza.
La prima analisi delle registrazioni sarà effettuata senza differenziazione per autorizzato.
L'eventuale problema individuato verrà segnalato all'utenza e verrà indicato contestualmente il comportamento da tenere per risolverlo.
In caso di persistenza del problema verrà effettuata una seconda analisi differenziata per gruppo di autorizzati o per gruppo di computer (se possibile).
L'eventuale problema individuato verrà segnalato all'utenza del gruppo e verrà indicato contestualmente il comportamento da tenere per risolverlo.
Solo nel caso in cui i due controlli di cui sopra e le relative azioni correttive non abbiano sortito alcun risultato sarà effettuata l'analisi individuale.

Anche in quest'ultimo caso l'eventuale problema individuato verrà segnalato all'autorizzato e verrà indicato contestualmente il comportamento da tenere per risolverlo.
Nel caso in cui gli incaricati dell'assistenza e della manutenzione degli strumenti elettronici effettuino controlli sul singolo autorizzato quest'ultimo sarà preventivamente informato in forma scritta e le finalità della verifica dovranno essere espressamente indicate.

Organizzazione della sicurezza informatica
Il Titolare ha affidato l'organizzazione, la gestione, la verifica ed il controllo sull'utilizzo di tutti gli strumenti informatici previsti nel presente Regolamento a Strutture e/o persone qualificate (Operatore di Sistema-Tecnico incaricato anche con affidamento a Ditta esterna incaricata), cui tutti i settori e servizi dovranno fare riferimento.
Per le sedi del Titolare è stato designato un Referente dei sistemi informativi. I Collaboratori dovranno fare riferimento al Referente indicato per la loro sede di riferimento.
Salvo tutto quanto previsto nelle precedenti specifiche disposizioni del Regolamento, l'Operatore di Sistema-Tecnico incaricato per l'espletamento delle sue funzioni:
- ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna in casi specifici ed autorizzati dal Titolare, previo cambio password;
- può accedere ai dati ed agli strumenti informatici esclusivamente per permettere al Titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dal Titolare, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività professionale nei casi in cui si renda indispensabile ed indifferibile l'intervento (ad esempio in caso di prolungata assenza od impedimento dell'Autorizzato, informando tempestivamente questo ultimo dell'intervento di accesso realizzato);
- può in qualunque momento procedere alla rimozione di ogni file o dell'applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli Autorizzati sia sulle unità di rete;
- provvede a segnalare al personale di segreteria preposto le anomalie sull'utilizzo degli strumenti informatici previsti nel Regolamento che possano essere configurate quali attività non conformi.

Disposizioni finali.
Al termine del rapporto di collaborazione professionale, il Titolare disattiverà l'account di posta elettronica dell'Autorizzato. Verranno altresì disattivati tutti gli account personali dell'autorizzato relativi ai servizi informatici del Titolare.
Al termine del rapporto di collaborazione col Titolare, il Collaboratore dovrà distruggere tutte le copie delle credenziali di accesso ad account condivisi relativi a servizi del Titolare.
Al termine del rapporto di collaborazione, l'Autorizzato riconsegnerà i PC portatili e gli smartphone del Titolare sottoscrivendo apposito verbale di riconsegna. Per quanto concerne le attività di cancellazione e distruzione dei dati personali contenuti negli archivi di posta elettronica il Titolare si atterrà alle procedure adottate nel rispetto delle norme di legge, di settore, nonché deontologiche. In ogni caso, il rapporto di mandato professionale congiunto o disgiunto degli Autorizzati il Titolare viene regolato da specifico accordo;
Gli Autorizzati possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Titolare.

ISTRUZIONI FINALIZZATE AL CONTROLLO E LA CUSTODIA DEGLI ATTI E DOCUMENTI CONTENENTI DATI PERSONALI

Istruzioni particolareggiate applicabili al trattamento di dati personali

- Il Titolare ha messo a disposizione archivi e scaffali (luogo sicuro), ove sono di norma custoditi i documenti contenenti dati personali; come regola generale, tali documenti non devono essere asportati da tale luogo sicuro e, ove ciò avvenga, la asportazione deve essere ridotta al minimo tempo necessario per effettuare le operazioni di trattamento.
- Dal luogo sicuro devono essere asportati solo i documenti strettamente necessari per le operazioni di trattamento e non intere pratiche, se ciò non è necessario.
- Al termine delle operazioni di trattamento, i documenti devono essere immediatamente riposti nel luogo sicuro.
- Per tutto il periodo in cui i documenti sono all'esterno del luogo sicuro, l'incaricato non deve mai perderli di vista, adempiendo ad un preciso obbligo di custodia dei documenti stessi.
- L'incaricato deve inoltre controllare che i documenti, composti da numerose pagine o più raccoglitori, siano sempre completi, verificando che sia il numero dei fogli che l'integrità del contenuto, rispetto a quanto presente, all'atto del prelievo dal luogo sicuro.
- Se si debbono abbandonare, ad esempio di sera, in ufficio o al termine dell'orario di lavoro, gli anzidetti documenti, l'incaricato deve identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione da accessi non autorizzati (un armadio chiuso a chiave, un cassetto chiuso a chiave, una cassaforte, un armadio blindato, un classificatore chiuso a chiave); ove si utilizzi un contenitore chiuso a chiave, di qualunque natura, occorre accertarsi che non esistano duplicati abusivi delle chiavi e che tutte le chiavi siano in possesso solo di incaricati autorizzati.
- I documenti di cui sopra non devono essere mai lasciati incustoditi sul tavolo durante il giorno.
- Ci si deve in particolare accertare che un visitatore o terzo (addetto alla manutenzione, addetto alle pulizie, collega non autorizzato) possa entrare in ufficio anche non invitato o per cause accidentali, non possa venire a conoscenza dei contenuti dei documenti (attenti alla lettura alla rovescia!).
- Si deve adottare una procedura per la consegna delle copie con dati personali e/o particolari ai destinatari, che dia tutte le garanzie di sicurezza, in particolare utilizzando buste di sicurezza sigillate, oppure effettuando la consegna personalmente, di modo da ridurre al minimo la possibilità che soggetti terzi non autorizzati possano prendere visione del contenuto, od addirittura fotocopiarlo dall'insaputa del mittente e destinatario.
- Documenti contenenti dati particolari o dati che, per una qualunque ragione, siano stati indicati dal responsabile come meritevoli di particolare attenzione, in fase di affidamento, devono essere custoditi con misure più rigide, rispetto a quelle sinora indicate (per eventuali ulteriori informazioni, rivolgersi al responsabile di settore).
- Nel caso la consegna degli originali o delle fotocopie dei documenti avvenga per posta, si utilizzi la spedizione con uno strumento che garantisca un continuo tracciamento del movimento del documento e una sicura consegna al destinatario.
- Quale che sia il tipo di spedizione adottato, ci si accerti che esso consenta di avere prova certa del fatto che il destinatario ha effettivamente ricevuto i documenti inviati e che essi sono giunti integri, e quindi non manomessi o alterati in fase di trasporto.
- Eventuali fotocopie non riuscite bene debbono essere distrutte in un apposito distruggi-documenti, se disponibile, oppure devono essere strappate in pezzi talmente piccoli, da non consentire in alcun modo la ricostruzione del contenuto, che deve essere comunque illeggibile.
- È tassativamente proibito utilizzare le fotocopie non riuscite come carta per appunti.
- È parimenti tassativamente proibito trasportare all'esterno del posto di lavoro fotocopie non riuscite, da utilizzare altrove come carta per appunti.
- Quando i documenti devono essere trasportati all'esterno del luogo di lavoro, l'incaricato deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti; deve inoltre evitare che sia possibile esaminare, da parte di un soggetto terzo non autorizzato, anche solo la copertina del documento in questione.
- Durante il trasporto, la cartella non deve essere mai lasciata incustodita e preferibilmente deve essere tenuta chiusa a chiave o devono essere azionate le serrature a combinazione presenti sulla cartella o valigia.
- È tassativamente proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il corrispondente sia un incaricato, il cui profilo di autorizzazione sia tale da potere trattare i dati in questione.
- Si raccomanda vivamente non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando cellulari all'esterno dell'azienda o anche all'interno, in presenza di terzi non autorizzati, per evitare che dati personali possano venire a conoscenza di terzi non autorizzati,

anche accidentalmente. Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico od aperto al pubblico.
In caso di dubbio sulle modalità di applicazione di quanto sopra illustrato, o per chiedere ulteriori chiarimenti in merito, l'incaricato deve rivolgersi al proprio Responsabile di Settore.