MANSIONARIO PRIVACY

1 – Generalità

Il presente mansionario, firmato in calce dal Responsabile, contiene le norme specifiche di compro tamento che integrano quelle di carattere generale citate nelle lettere d'incarico.

Ogni Incaricato, in funzione dei compiti che gli sono stati assegnati dal Titolare, è tenuto ad osservarle, ed a fare presente al Titolare eventuali errori od omissioni.

L'elenco degli Incaricati, completo di recapito telefonico e della rispettiva qualifica, sono disponibili nel paragrafo **A – Elenco degli Incaricati**.
I codici di riferimento sono quelli citati nel Documento Programmatico Sulla Sicurezza.

L'originale del presente mansionario è conservato presso ***Locale L1 – Scaffalatura C1***
ed è a disposizione di tutti gli Incaricati della Sede Operativa.

Una copia aggiornata è allegata al Documento Programmatico Sulla Sicurezza.

Letto, approvato e sottoscritto

(Il Responsabile)

Torino, 00/00/2000

1 – Generalità

Definizioni

Ai soli fini del presente mansionario, si intende per:

- **Trattamento**
  qualunque operazione, effettuata con o senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la comunicazione, la diffusione, la cancellazione e la distruzione di dati personali presenti nella Sede Operativa;
- **Luoghi fisici**
  i locali della Sede Operativa nei quali sono effettuati i trattamenti dei dati personali;
- **Hardware**
  gli impianti installati nei locali della Sede Operativa: impianto elettrico, impianto idraulico, impianto termico, apparecchiature elettriche (ventilatori, condizionatori, ecc.) ed elettroniche (computer, telefoni, fax, ecc.) e tutti i rispettivi accessori;
- **Software**
  le procedure che effettuano o consentono l'effettuazione del trattamento dei dati con l'ausilio di strumenti elettronici;
- **Dati personali**
  qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, che consenta la sua identificazione, anche indiretta;

  se essa è idonea a rivelare la razza, le convinzioni religiose o filosofiche, le opinioni politiche, lo stato di salute o la vita sessuale, viene definita dato sensibile;

  se essa è idonea a rilevare provvedimenti iscritti nel casellario giudiziario o la qualità di imputato o di indagato per un'ipotesi di reato, viene definita dato giudiziario;
- **Incaricato**
  la persona fisica autorizzata, dal Titolare o dal Responsabile, a compiere le operazioni di trattamento sui dati presenti, a qualunque titolo, nella Sede Operativa;

  alcune di esse possono aver ricevuto uno dei seguenti incarichi specifici:

  - Amministrazione del Sistema;
  - Custodia del Parole Chiave;
  - Salvataggio dei Dati;
  - Custodia della Sede Operativa;

  altri incarichi specifici potranno essere assegnati dal Titolare in funzione delle future esigenze dell'Azienda.

2 – Incaricati

Tutti gli Incaricati devono:

- fornire, al primo contatto con gli utenti, l'informativa ai sensi dell'art. 13 D.Lgs.196/2003 e, se previsto, farsi rilasciare il relativo consenso;
- raccogliere i dati personali e registrarli unicamente per finalità inerenti l'attività svolta;
- verificare l'esattezza, la completezza e la pertinenza dei dati trattati;
- accedere ai dati limitatamente per l'espletamento delle proprie mansioni ed esclusivamente durante l'orario di lavoro, salvo espressa richiesta da parte del Titolare;
- sostituire, secondo le modalità previste nel seguito, le parole chiave (Password);
- verificare che i dati trattati, anche in caso di interruzione temporanea del lavoro, non siano accessibili a terzi non autorizzati, attivando lo *screen saver* e riponendo i supporti cartacei nella cassettiera della scrivania;
- avvisare l'Incaricato all'Amministrazione del Sistema in caso di anomalie del software, dell'hardware e, se si utilizza Internet o un sistema di posta elettronica, della presunta presenza di virus informatici;
- archiviare, al termine della giornata lavorativa o nei casi di assenza prolungata, i dati cartacei nei contenitori previsti: se ciò non è possibile utilizzare le cassettiere delle scrivanie;
- spegnere il computer, al termine della giornata lavorativa o in caso di assenza prolungata, salvo che lo stesso debba essere lasciato acceso per altri motivi (es. un server di rete).

Tutti gli Incaricati non devono:

- comunicare a terzi i dati personali di cui, per qualunque motivo, sono venuti a conoscenza nell'esercizio delle proprie mansioni, salvo diversa e motivata richiesta da parte del Titolare;
- diffondere, senza la preventiva autorizzazione del Titolare, i dati personali trattati;
- comunicare agli altri Incaricati ed a terzi, anche in modo indiretto, le proprie credenziali di autenticazione (UserName e Password).

2 – Incaricati

Credenziali di Autenticazione

Le credenziali di autenticazione sono riservate e personali.

Le credenziali di autenticazione possono essere utilizzate da altri Incaricati, previa autorizzazione da parte del Titolare, esclusivamente per i seguenti motivi:

- prolungata assenza dell'Incaricato (ferie, malattia, ecc.);
- reali motivi di urgenza;
- cessazione dell'abilitazione dell'Incaricato.

In ogni caso il Titolare è tenuto a documentare in forma scritta l'avvenuto utilizzo e, eccetto nell'ultimo caso, comunicarlo all'Incaricato al suo rientro.
Tale documentazione sarà allegata al successivo Documento Programmatico Sulla Sicurezza.

Lo UserName è assegnato dall'Incaricato all'Amministrazione del Sistema in modo univoco.
Nessun UserName, anche se obsoleto, potrà essere uguale ad uno UserName esistente.

La Password è inserita dall'Incaricato e deve avere le seguenti caratteristiche:

- essere lunga almeno **8 (otto)** caratteri;
- iniziare con un carattere alfabetico;
- contenere almeno un carattere numerico e/o un carattere speciale (£, $, %,), ecc.)
- essere diversa dalla precedente.

La Password deve essere sostituita:

- ad ogni dimenticanza della stessa da parte dell'Incaricato, previa operazione di sblocco da parte dell'Incaricato all'Amministrazione del Sistema;
- ogni **90 (novanta)** giorni solari o al primo accesso successivo a tale scadenza;
- al primo accesso successivo ad un accesso di terzi autorizzato dal Titolare.

Ad ogni sostituzione l'Incaricato dovrà inserire la nuova Password in busta chiusa e consegnarla all'Incaricato alla Custodia delle Parole Chiave (ved. paragrafo **A – Elenco degli Incaricati**).

3 – Incaricato all'Amministrazione del Sistema

L'Incaricato all'Amministrazione del Sistema deve:

- mantenere in efficienza il Sistema Informativo, sia per quanto concerne il software che l'hardware;

- comunicare al Titolare eventuali esigenze di installazione di nuovo software o hardware ed attenersi alle sue disposizioni;

- realizzare, in proprio e/o tramite personale delle aziende fornitrici e/o di consulenti eventualmente preposti, quanto richiesto dal Piano di adeguamento delle misure di sicurezza di cui al Documento Programmatico Sulla Sicurezza, limitatamente a ciò che concerne il Sistema Informativo;

- eseguire, in proprio e/o tramite personale delle aziende fornitrici, eventuali interventi sull'hardware e sul software, per nuove installazioni, normale manutenzione o anomalie;
  se il tempo richiesto per l'intervento, compreso quello per "Disaster Recovery", è superiore a 7 giorni, dovrà metter a disposizione dell'utente una postazione, anche temporanea, che contenga gli stessi dati e fornisca le stesse prestazioni;
  (*se l'Amministrazione del Sistema viene effettuata da un Incaricato esterno*) fornire, al termine di ogni intervento, una dichiarazione di conformità al D.Lgs. 196/2003 (Codice Privacy), contenente una breve descrizione dei lavori effettuati;

- relazionare al Titolare, su richiesta dello stesso, circa lo stato del Sistema Informativo, il livello di servizio fornito all'utenza e lo stato di avanzamento di eventuali interventi sull'hardware o sul software;

- (*se non è disponibile un sistema automatico di aggiornamento del software antivirus*) aggiornare ogni 30 (trenta) giorni solari il software antivirus;

- (*se non è disponibile un sistema automatico di aggiornamento del software firewall*) aggiornare ogni 30 (trenta) giorni solari il software firewall;

- (*se non è disponibile un sistema automatico di aggiornamento del software antispamming*) aggiornare ogni 30 (trenta) giorni solari il software antispamming;

- (*se non è disponibile un sistema automatico di aggiornamento del software di sistema*) aggiornare ogni 30 (trenta) giorni solari le patch del sistema operativo;

- sostituire ogni 30 (trenta) giorni solari le password di gestione e cancellare le credenziali utente obsolete.

4 – Incaricato alla Custodia delle Parole Chiave

L'incaricato alla Custodia delle Parole Chiave deve:

- ricevere, in busta chiusa, dagli Incaricati interni ed esterni le nuove parole chiave (Password) e conservarle in un contenitore chiuso a chiave;
- (*se non è disponibile un sistema automatico di preavviso e blocco della Password alla scadenza*) avvisare ogni Incaricato circa la scadenza di validità della Password;
- verificare ogni 3 (tre) mesi che tutti gli incaricati abbiano ottemperato alla sostituzione delle loro Password entro i termini stabiliti al paragrafo **2 – Incaricati**;
- relazionare al Titolare, su richiesta dello stesso, circa gli interventi effettuati sulle Password dagli Incaricati per quanto riguarda la periodica sostituzione, lo sblocco e le anomalie.

L'Incaricato alla Custodia delle Parole Chiave detiene:

- una copia della chiave del contenitore delle Password (un'altra copia della stessa è in possesso del Titolare);
- un registro degli interventi effettuati da tutti gli Incaricati sulle proprie Password, al di fuori delle periodiche sostituzioni.

5 – Incaricato al Salvataggio dei Dati

L'incaricato al Salvataggio dei Dati deve:

- (*se non è disponibile un sistema automatico di salvataggio dei dati*) effettuare ogni 7 (sette) giorni solari il salvataggio di tutti gli archivi elettronici (Base Dati);
- (*se è disponibile un sistema automatico di salvataggio dei dati*) verificare la corretta esecuzione del salvataggio di tutti gli archivi elettronici;
- archiviare, al termine della procedura di salvataggio e nei contenitori previsti (ved. Documento Programmatico Sulla Sicurezza), le copie di backup degli archivi elettronici;
- verificare ogni 30 (trenta) giorni solari la leggibilità delle copie di backup e sostituire i supporti usurati;
- eseguire ogni 30 (trenta) giorni solari la procedura di "Disaster Recovery" (esistenza ed efficienza del software di sistema e delle copie di backup);
- archiviare ogni anno nei contenitori previsti (ved. Documento Programmatico Sulla Sicurezza) gli archivi cartacei dell'anno precedente;
- archiviare ogni anno nei contenitori previsti (ved. Documento Programmatico Sulla Sicurezza) le copie di backup al 31 dicembre degli archivi elettronici;
- relazionare al Titolare, su richiesta dello stesso, circa gli interventi effettuati e le anomalie riscontrate.

6 – Incaricato alla Custodia della Sede Operativa

L'Incaricato alla Custodia della Sede Operativa deve:

- controllare, all'inizio ed al termine di ogni giornata lavorativa, che tutte le vie di accesso ai locali della Sede Operativa siano regolarmente chiuse;
- controllare, all'inizio ed al termine di ogni giornata lavorativa, che tutti i contenitori dei dati sensibili e/o giudiziari siano regolarmente chiusi;
- controllare, all'inizio ed al termine di ogni giornata lavorativa, che il sistema d'allarme sia regolarmente inserito;
- relazionare al Titolare se una delle direttive sopraccitate non può essere rispettata per la presenza autorizzata di altri Incaricati oltre l'orario di lavoro;
- avvisare prontamente il Titolare e/o l'Autorità di Pubblica Sicurezza nel caso di gravi anomalie;
- verificare che gli addetti esterni all'organizzazione siano muniti di regolare autorizzazione da parte del Titolare e che gli interventi si svolgano nel rispetto delle disposizioni di cui al D.Lgs. 196/2003 (Codice Privacy);
- far verificare dagli addetti alla manutenzione, in base al programma di manutenzione previsto dal Titolare, l'efficienza dei dispositivi di chiusura, antifurto e antincendio;
- tenere aggiornato il paragrafo A – Elenco degli Incaricati del presente Mansionario Privacy;
- relazionare al Titolare, su richiesta dello stesso, circa gli interventi effettuati e le anomalie riscontrate.

L'Incaricato alla custodia della Sede Operativa detiene:

- una copia delle chiavi del locale e dell'impianto d'allarme (le altre copie sono in possesso del Titolare);
- una copia del presente Mansionario Privacy.

A – Elenco degli Incaricati

Cod.	*Cognome/Nome o Ragione Sociale*	*Telefono*	*Qualifica*	*Out*
U1	ROSSI Mario		Responsabile	
U2	BIANCHI Luigi		Amministrazione Sistema	x
U1	ROSSI Mario		Custodia Parole Chiave	
U1	ROSSI Mario		Salvataggio dei dati	
U3	VERDI Giovanni		Custodia Sede Operativa	
U1	ROSSI Mario		Incaricato	
U2	BIANCHI Luigi		Incaricato	x
U3	VERDI Giovanni		Incaricato	
U4	PINCOPALLO s.p.a.		Affidato	x
U5	TIZIOCAIO s.n.c.		Responsabile	x
			Incaricato	
			Incaricato	
			Incaricato	
			Incaricato	
			Incaricato	
			Incaricato	
			Incaricato	
			Incaricato	
			Incaricato	
			Incaricato	
			Incaricato	
			Incaricato	
			Incaricato	
			Incaricato	
			Incaricato	

Le colonne della tabella contengono i seguenti dati:

- ***Cod***. = il codice di riferimento citato nel Documento Programmatico Sulla Sicurezza;
- ***Cognome/Nome o Ragione Sociale*** = il nominativo dell'Incaricato;
- ***Telefono*** = i recapiti telefonici dell'Incaricato;
- ***Qualifica*** = l'incarico ricoperto nell'azienda ai fini del Codice Privacy;
- ***Out*** = l'indicativo (x) di Incaricato esterno (Outsourcing).

La tabella è aggiornata dall'Incaricato alla Custodia della Sede Operativa.

B – Procedura di "Disaster Recovery"

La procedura di Disaster Recovery del Computer, in funzione della tipologia di intervento richiesta, è costituita da:

- se sono state rilevate anomalie gravi, che potrebbero compromettere l'utilizzo del computer e la salvaguardia dei dati, e se le riparazioni possono essere effettuate entro 7 giorni, eseguire in sequenza quanto descritto al successivo paragrafo **1**;

- se sono state rilevate anomalie gravi, che potrebbero compromettere l'utilizzo del computer e la salvaguardia dei dati, e se le riparazioni richiedono oltre 7 giorni, eseguire in sequenza quanto descritto al successivo paragrafo **2**;

- se si deve eseguire la verifica periodica di funzionalità del computer, eseguire in sequenza quanto descritto al successivo paragrafo **3**.

1) RIPRISTINO ENTRO 7 GIORNI

Eseguire in sequenza i seguenti passi operativi:

1. smontare l'hard disk dal computer e sottoporlo ai test standard di lettura/scrittura
2. se il test è negativo, passare al punto 6
3. riparare i componenti avariati
4. rimontare l'hard disk
5. passare al punto 10
6. montare un nuovo hard disk
7. definire le partizioni secondo le specifiche preesistenti (ved. DPSS – paragrafo 3.4) ed eseguire la formattazione
8. installare il sistema operativo secondo le specifiche preesistenti (ved. DPSS – paragrafo 3.5)
9. installare e configurare tutti i software preesistenti utilizzando i supporti presenti nell'armadio o nella cassettiera prevista (ved. DPSS – paragrafo 7.2)
10. eseguire una verifica funzionale su tutto il software installato
11. eseguire il recupero dei dati dagli ultimi supporti di backup conservati nell'armadio o nella cassettiera prevista (ved. DPSS – paragrafo 7.2)
12. eseguire una verifica funzionale sulle base dati previste (ved. DPSS – paragrafo 4.1)
13. compilare il report di avvenuta verifica di funzionalità

B – Procedura di "Disaster Recovery"

2) RIPRISTINO OLTRE 7 GIORNI

Eseguire in sequenza i seguenti passi operativi:

1. smontare l'hard disk dal computer e sottoporlo ai test standard di lettura/scrittura
2. se il test è negativo, passare al punto 11
3. montare l'hard disk su un computer per uso temporaneo
4. eseguire una verifica funzionale su tutto il software installato
5. eseguire una verifica funzionale sulle base dati previste (ved. DPSS – paragrafo 4.1)
6. consegnare all'utente il computer per uso temporaneo
7. riparare i componenti avariati
8. ritirare dall'utente il computer per uso temporaneo
9. rimontare l'hard disk sul computer originale
10. passare al punto 22
11. montare un nuovo hard disk su un computer per uso temporaneo
12. definire le partizioni secondo le specifiche preesistenti (ved. DPSS – paragrafo 3.4) ed eseguire la formattazione
13. installare il sistema operativo secondo le specifiche preesistenti (ved. DPSS – paragrafo 3.5)
14. installare e configurare tutti i software preesistenti utilizzando i supporti presenti nell'armadio o nella cassettiera prevista (ved. DPSS – paragrafo 7.2)
15. eseguire una verifica funzionale su tutto il software installato
16. eseguire il recupero dei dati dagli ultimi supporti di backup conservati nell'armadio o nella cassettiera prevista (ved. DPSS – paragrafo 7.2)
17. eseguire una verifica funzionale sulle base dati previste (ved. DPSS – paragrafo 4.1)
18. consegnare all'utente il computer per uso temporaneo
19. riparare i componenti avariati
20. ritirare dall'utente il computer per uso temporaneo
21. rimontare l'hard disk sul computer originale
22. eseguire una verifica funzionale su tutto il software installato
23. eseguire il recupero dei dati dagli ultimi supporti di backup conservati nell'armadio o nella cassettiera prevista (ved. DPSS – paragrafo 7.2)
24. eseguire una verifica funzionale sulle base dati previste (ved. DPSS – paragrafo 4.1)
25. compilare il report di avvenuta verifica di funzionalità

N.B. I punti 1, 3-6 e 11-18 devono sempre essere eseguiti entro 7 giorni dal manifestarsi dell'anomalia.

B – Procedura di "Disaster Recovery"

3) VERIFICA DI FUNZIONALITA'

Eseguire in sequenza i seguenti passi operativi:

1. eseguire il salvataggio dei dati sui supporti di backup previsti (ved. DPSS – paragrafo 4.3)
2. eseguire una verifica funzionale su tutto il software installato
3. eseguire il recupero dei dati dagli ultimi supporti di backup creati al passo 1
4. eseguire una verifica funzionale sulle base dati previste (ved. DPSS – paragrafo 4.1)
5. compilare il report di avvenuta verifica di funzionalità