PROCEDURA DI GESTIONE DELLA DOCUMENTAZIONE CON L'AUSILIO DI STRUMENTI ELETTRONICI "I C T"

SCOPO E CAMPO DI APPLICAZIONE

Scopo della presente procedura è quello di definire le modalità e le responsabilità atte a garantire un'efficace gestione dei documenti trattati con strumenti elettronici e delle registrazioni del Trattamento dei dati personali così come previsto dalla normativa vigente in materia, "GDPR 679/2016".
La presente procedura si applica a tutta la documentazione su supporto elettronico trattata dal TITOLARE DEL TRATTAMENTO e dai soggetti da esso autorizzati.
L'esigenza di definire delle procedure nasce dalla necessità di avere una chiara e trasparente modalità di svolgimento dei processi fondamentali interni.
Le Procedure sono destinate al solo uso interno e pertanto vengono messe a disposizione del personale sia in forma cartacea che in file.

GESTIONE DELLA DOCUMENTAZIONE

Generalità

La procedura di gestione della documentazione riguarda i seguenti documenti:

- Documenti di origine interna;
- Documenti di origine esterna:

Il processo di gestione della documentazione si articola nelle seguenti attività:

- redazione;
- verifica;
- approvazione / emissione;
- distribuzione o messa a disposizione;
- modifica / aggiornamento;
- conservazione e archiviazione;
- rimozione/distruzione.

REGOLE

Al fine di rispettare la normativa e l'interesse dei dati personali dei soggetti terzi, e non solo, gli incaricati dovranno operare con la massima attenzione in tutte le fasi di trattamento, dall'esatta acquisizione dei dati, all'eventuale loro aggiornamento, nonché alla conservazione ed eventuale distruzione.
Tutti i personal computer (hardware) messi a disposizione dal TITOLARE del Trattamento all'utente e il complesso delle applicazioni e dei programmi che il TITOLARE installa sui medesimi (software) sono di proprietà del TITOLARE stesso. Sia l'hardware che il software sono esclusivamente strumenti di lavoro e debbono essere utilizzati secondo questa unica finalità; ambienti condivisi eventualmente con altri utenti e certamente con **l'eventuale Amministratore di sistema;** tanto l'account quanto la password possono essere in qualunque momento disattivati dal TITOLARE e/o **dall'eventuale Amministratore di sistema.**
Le regole che dovranno essere rispettate sono le seguenti:

1. tutti gli incaricati devono essere dotati di credenziali di autenticazione, consistenti in un codice per l'identificazione dell'incaricato (USER ID) associato ad una parola chiave riservata (PASSWORD), conosciuta soltanto dall'incaricato medesimo e con le caratteristiche di seguito specificate. Le credenziali consentono il superamento di una procedura di autenticazione, necessaria per accedere agli archivi informatici ai quali sia abilitato l'incaricato. Al fine di rispettare quanto sopra indicato, l'incaricato deve:

- adottare idonee cautele per mantenere segreta la password e, in particolare, evitare di digitare la stessa di fronte ad altre persone;
- creare e utilizzare password di almeno 8 caratteri. Nel caso in cui lo strumento elettronico non lo consenta, dovrà crearla nel numero massimo di caratteri consentito;
- adottare password che non contengano riferimenti agevolmente riconducibili all'incaricato (es. nomi di familiari o località conosciute etc.) e con una composizione casuale (consigliabile usare combinazioni miste di lettere, cifre e caratteri di interpunzione);
- modificare la password ogni tre mesi. La password dovrà essere sostituita almeno ogni tre mesi. Se tecnicamente possibile in relazione alle caratteristiche dell'elaboratore, sarà consentita anche l'autonoma sostituzione della password da parte dell'incaricato.

1. In caso di prolungata assenza, impedimento o altra causa per la quale l'incaricato non abbia la possibilità di attivare il sistema di autenticazione, laddove si renda indifferibile o urgente accedere agli archivi per esclusive necessità di operatività e di sicurezza del sistema e comunque su disposizione del delegato interno, si dovrà ricorrere ai custodi delle password. Le disposizioni di questo punto non si applicano all'archivio inerente alla casella di posta elettronica, per il quale vige una autonoma regolamentazione;
2. Se possibile in relazione alle caratteristiche dell'elaboratore, sarà consentita l'autonoma sostituzione della password da parte dell'incaricato;
3. Durante una sessione di trattamento, qualora lo strumento elettronico che consente l'accesso agli archivi sia momentaneamente incustodito, l'incaricato dovrà bloccare la consultazione e comunque l'accesso al sistema mediante idonei strumenti che richiedano per la riattivazione l'utilizzo di credenziali di autenticazione (es. attivazione della funzione di blocco del computer attraverso la digitazione congiunta di CTRL+ALT+CANC e successivamente BLOCCA COMPUTER);
4. Gli elaboratori saranno protetti da *software antivirus* idoneo, aggiornato costantemente; nel caso in cui riscontrasse la presenza di virus in *file* presenti negli archivi degli elaboratori o su supporti magnetici, l'incaricato avviserà tempestivamente l'eventuale Amministratore di Sistema e adotterà le procedure per eliminare o neutralizzare il file infetto di volta in volta specificate dall'amministratore medesimo;
5. Al fine di evitare la perdita e/o l'alterazione dei dati, viene effettuato un Backup aziendale, con cadenze e modalità previste nell'apposito registro;
6. In linea generale è vietato l'uso di qualsiasi supporto rimovibile (es. *USB Driver, HD esterni, DVD, floppy disk*), sia per la riproduzione che per la registrazione, salvo espressa autorizzazione. Nell'ipotesi in cui, sempre dietro espressa autorizzazione, per l'esecuzione dei *back up* dovessero essere utilizzati supporti rimovibili, detti supporti dovranno essere custoditi ai armadi/cassetti chiusi a chiave; in nessun caso potranno essere lasciate le copie di *back up*, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese illeggibili le informazioni in esse registrate;

7. Nell'eventuale caso di trattamento dei dati particolari (sensibili) o giudiziari, potranno essere impiegati supporti rimovibili (es. *USB Driver, HD esterni, DVD, floppy disk)* solo quando il loro impiego si riveli indispensabile in funzione della finalità del trattamento medesimo o delle categorie di soggetti interessati e, in ogni caso, per il lasso di tempo strettamente necessario allo stesso. I supporti rimovibili andranno accuratamente custoditi e, se non utilizzati, saranno distrutti o resi inutilizzabili; essi potranno essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, solo qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili;
8. L'eventuale consegna all'esterno di supporti elettronici (es. *USB Driver, HD esterni, DVD, floppy disk*) dovrà essere preceduta da un'apposita scansione dei file e dei programmi registrati; qualora i supporti contengano dati personali (esempio: indirizzari) la consegna dovrà essere preventivamente autorizzata dal delegato interno;
9. l'eventuale eliminazione di supporti magnetici contenenti dati personali dovrà essere preventivamente autorizzata dal Delegato interno
10. Se non diversamente previsto, per ragioni tecniche, dopo la chiusura i PC personali dovranno essere spenti;
11. E' assolutamente vietato l'uso di software non autorizzati e la navigazione, nonché scaricare file e/o programmi, da siti internet ritenuti non sicuri e, soprattutto, non coerenti ed autorizzati dal Titolare del Trattamento;
12. Sono obbligatori, con cadenza almeno annuale, gli aggiornamenti periodici dei programmi per gli strumenti elettronici, effettuati dall'eventuale Amministratore di sistema o da Personale Interno preventivamente autorizzato;
13. Tutti gli strumenti elettronici sono sottoposti a manutenzione nonché a sostituzione periodica al fine di mantenere alti gli standard di gestione e protezione dei dati;
14. La distruzione degli strumenti elettronici avviene tramite lo smaltimento e la demolizione in appositi centri autorizzati, previa formattazione degli strumenti stessi;
15. Al fine di evitare danni irreparabili e/o guasti tecnici dovuti a variazioni di tensioni nonché scariche atmosferiche, anche durante gli

orari di lavoro, gli strumenti elettronici sono protetti da gruppi di continuità/stabilizzatori come previsto dall’apposito registro.

In caso tali regole dovessero essere disattese o non rispettate in tutto o in parte, i soggetti ritenuti responsabili di tali violazioni saranno oggetto di provvedimenti disciplinari.