DISCIPLINARE INTERNO UTILIZZO STRUMENTI DI LAVORO



**SOMMARIO**

[POLITICHE GENERALI PER L’UTILIZZO DI DISPOSITIVI E STRUMENTI INFORMATICI 2](#_Toc83227985)

[Titolarità, autorizzazione e finalità di utilizzo degli strumenti informatici 2](#_Toc83227986)

[Postazioni di lavoro 2](#_Toc83227987)

[SISTEMI DI PROTEZIONE DEI DATI 7](#_Toc83227988)

[Credenziali di autenticazione 7](#_Toc83227989)

[Scelta della password 7](#_Toc83227990)

[Antivirus 9](#_Toc83227991)

[Sistemi di backup 9](#_Toc83227992)

[OPERATIVITÀ SU BANCHE DATI 10](#_Toc83227993)

[SERVIZI DI RETE 10](#_Toc83227994)

[UTILIZZO DI INTERNET 12](#_Toc83227995)

[POSTA ELETTRONICA 14](#_Toc83227996)

[COLLEGAMENTO REMOTO 17](#_Toc83227997)

[*\*SISTEMI DI TELEFONIA* 17](#_Toc83227998)

[ACCESSO AI SISTEMI 17](#_Toc83227999)

[PROTEZIONE DEI DATI – TECNICHE DI SOTTRAZIONE 19](#_Toc83228000)

[Il social engineering 19](#_Toc83228001)

[L’E-mail phishing 19](#_Toc83228002)

[POLITICHE GENERALI PER L’UTILIZZO DEGLI ARCHIVI CARTACEI 21](#_Toc83228003)

# POLITICHE GENERALI PER L’UTILIZZO DI DISPOSITIVI E STRUMENTI INFORMATICI

## Titolarità, autorizzazione e finalità di utilizzo degli strumenti informatici

Il Consiglio regionale della Basilicata è titolare dei dispositivi e degli strumenti informatici che vengono messi a disposizione del personale ai fini dell’esecuzione dell’attività lavorativa nonché di tutte le informazioni, le registrazioni ed i dati inerenti all’esercizio della propria attività che siano contenuti e/o trattati mediante utilizzo di tecnologie informatiche.

Ad ogni dipendente e/o collaboratore può essere assegnato uno o più dispositivi e strumenti informatici (personal computer, laptop, palmare, cellulare, etc.), tramite cui è possibile accedere ad una serie di risorse che possono essere fisicamente ubicate all'interno dei locali del Consiglio regionale o all'esterno della stessa.

L’autorizzazione all’utilizzo dei dispositivi e degli strumenti informatici, quali a titolo esemplificativo e non esaustivo l’accesso alle risorse della rete del Consiglio regionale, alla posta elettronica e ad Internet, concessa al dipendente al momento dell’assunzione o all’inizio del rapporto con il collaboratore, può essere revocata in qualsiasi momento da parte del Consiglio regionale.

L’utilizzo degli strumenti e delle risorse informative del Consiglio regionale deve essere strettamente vincolato all’esercizio delle attività lavorative, rispettando le normative interne e in ottemperanza alle disposizioni legislative vigenti. È proibito l’impiego delle risorse del Consiglio regionale per scopi personali o di terzi.

In particolare, si fa divieto esplicito di:

* Utilizzare le risorse per profitto personale;
* Impiegare le risorse per finalità diverse da quelle per le quali sono state progettate o utilizzare i sistemi informativi per compiere azioni illecite nei confronti di altri sistemi, sia interni che esterni, all’organizzazione;
* Recare volontariamente danni alle risorse del Consiglio regionale, ai sistemi informatici di pubblica utilità, agli strumenti di supporto, ai locali ed in generale ai dispositivi informatici utilizzati dall’organizzazione.

Ogni strumento o risorsa, concessa ai fini esclusivamente lavorativi, deve essere correttamente custodito e mantenuto in buono stato dall’utente che deve contribuire, in rapporto alle proprie responsabilità, alla protezione del patrimonio del Consiglio regionale.

## Postazioni di lavoro

La Postazione di Lavoro (di seguito postazione) è costituita dall’insieme di componenti hardware e software forniti all’utente o di proprietà dell’utente ed autorizzate dal rispettivo ente; essa consente l’accesso al complesso dei sistemi e servizi resi disponibili.

L’utente è consapevole e accetta di restituire la totalità delle risorse utilizzate nel momento in cui cessa il rapporto con ciascun ente. Ogni utente, di norma, è assegnatario o autorizzato all’uso di una sola postazione, fissa o mobile; è responsabile della medesima e deve custodirla con diligenza (sia all’interno dell’edificio del Consiglio regionale, sia al di fuori), nonché segnalare eventuali furti, danneggiamenti o smarrimenti.

Inoltre, è tenuto a prestare la massima collaborazione sia alle attività di censimento ed inventario delle risorse hardware e software, sia alle attività di aggiornamento di tali risorse.

**Utilizzo del Personal Computer**

Il Personal Computer (PC) installato presso la Postazione di Lavoro o fornito all’Utente è configurato in modo ottimale, tenuto conto delle necessità professionali e lavorative.

Il PC affidato al dipendente o collaboratore è uno strumento di lavoro; non ne è pertanto consentita l’utilizzazione non inerente all’attività lavorativa. A tale scopo l’utente potrà utilizzare le risorse disponibili sul proprio PC e dovrà salvare, se necessario, ogni appunto creato sulla memoria di massa del PC stesso (disco locale).

Il PC deve essere custodito con cura evitando ogni possibile forma di uso non autorizzato o di danneggiamento. Il PC dato in affidamento all’utente permette l’accesso alla rete del Consiglio regionale solo attraverso specifiche credenziali di autenticazione, secondo le “regole” definite dalil Consiglio regionale stessa.

Il PC che viene consegnato all’Utente contiene tutti i software necessari a svolgere gli incarichi affidati. Alla cessazione del rapporto intercorso con l’utente, il Personal Computer dovrà essere restituito nella sua interezza, comprese eventuali periferiche interne ed esterne.

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dalil Consiglio regionale, né viene consentito agli utenti di installare autonomamente programmi di qualsivoglia natura, 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 il Consiglio regionale 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 Consiglio regionale, 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, ecc.

In ogni caso, all’utente non è consentito:

* modificare le configurazioni già impostate sul PC consegnato;
* modificare impostazioni di sistema che abbiano un impatto sulla sicurezza o la funzionalità del sistema;
* impedire in qualsiasi modo (personal firewall, cambio di diritti di accesso, rimozione delle condivisioni di sistema, ecc.) l’accesso al software installato sul proprio PC e ai documenti ivi registrati;
* utilizzare programmi e/o sistemi di crittografia senza la preventiva autorizzazione scritta del Consiglio regionale;
* installare alcun software né alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul PC consegnato, senza l’espressa autorizzazione del Consiglio regionale;
* fare copia del software installato al fine di farne un uso personale;
* fare copia dei documenti del Consiglio regionale in modo diverso dalla copia di back-up prevista dalle procedure interne;
* caricare alcun documento, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate;
* aggiungere o collegare dispositivi hardware (hard disk, drive, PMC, USB, seriale, firewall ecc.) o periferiche (telecamere, macchine fotografiche ecc.) diversi da quelli consegnati, senza l’autorizzazione espressa del Consiglio regionale;
* creare o diffondere programmi idonei a danneggiare il sistema informatico del Consiglio regionale, quali per esempio virus, trojan horses, ecc.;
* impostare connessioni private ad Internet o ad altre reti, ovvero connessioni private di comunicazione verso dispositivi mobili (telefoni cellulari e palmari) (ad es. Bluetooth);
* rimuovere la protezione automatica all’accesso al PC, ovvero lo screensaver a tempo (max 10 minuti);
* utilizzare il PC per scopi privati e comunque non inerenti all’attività lavorativa, salvo quanto specificato riguardo le modalità di utilizzo di Internet e della posta elettronica di seguito riportate.

Al fine di ridurre al minimo i rischi sopra evidenziati, non vengono concessi diritti di Amministratore del sistema operativo e, in caso di necessità, possono essere automaticamente forzate alcune impostazioni di sicurezza (ad esempio lo screensaver con password). I dischi fissi locali del PC sono gestiti sotto la responsabilità dell’utente che deve preoccuparsi di salvare, cancellare e proteggere le informazioni ivi presenti. Al momento della restituzione del PC, tutti i dati presenti sulla memoria di massa locale vengono definitivamente cancellati senza effettuarne alcuna copia.

Ogni utente è tenuto ad operare, con la necessaria diligenza, la custodia dei dati salvati sul proprio PC e non in rete. Considerato che i dati potrebbero accidentalmente essere perduti o danneggiati, l’utente deve valutare se conservare copia dei files presenti registrati sul disco fisso del proprio PC. Se l’eventuale copia fosse effettuata su supporti informatici (dispositivi USB, CD-ROM, DVD, Memory Card, Cellulari ecc.) gli stessi dovranno essere custoditi in modo adeguato al tipo di informazioni contenute e dovranno essere distrutti o cancellati quando le suddette informazioni non saranno più utili.

Nell’utilizzo della postazione di lavoro è opportuno non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

È opportuno terminare la sessione di lavoro svolta tramite utilizzo di un personal computer, ogni volta che ci si deve allontanare, anche solo per un breve periodo, effettuando il “log out” dell’account utente o mettendo in atto accorgimenti tali per cui il PC non resti:

* incustodito: può essere sufficiente, a titolo esemplificativo, che un collega rimanga nella stanza durante l'assenza di chi sta utilizzando il PC anche se la stanza rimane aperta;
* accessibile: può essere sufficiente chiudere a chiave la stanza all’interno della quale è situato lo strumento elettronico.

Non devono mai verificarsi situazioni in cui un Personal Computer venga lasciato attivo, durante una sessione di trattamento, senza che sia controllato da un Autorizzato al trattamento o senza che la stanza in cui è ubicato venga chiusa a chiave.

È possibile predisporre strumenti software specifici (es.: screen saver) che, trascorso un breve periodo di tempo predeterminato in cui l'elaboratore resta inutilizzato, non consente più l'accesso all'elaboratore se non previo inserimento di credenziali di accesso (es.: password, ecc.).

L’utente è tenuto a dare tempestiva segnalazione ai referenti IT di eventuali anomalie o irregolarità nel funzionamento del PC consegnato, al fine di prevenire la perdita totale o parziale della riservatezza, integrità e/o disponibilità delle informazioni in esso contenute nonché di prevenire eventuali guasti all’intero sistema. All’utente non è consentito stampare un documento elettronico, contenente informazioni riservate, trasformandolo in un documento cartaceo, se non solo ed esclusivamente per esigenze di lavoro. In tale ipotesi, il grado di riservatezza e segretezza delle informazioni contenute nel documento cartaceo dovrà ritenersi esattamente equivalente a quello delle medesime informazioni contenute nel documento elettronico trasformato mediante stampa. L’utente dovrà assicurare alle informazioni riservate contenute nel documento cartaceo una protezione adeguata ed equivalente a quella richiesta per i documenti elettronici corrispondenti.

Per ogni necessità interna, il personale espressamente incaricato ed autorizzato dalil Consiglio regionale quale Amministratore di Sistema potrà accedere alla memoria di massa locale del PC e ai server nonché, previa comunicazione all’utente, accedere al PC di quest’ultimo anche in modalità “da remoto”.

Al personale espressamente incaricato dalil Consiglio regionale quale Amministratore di Sistema è riconosciuta 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.

Inoltre, dal momento che la violazione delle regole di cui sopra potrebbe esporre il Consiglio regionale al rischio di danneggiamento del sistema informatico, il loro rispetto potrebbe essere oggetto di controllo attraverso periodiche verifiche del contenuto della memoria di massa dei server oltre che del PC consegnato.

**Utilizzo di dispositivi rimovibili**

La postazione e gli eventuali supporti di memoria rimovibili (CD, chiavi USB, memory card ecc.) devono essere conservati in luoghi protetti; è sempre necessario verificare il contenuto informativo dei supporti di memoria, prima della loro consegna a terzi e prima della loro eliminazione / distruzione. L'utente non è autorizzato ad accedere, né a tentare l’accesso alle informazioni per le quali non ha alcun privilegio; è altresì vietato tentare di guadagnare privilegi non concessi dal proprietario del dato.

Tutti i supporti magnetici rimovibili (CD, DVD riscrivibili, supporti USB, memory card, cellulari ecc.), contenenti dati “sensibili” nonché informazioni costituenti patrimonio del Consiglio regionale, 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”, ogni utente dovrà contattare il personale IT del Consiglio regionale e seguire le istruzioni da questo impartite. In ogni caso, i supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti in armadi chiusi. L’utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

# SISTEMI DI PROTEZIONE DEI DATI

## Credenziali di autenticazione

Le credenziali di autenticazione ai sistemi informatici, generalmente composte da un “identificativo utente” (c.d. username o user) al quale è associata una specifica “password”, sono informazioni di carattere assolutamente personale e non cedibili, per nessuna ragione.

Se si è in possesso di più credenziali di autenticazione, è necessario fare attenzione ad accedere ai dati unicamente con le credenziali relative al trattamento in oggetto. Nell’utilizzo delle credenziali di autenticazione l’utente è tenuto a rispettare:

- l'ambito di competenza assegnato;

- le base dati a cui poter accedere;

- il profilo di autorizzazione assegnato;

- le tipologie di trattamento consentito;

segnalando tempestivamente eventuali anomalie e/o malfunzionamenti riscontrati.

## Scelta della password

Elaborare le password seguendo le istruzioni sotto riportate.

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

Di norma la password deve essere composta da **almeno otto caratteri** o, se il sistema non l'accetta, da un numero di caratteri pari a quello consentito dal sistema; è buona norma che, di questi caratteri, da un quarto alla metà siano di natura numerica.

L’utente deve provvedere a modificare la password immediatamente, non appena la riceve per la prima volta, da chi amministra il sistema.

La password deve essere modificata dall'utente con una frequenza di **almeno 6 mesi** o nel caso in cui il sistema lo preveda, alle scadenze proposte dal sistema stesso.

Se il trattamento riguarda categorie particolari di dati o dati di natura giudiziaria, la password deve essere modificata con frequenza maggiore (es.: **ogni 3 mesi**).

Di seguito sono riportate alcune indicazioni “utili” per la scelta di una password

**Cose da fare**

* Creare password lunghe e/o utilizzare più di una parola (a volte è più semplice ricordare una frase completa di senso compiuto piuttosto che una parola complicata, e questa tecnica oltre a facilitare la memorizzazione migliora la sicurezza stessa della parola chiave: la lunghezza influisce sulle difficoltà di individuazione e ci consente di utilizzare lo "spazio" tra una parola e l'altra come ulteriore elemento da intercettare);
* È utile sapere che la maggior parte degli “strumenti di intercettazione” presumono che le password non siano formate da più di 14 caratteri, e quindi, anche senza complessità, le password molto lunghe (da 14 a 128 caratteri) possono rappresentare un’ottima protezione contro possibili violazioni (non tutti i software sono tuttavia in grado di accettare password superiori a 14 caratteri);
* Utilizzare numeri e simboli al posto di caratteri;
* Non limitarsi alle sole lettere ma, dove possibile, utilizzare l'ampia gamma di minuscole/maiuscole, numeri e simboli a disposizione sulla propria tastiera:
* Caratteri minuscoli: Es.: a, b, c,
* Caratteri maiuscoli: Es.: A, B, C,
* Caratteri numerici: Es.: 0,1,2,3,4,5,6,7,8,9
* Caratteri non alfanumerici: Es.: < > ` ~! $ % ^ ; \* - + = | \ { @ # } [ / ] : ; " '?
* Non inserire i “caratteri speciali” alla fine di una parola nota (ad esempio la password “computer987" può essere identificata abbastanza facilmente - la parola "computer" è inclusa in molti dizionari contenenti nomi comuni e quindi dopo aver scoperto il nome restano solo 3 caratteri da identificare);
* Sostituire una o più lettere all'interno della parola con simboli che possono essere ricordati facilmente (ad esempio si può provare a utilizzare "@"al posto di "A", "$"al posto di "S", zero (0) o la doppia parentesi () al posto di "O", e "3" al posto di "E"). Si tratta di trovare delle analogie che ci rendano familiare la sostituzione di lettere con simboli e numeri (con alcune sostituzioni si possono creare password riconoscibili per l'utente, ad esempio "Ve$tit0 di Mari0", già sufficientemente lunghe e estremamente difficili da identificare o decifrare).
* Cercare di realizzare password utilizzando caratteri appartenenti a tutti i quattro gruppi rappresentati nella lista sopra riportata.

**Cose da NON fare**

* + NON divulgare la propria password: lo scopo principale per cui si usa una password è assicurare che nessun altro possa utilizzare le risorse o possa farlo per conto dell’utente;
	+ NON scrivere la password in nessun posto in cui possa essere letta facilmente, soprattutto vicino al PC;
	+ In fase di immissione della password assicurarsi di non essere osservato;
	+ NON scegliere password che siano contenute all’interno di un dizionario: su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per individuare quale giusta (l’utilizzo di parole straniere non consente di aggirare tale problema);
	+ NON è opportuno utilizzare il “nome utente” quale password (è la password più semplice da indovinare);
	+ NON è opportuno utilizzare password che possano in qualche modo essere facilmente collegate all’utente (Es.: nome, nome della moglie / marito, nome dei figli, del cane, date di nascita, numeri di telefono, ecc.).

## Antivirus

Ogni utente deve accertarsi che, sulla propria postazione di lavoro, il software antivirus sia sempre aggiornato e funzionante, secondo quanto definito dalil Consiglio regionale.

Non è consentito agli utenti disabilitare o inibire il corretto funzionamento del software antivirus eventualmente installato sulla propria Postazione di Lavoro, o modificarne la configurazione, disabilitando o disattivando i meccanismi di notifica automatica degli eventi e di segnalazione degli allarmi.

Qualora per la propria postazione di lavoro non esista un software antivirus rispondente alle norme, o non sia possibile installare correttamente il software antivirus, l’utente dovrà informare immediatamente il proprio Responsabile.

Nel caso in cui il software antivirus rilevi la presenza di un virus che non è riuscito ad eliminare, l’utente deve immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer e segnalare l'accaduto ai referenti IT del Consiglio regionale.

Non è consentito agli utenti rimuovere virus con azioni personali, ma è necessario avvalersi dell’assistenza necessaria, attenendosi alle modalità stabilite dalle eventuali procedure di “gestione degli incidenti”; ad operazione ultimata, gli utenti devono accertarsi dell’eliminazione del virus e della riusabilità della Postazione di Lavoro.

## Sistemi di backup

Per ogni applicazione utilizzata dalil Consiglio regionale devono essere previste attività di backup periodico per le quali sono definiti i seguenti aspetti:

- la frequenza di esecuzione dell’attività;

- le modalità di effettuazione;

- il numero di copie da produrre;

- il periodo di conservazione dei dati.

I servizi di backup devono essere adeguati in relazione alla tipologia di dati contenuti all’interno delle diverse applicazioni e devono essere volti a garantire che tutte le informazioni essenziali e il software possano essere recuperati a seguito di un guasto o di un disastro.

Durante la progettazione di un sistema di backup, devono essere presi in considerazione i seguenti elementi:

* + misura (ad esempio, completo o differenziale di backup) e frequenza dei backup devono riflettere le esigenze di business dell'organizzazione, i requisiti di sicurezza delle informazioni in questione e la criticità delle informazioni per il continuo funzionamento dell'organizzazione;
	+ i backup devono essere memorizzati in una posizione remota (con protezione ambientale e fisica), ad una distanza sufficiente per sfuggire ai danni eventualmente provocati da un disastro al luogo principale;
	+ supporti di backup devono essere testati regolarmente per garantire che possano essere effettivamente utilizzati in caso di emergenza.

È opportuno prevedere specifiche procedure interne per monitorare l'esecuzione dei backup e degli eventuali fallimenti, al fine di garantire la completezza dei backup stessi. Nel caso di sistemi e servizi critici, le modalità di backup devono coprire tutti i sistemi informativi, applicazioni e dati necessari per ripristinare il sistema completo in caso di disastro. Il periodo di conservazione deve essere determinato, tenendo conto di ogni esigenza dell’organizzazione.

# OPERATIVITÀ SU BANCHE DATI

È raccomandabile, laddove possibile, che l’estrazione, la copia, il salvataggio e la stampa su qualunque supporto d’informazioni contenute in banche dati sia precluso, mediante adozione di idonei dispositivi tecnologici e strumenti organizzativi, a tutti gli utenti con la sola esclusione di quelli a ciò specificamente autorizzati per ragioni tecniche. Tale previsione non risulta applicabile alle banche dati funzionali al raggiungimento delle finalità istituzionali del Consiglio regionale e utilizzate per lo svolgimento dei propri servizi, ovvero che siano prodotte e commercializzate con espressa concessione di tali facoltà in virtù della loro natura di strumenti di diffusione di determinati contenuti informativi.

# SERVIZI DI RETE

Nell’utilizzo della rete interna gli utenti devono tenere un comportamento corretto e diligente. A tal riguardo, l’utente non deve effettuare nessun tipo di attività volta ad eludere o compromettere i meccanismi di protezione dei sistemi informatici.

Per l’accesso alla rete del Consiglio regionale 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. La parola chiave d'ingresso alla rete ed ai programmi è segreta e deve essere comunicata e gestita con la massima riservatezza nel rispetto delle eventuali procedure interne definite.

Le cartelle utenti presenti nei server del Consiglio regionale 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, sulle quali vengono, peraltro, svolte regolari attività di controllo, amministrazione e back up da parte del personale IT del Consiglio regionale.

Conseguentemente, agli utenti non è consentito conservare, salva espressa autorizzazione del Consiglio regionale:

- dati non relativi all’attività del Consiglio regionale;

- copie di software ed applicativi;

- files o filmati (.MPEG, .AVI, .MOV, ecc.) o musica (.WAV, .MP3, ecc.).

Ciascun ente può, in qualunque momento, previo avviso al dipendente o collaboratore (fatti salvi i casi di urgenza e gravità), procedere alla rimozione di ogni file o applicazione che riterrà pericolosi per la sicurezza del sistema, sia dai PC degli incaricati sia dalle unità di rete.

È opportuno che, con regolare periodicità, 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.

L’accesso alla rete è consentito solo ai PC che siano usati conformemente alle regole definite da ciascun ente. Il dipendente o il collaboratore è tenuto a dare tempestiva segnalazione di eventuali anomalie o irregolarità nel funzionamento delle risorse di rete, al fine di prevenire la perdita totale o parziale della riservatezza, integrità e/o disponibilità delle informazioni in esse contenute nonché di prevenire eventuali guasti all’intero sistema.

Per motivi di urgenza, ovvero per provvedere alla manutenzione dei sistemi informativi, il personale espressamente incaricato dalil Consiglio regionale può accedere ai server ed alle aree di condivisione di informazioni. In particolare, il personale incaricato dalil Consiglio regionale, nella qualità di Amministratore di Sistema, è autorizzato a compiere interventi nel sistema informativo 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 ciascun utente.

Inoltre, dal momento che la violazione delle regole di cui sopra potrebbe esporre il Consiglio regionale al rischio di danneggiamento o mal funzionamento del sistema informatico, il rispetto di tali regole potrebbe essere oggetto di controllo attraverso periodiche verifiche del contenuto della memoria di massa dei server oltre che del PC consegnato all’utente. Tale controllo costituisce una procedura di controllo di carattere “ordinario” (o di 1° livello), rivolta principalmente in modo indistinto alla popolazione del Consiglio regionale, giustificata da esigenze operative, organizzative e produttive del Consiglio regionale nonché dalla necessità di tutela del patrimonio informativo del Consiglio regionale stessa, e potrà essere eseguita anche mediante l’utilizzo di strumenti automatizzati. L’accesso ai sistemi ed alle evidenze del controllo è riservato esclusivamente al personale incaricato dalil Consiglio regionale quale Amministratore di Sistema.

# UTILIZZO DI INTERNET

Il servizio di connessione ad Internet del Consiglio regionale è uno strumento operativo che viene reso disponibile agli utenti che ne abbiano effettiva necessità.

L’accesso ad Internet è fornito allo scopo di ottenere informazioni necessarie allo svolgimento dell’attività lavorativa. Essendo uno strumento di lavoro di proprietà del Consiglio regionale della Basilicata, i soggetti cui il Consiglio regionale attribuisce l’accesso sono responsabili del suo corretto utilizzo.

Esso costituisce una risorsa ed un’opportunità di sviluppo del Consiglio regionale, ma rappresenta anche una potenziale minaccia alla sicurezza dei sistemi e delle informazioni. L’uso incauto può essere una fonte di rischio per la sicurezza, oltre che un costo rilevante per gli enti.

Il Consiglio regionale, qualora lo ritenga necessario, ha la facoltà di revocare l’accesso ad Internet dei singoli utenti e di installare software atti a filtrare / bloccare in automatico l’accesso a siti che non sono ritenuti di interesse del Consiglio regionale o attinenti ad attività lavorative. L’utente che accede ad un sito Internet deve prendere visione se specificato nel sito stesso, dei termini e le condizioni che ne regolano l’utilizzo e operare in conformità delle stesse.

L’uso di Internet attraverso le apparecchiature del Consiglio regionale è consentito solo per motivi di lavoro e nell’interesse esclusivo del Consiglio regionale. La connessione ad Internet dai computer (inclusi portatili e palmari) e ogni accesso alla rete Internet potrebbero essere registrati nel proxy Server del Consiglio regionale.

L’accesso ad Internet deve avvenire solo attraverso le infrastrutture tecnologiche poste in essere dalil Consiglio regionale e deve essere configurato dal personale IT specializzato. Non è autorizzato pertanto l’accesso a Internet utilizzando collegamenti via modem o altri mezzi di collegamento personali.

L’utente si impegna, nei confronti del Consiglio regionale cui appartiene, a non utilizzare il servizio di connessione ad Internet per scopi illegali o che comunque possano recare danno o pregiudizio alla medesima o a terzi, assumendosi ogni responsabilità derivante dall’uso improprio del servizio ed esonerando contestualmente il Consiglio regionale da ogni pretesa o azione che dovesse essere rivolta alla medesima da qualunque soggetto, in conseguenza di tale uso improprio.

L’utente, inoltre, non può utilizzare la connessione a Internet in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con l’utilizzo e il godimento della stessa da parte di altri Utenti. In ogni caso al dipendente o collaboratore non è consentito:

* + accedere ai siti Internet assoggettati a restrizione da parte del Consiglio regionale, forzando i sistemi di sicurezza dalla medesima predisposti ed in ogni caso utilizzare siti o altri strumenti (es. Cracking Programs) che realizzino tale fine;
	+ effettuare il download di software, ancorché gratuito (freeware), o messo a disposizione in rete per essere provato (shareware, demo), e comunque il download di qualsiasi software nonché di file multimediali (come file musicali o video) senza l’espressa autorizzazione del Consiglio regionale;
	+ modificare la configurazione del browser o del PC in modo da diminuirne il livello di protezione Internet;
	+ effettuare qualsiasi genere di attività personale di guadagno economico, nonché di transazione finanziaria in rete, ivi compresi gli acquisti on line e le operazioni di remote banking per scopi estranei allo svolgimento dell’attività lavorativa;
	+ accedere a siti Internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell’ordine pubblico;
	+ utilizzare Internet per effettuare attività considerate illegali e, comunque, accedere a siti contenenti:
* materiale teso alla promozione di comportamenti criminali o violenti;
* materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.;
* materiale che violi la legge in materia di protezione dati personali;
* contenuti o materiali che violino i diritti di proprietà di terzi;
* materiale pornografico o simile, in particolare in violazione della legge n.269 del 1998 “Norme contro lo sfruttamento sessuale dei minori degli anni 18”;
* altri contenuti inappropriati o contrari alla legge;
	+ accedere, attraverso le apparecchiature del Consiglio regionale, a qualsivoglia gruppo di discussione o conferenza in rete (chat lines o altro) o banche dati esterne, con la sola esclusione di quelli espressamente autorizzati;
	+ utilizzare identificativi altrui al fine di effettuare la connessione a Internet;
	+ utilizzare l’accesso ad Internet in violazione delle norme in vigore nell’ordinamento giuridico italiano a tutela del diritto d’autore.

Qualunque attività eseguita in Internet deve tenere conto, in qualunque momento, dell’integrità dei dati del Consiglio regionale, per esempio: non si devono divulgare informazioni tecniche quali IP address, password o identificativi utenti.

Il Consiglio regionale potrebbe utilizzare prodotti di *Content Filtering* per selezionare il traffico di Internet e si potrebbe dotare di apposite procedure per la gestione dei profili di accesso al servizio, che regolamentano e limitano l’accesso al servizio e ad alcuni siti.

Il dipendente è tenuto a dare tempestiva segnalazione di eventuali anomalie o irregolarità nel funzionamento dell’accesso a Internet, al fine di prevenire eventuali guasti all’intero sistema.

Dal momento che la violazione delle regole sopra riportate potrebbe esporre il Consiglio regionale al rischio di danneggiamento o mal funzionamento del sistema informatico, il rispetto di tali regole potrà essere oggetto di controllo anche mediante accesso in remoto, attraverso periodiche verifiche del contenuto della memoria di massa dei server di accesso a Internet (proxy), dei PC e dei sistemi di “Content Filtering”, nonché mediante esame dei file di log della navigazione svolta.

Tale controllo costituisce una procedura di controllo di carattere “ordinario” (o di 1° livello), rivolta principalmente in modo indistinto alla popolazione del Consiglio regionale, giustificata da esigenze operative, organizzative e produttive del Consiglio regionale nonché dalla necessità di tutela del patrimonio informativo del Consiglio regionale stessa, e potrà essere eseguita anche mediante l’utilizzo di strumenti automatizzati. L’accesso ai sistemi ed alle evidenze del controllo è riservato esclusivamente al personale del Consiglio regionale individuato quale “Amministratore di Sistema”.

# POSTA ELETTRONICA

Il Consiglio regionale può attribuire agli utenti un "Account" o indirizzo di posta elettronica utilizzabile per inviare e ricevere e-mail. La casella di posta elettronica assegnata all’utilizzatore, il relativo indirizzo e i messaggi in entrata ed in uscita dalla stessa, sono di proprietà del Consiglio regionale. Essi rappresentano uno strumento di lavoro affidato all’utente al solo fine di consentirgli di svolgere le proprie mansioni ed attività lavorativa.

Le persone cui il Consiglio regionale attribuisce l’uso di caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Il personale incaricato dalil Consiglio regionale quale Amministratore di Sistema, inoltre, è autorizzato a compiere interventi nel sistema informativo del Consiglio regionale 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.). Tali interventi, potranno anche comportare l’accesso in qualunque momento alle caselle di posta elettronica degli utenti, escludendo tuttavia che l’accesso sia finalizzato, in tali circostanze, ad attività di controllo.

Utilizzando l’indirizzo di posta elettronica del Consiglio regionale, l’utente è a conoscenza e consapevole che:

* + un messaggio di posta elettronica si configura, da un punto di vista giuridico, come corrispondenza aperta, potendo essere letto da chiunque durante il suo percorso sulla rete Internet fino al destinatario, nonché dall’Amministratore di sistema sui server;
	+ l’uso dell’indirizzo di posta elettronica del Consiglio regionale è ammesso per motivi attinenti all’attività lavorativa: l’uso per motivi personali è consentito solo nei limiti della normalità e cioè per un limitato numero di messaggi di cortesia o inerenti rapporti parentali o amicali, sempre nel rispetto delle norme di comportamento interne e tenuto conto dell’interesse del Consiglio regionale;
	+ a tutela del proprio diritto alla privacy, relativa ai messaggi di posta elettronica in entrata ed in uscita utilizzando l’indirizzo del Consiglio regionale, l’accesso ai messaggi personali ivi contenuti, qualora esso si dovesse rendere necessario (es. in caso di assenza non programmata dell’utente), oppure per motivazioni di carattere lavorativo ed a giudizio del Consiglio regionale, può avvenire per il tramite di altro collega (fiduciario) indicato dal dipendente stesso. Sarà comunque consentito al superiore gerarchico o, sentito l’utente (qualora raggiungibile), a persona individuata dalil Consiglio regionale, accedere alla propria casella di posta elettronica per ogni ipotesi di carattere lavorativo per cui ciò si dovesse rendere necessario. Il fiduciario, che agirà all’occorrenza in caso di assenza dell’utente, ovvero il superiore gerarchico, o la persona individuata dalil Consiglio regionale come sopra indicato, utilizzerà una password d’ingresso creata “ad hoc” dal fiduciario (ovvero dal superiore gerarchico o persona individuata dalil Consiglio regionale) mediante autorizzazione del Consiglio regionale. La password dovrà essere custodita dal fiduciario (ovvero dal superiore gerarchico o persona individuata dalil Consiglio regionale) e dovrà essere resettata al cessare delle suddette motivazioni o al rientro del titolare. È cura dell’utente segnalare al proprio superiore gerarchico il nominativo del fiduciario prescelto;
	+ il messaggio di posta elettronica potrebbe essere letto da destinatari diversi da quelli a cui era diretto, e ciò potrebbe determinare danni anche gravi alil Consiglio regionale;
	+ falsi o errati messaggi di posta elettronica scritti per conto e nel nome del Consiglio regionale potrebbero essere spediti
	+ per errore sia all’interno che all’esterno del Consiglio regionale;
	+ messaggi di posta elettronica spediti potrebbero non essere recapitati, essere distrutti o subire ritardi. In ogni caso al dipendente o collaboratore non è consentito:
	+ inviare un messaggio con allegato un file eseguibile (.exe);
	+ utilizzare l’indirizzo di posta elettronica contenente il dominio del Consiglio regionale per iscriversi a qualsivoglia sito per motivi non attinenti all’attività lavorativa, senza espressa autorizzazione scritta del Consiglio regionale, nonché per partecipare a qualunque genere di petizione, “catene di Sant’Antonio” o in generale, a qualunque pubblico dibattito su qualsivoglia tema;
	+ indicare liberatorie personalizzate all’interno dei messaggi;
	+ utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni alil Consiglio regionale informazioni riservate o documenti interni, se non nel caso in cui ciò sia necessario in base alle mansioni svolte;
	+ accedere a caselle di posta elettronica personali attraverso la rete (Webmail) e le apparecchiature del Consiglio regionale. L’utente non potrà, peraltro, inoltrare automaticamente i messaggi ricevuti all’indirizzo di posta elettronica del Consiglio regionale su indirizzi personali;
	+ inviare o archiviare messaggi in forma crittografata senza l’espressa autorizzazione che deve essere richiesta ai referenti IT;
	+ inviare, tramite la posta elettronica, anche all’interno della rete del Consiglio regionale, alcun 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. Qualora il dipendente riceva messaggi aventi tale contenuto, è tenuto a darne comunicazione tempestiva al proprio responsabile;
	+ ricevere ed inviare messaggi con allegati diversi da quelli inerenti alla prestazione lavorativa;
	+ creare, archiviare o spedire, anche all’interno della rete del Consiglio regionale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) in nessun modo connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto utilizzando l’indirizzo del Consiglio regionale;
	+ utilizzare la posta elettronica del Consiglio regionale in violazione delle norme in vigore nell’ordinamento giuridico italiano a tutela del diritto d’autore.

Il dipendente o il collaboratore è tenuto a dare tempestiva segnalazione di eventuali anomalie o irregolarità nel funzionamento della posta elettronica, al fine di prevenire la perdita totale o parziale della riservatezza, integrità e/o disponibilità delle informazioni in essa contenute nonché di prevenire eventuali guasti all’intero sistema.

Dal momento che la violazione delle regole sopra riportate potrebbe esporre il Consiglio regionale al rischio di danneggiamento o mal funzionamento del sistema informatico, il rispetto di tali regole potrebbe essere oggetto di controllo attraverso periodiche verifiche del contenuto della memoria di massa dei server oltre che del PC consegnato al dipendente. Tale controllo costituisce una procedura di controllo di carattere “ordinario” (o di 1° livello), rivolta

principalmente in modo indistinto alla popolazione del Consiglio regionale, giustificata da esigenze operative, organizzative e produttive del Consiglio regionale nonché dalla necessità di tutela del patrimonio informativo del Consiglio regionale stessa, e potrà essere eseguita anche mediante l’utilizzo di strumenti automatizzati. L’accesso ai sistemi ed alle evidenze del controllo è riservato esclusivamente al personale del Consiglio regionale individuato quale “Amministratore di Sistema”.

# COLLEGAMENTO REMOTO

Il collegamento remoto a reti, sistemi o applicazioni del Consiglio regionale è consentito esclusivamente per finalità interne attraverso i punti di ingresso identificati ed autorizzati (server di posta, concentratori VPN, o altro) e per il tempo strettamente necessario all’esecuzione delle attività lavorative.

Il collegamento tramite computer non del Consiglio regionale è consentito esclusivamente se preventivamente autorizzato o per gravi e motivate situazioni di emergenza. In ogni caso, il computer utilizzato deve essere dotato di sistemi antivirus, attivi ed aggiornati. È vietato il collegamento da dispositivi pubblici, ad esempio Internet point.

# *\*SISTEMI DI TELEFONIA*

L’utilizzo delle credenziali di accesso ai sistemi di telefonia che lo prevedono (VoIP o cellulari di lavoro) costituisce a tutti gli effetti un accesso a rete o sistema, con l’assunzione di responsabilità da parte dell’utente che ne consegue per le operazioni successivamente eseguite. I telefoni cellulari di lavoro devono essere impostati con la richiesta del PIN all’accensione. Ove possibile deve essere attivata la funzione di crittografia automatica del dispositivo portatile in caso di spegnimento dell’apparato.

# ACCESSO AI SISTEMI

L’accesso ai sistemi, alle reti ed alle applicazioni deve essere preventivamente autorizzato e deve svolgersi con modalità conformi allo svolgimento delle attività del Consiglio regionale. Il Consiglio regionale attribuisce ad ogni utente delle credenziali di autentificazione (user-id e password) per l’accesso alle risorse e alla rete locale. L’accesso deve avvenire esclusivamente attraverso l’utilizzo della utenza personale (user-id) assegnata o, in casi particolari per finalità di test, assistenza o manutenzione, con altra, apposita utenza.

La mera possibilità di utilizzo di sistemi, reti o applicazioni per le quali non si sia stati preventivamente autorizzati non costituisce una implicita autorizzazione, ma al contrario è da ritenere una possibile esposizione di sicurezza da segnalare alle strutture competenti. L’accesso ai sistemi, alle reti ed alle applicazioni è sottoposto a registrazione. Le credenziali di accesso, costituendo la base per l’identificazione e l’autenticazione degli utenti nella fase di accesso ai sistemi informatici, devono essere custodite con la massima riservatezza e non rivelate ad alcuno (neanche ai colleghi). Qualunque accesso effettuato utilizzando le credenziali personali dell’utente è da considerare sotto la diretta responsabilità dell’utente stesso così come lo sono le conseguenti operazioni effettuate.

Analoga riservatezza deve essere osservata nei confronti delle credenziali di accesso “applicative” (cioè delle credenziali utilizzate da applicazioni, sistemi o dispositivi) di cui si venga a conoscenza. Qualora l’utente ritenga che la confidenzialità delle credenziali sia stata compromessa, deve provvedere, nel caso di password, al cambio immediato della stessa, o, nel caso di credenziali di autenticazione di altro genere (smart card, token, ecc.), all’immediata segnalazione ai referenti IT. Le credenziali di accesso rilasciate all’utente sono conservate con modalità che non ne consentono la conoscenza o la ricostruzione, neanche da parte del personale IT.

# PROTEZIONE DEI DATI – TECNICHE DI SOTTRAZIONE

Informazioni di normale utilizzo nel corso dell’attività operativa del Consiglio regionale o ritenute non riservate nell’ambito delle comunicazioni interne tra il personale aziendale, potrebbero assumere una diversa importanza se comunicate all'esterno a soggetti terzi, necessitando quindi di una maggiore tutela.

La salvaguardia delle informazioni e dei dati oltre ad essere un requisito fondamentale per la sicurezza del patrimonio informativo aziendale, è anche un espresso obbligo di legge nei confronti di qualsiasi soggetto definito "interessato". A fronte di tali motivazioni è importante sottolineare la necessità di osservare ogni cautela nel trasferire all'esterno qualsiasi informazione proporzionalmente al loro contenuto e all'attendibilità dell'interlocutore.

Nel corso anni si sono sviluppate numerose tecniche per la sottrazione “fraudolenta” di dati e informazioni gestiti da parte degli utenti nell’ambito dell’attività lavorativa tra cui le più rilevanti sono:

- il social engineering;

- l’E-mail phishing.

## Il social engineering

Il Social Engineering è un insieme di “tecniche psicologiche” usate da chi vuole indurre qualcun altro ai propri scopi presentandosi personalmente presso l’utente o contattandolo dall'esterno a mezzo telefono o posta elettronica. Gli obiettivi possono andare dalla raccolta di informazioni apparentemente innocue riguardanti l'azienda o la sua organizzazione e il personale in forza, ma possono arrivare a raggiungere dati anche molto riservati.

Con l'ausilio di messaggi studiati e abili tecniche di persuasione, l'aggressore può anche rendere l’utente complice inconsapevole di azioni che andranno a suo beneficio come, ad esempio, l'acquisizione di informazioni o l'ottenimento della fiducia degli utenti, l'apertura di allegati infetti o la visita di siti che contiene “dialer” o altro materiale pericoloso.

Uno dei principali problemi degli autori di virus è che molti utenti utilizzano strumenti di difesa aggiornati che non consentono l'esecuzione in automatico di applicativi e quindi non consentono l'attivazione di programmi dannosi. Per scavalcare queste precauzioni e quindi attivare l’azione di un virus, attraverso tecniche di social engineering si potrebbe indurre la vittima, tramite espedienti psicologici, a fidarsi dell'allegato e quindi eseguirlo, o fidarsi del collegamento ad un sito web contenuto nel messaggio e quindi raggiungerlo. In questo modo l'aggressore potrebbe essere capace di sfruttare i punti di debolezza redigendo abili messaggi che, inducendo fiducia o curiosità, riescono ad arrivare allo scopo.

## L’E-mail phishing

Altro scopo di possibili aggressori è indurre l'utente a fidarsi dell'intero contenuto di un messaggio di posta elettronica e quindi ottenere una fedele esecuzione delle istruzioni contenute: ad esempio, vengono inviate false comunicazioni e-mail aventi grafica, forma, autorevolezza e loghi ufficiali di enti noti, banche, intermediari finanziari, assicurazioni, etc., chiedendo informazioni attraverso moduli o link a pagine web debitamente camuffate.

Attraverso questa modalità vengono richieste all’utente informazioni riservate (es.: password, numeri di carta di credito, ecc.) senza che in realtà la raccolta dati abbia nulla a che vedere con l'organismo ufficiale imitato. La vittima crede di comunicare con essi ma in realtà sta trasmettendo informazioni riservate all'aggressore.

Le tecniche di sottrazione dati di cui sopra spesso sono abbinate tra loro e applicate più volte nel tempo sulla stessa vittima in modo da poter ottenere dei risultati.

Al fine di ridurre i rischi di sottrazione dati è opportuno:

* evitare di fornire informazioni confidenziali al telefono o di persona a interlocutori non conosciuti;
* limitarsi a fornire informazioni a interlocutori noti e operanti con l’utente per disposizione aziendale nei limiti dei contenuti afferenti all'ambito lavorativo assegnato;
* diffidare di messaggi provenienti da fonte non conosciuta;
* non aprire messaggi provenienti da fonte non conosciuta contenenti allegati;
* non aprire messaggi contenenti allegati sospetti;
* non utilizzare mai link contenuti nel testo del messaggio perché possono essere facilmente falsificati;
* non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonte sconosciuta;
* non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonti istituzionali o apparentemente conosciute (ad es.: banche) in quanto tali strutture non richiedono mai dati utilizzando questa modalità;
* in caso di dubbio è sempre preferibile verificare l'attendibilità delle richieste con il proprio Responsabile.

# POLITICHE GENERALI PER L’UTILIZZO DEGLI ARCHIVI CARTACEI

Tutto il materiale cartaceo contenente dati personali deve essere gestito evitando che esso risulti facilmente visibile a persone terze o, comunque, ai non autorizzati al trattamento. Non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro.

In caso di trattamento di dati particolarmente c.d. sensibili (condizioni di salute, dati giudiziari, ecc.), tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro.

I documenti contenenti dati “sensibili” particolari devono essere controllati e custoditi in modo che non vi accedano persone non autorizzate. La consultazione deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati.

Ogni dipendente o collaboratore ha la responsabilità dei propri documenti e in presenza di dati personali, deve:

* consentire l’accesso unicamente per finalità lavorative, a persone autorizzate e limitatamente ai dati la cui conoscenza è strettamente necessaria;
* proteggere i documenti cartacei e i dati personali in essi contenuti da perdite, distruzione, falsificazione, accesso e divulgazione non autorizzati;
* conservare gli atti e i documenti contenenti dati personali in archivi ad accesso selezionato, secondo le istruzioni del proprio responsabile;
* distruggere fisicamente i documenti cartacei che contengono dati personali prima di cestinarli;
* restituire i documenti al termine delle operazioni affidate.