# AZIENDA UNITÀ SANITARIA LOCALE FROSINONE


Istruzioni ai responsabili ed incaricati del trattamento dei dati personali comuni, sensibili e/o giudiziari

*(Decreto legislativo 30 giugno 2003, n. 196)*

# Indice

**INDICE** ..... **3**

**1. INTRODUZIONE** ..... **4**

1.1. RIFERIMENTI NORMATIVI E ALLE DISPOSIZIONI AZIENDALI. ..... 5
1.2. ORGANIZZAZIONE DEL DOCUMENTO ..... 5

**2. MISURE DI SICUREZZA** ..... **5**

2.1. CRITERI TECNICI ED ORGANIZZATIVI PER LA PROTEZIONE DELLE AREE E DEI LOCALI. ..... 5
*2.1.1. Archivi cartacei temporanei* ..... *6*
*2.1.2. Archivi cartacei di deposito* ..... *6*
*2.1.3. Selezione e scarto* ..... *7*
*2.1.4. Altre misure per il rispetto dei diritti degli interessati.* ..... *7*

**3. ISTRUZIONI PER IL TRATTAMENTO DEI DATI** ..... **7**

3.1. TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI. ..... 7
*3.1.1. Custodia* ..... *8*
*3.1.2. Comunicazione* ..... *8*
*3.1.3. Distruzione* ..... *8*
*3.1.4. Istruzioni per il trattamento di dati sensibili e/o giudiziari.* ..... *8*
3.2. TRATTAMENTI CON L'AUSILIO DI MEZZI ELETTRONICI. ..... 8
*3.2.1. Gestione delle password* ..... *9*
*3.2.2. Custode delle password* ..... *9*
*3.2.3. Presenza di estranei all'azienda* ..... *9*
*3.2.4. Istruzioni per il trattamento di dati sensibili e/o giudiziari.* ..... *9*
*3.2.5. Distruzione dei dati* ..... *9*
3.3. ISTRUZIONI PER LA REGOLARIZZAZIONE DEI RAPPORTI CON I FORNITORI: INFORMATIVA ..... 10
*3.3.1. Designazione dei Responsabili esterni del trattamento* ..... *10*
3.4. ISTRUZIONI PER REGOLARIZZARE IL TRATTAMENTO DEI DATI DEI DIPENDENTI/COLLABORATORI ..... 10
3.5. ISTRUZIONI PER LA DESIGNAZIONE DEGLI INCARICATI DEL TRATTAMENTO ..... 10
3.6. INFORMATIVA UTENTI ..... 10

**4. SICUREZZA DEL SOFTWARE E DELL'HARDWARE** ..... **10**

4.1. PROTEZIONE DA VIRUS INFORMATICI ..... 11
4.2. BACKUP DEI DATI ..... 11
4.3. UTILIZZO DELLA RETE INTERNET ..... 11

**5. SANZIONI PER INOSSERVANZA DELLE NORME** ..... **12**

# 1. Introduzione

Le presenti istruzioni costituiscono una serie organica di prescrizioni, orientate a garantire la sicurezza dei dati e delle informazioni detenute dagli uffici e dalle strutture della Azienda Sanitaria Locale di Frosinone. Tali prescrizioni devono intendersi come istruzioni impartite dal titolare del trattamento (la ASL di Frosinone) ai sensi dell'art. 29, comma 5[1] del decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali (di seguito anche denominato semplicemente Codice). Lo scopo delle prescrizioni è quello di costituire un supporto minimo all'azione dell'apparato burocratico, evitando i rischi di danneggiamento o dispersione dei dati, in ragione di un trattamento non corretto.

In ogni caso, il trattamento dei dati presso gli uffici e le strutture dell'Azienda deve avvenire:

- *nel rispetto del principio di riservatezza;*
- *in modo lecito e secondo correttezza;*
- *per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti e, successivamente, trattati;*
- *nel rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.*

Nello specifico, deve intendersi per:

- **Tutela della riservatezza**: l'attivazione di procedure di conoscenza delle informazioni detenute, a qualsiasi titolo, dall'Azienda, tali da consentire l'accesso solo a soggetti identificati e dotati di un adeguato grado di autorizzazione;
- **Integrità**: l'aggiornamento dei dati e delle informazioni realizzato periodicamente da personale autorizzato;
- **Disponibilità**: l'attivazione di procedure che consentano ai soggetti autorizzati di accedere in tempi utili alle informazioni.

Il livello di sicurezza in materia di trattamento dei dati raggiungibile mediante la mera applicazione delle procedure ed il corretto uso dei mezzi tecnici è tuttavia limitata. La sicurezza delle informazioni, per arrivare ad i livelli più elevati, richiede la condivisione degli obiettivi da parte del personale dell'Azienda. Esiste infatti una relazione tra la sicurezza e il sistema organizzativo: intanto l'Azienda può perseguire i suoi obiettivi, in quanto il personale impegnato sia motivato ad incrementare la propria produttività, efficienza, efficacia delle attività, in un sistema di flessibilità e di integrazione.

La prima misura di sicurezza è quindi di carattere organizzativo e coinvolge l'esatta definizione dei ruoli e delle responsabilità. A tal fine l'Azienda, quale titolare del trattamento dei dati personali, con la delibera del 22 novembre 2005, n° 1405, ha riconosciuto ai soggetti indicati la qualità di responsabili del trattamento dei dati, ai sensi dell'art. 29 del d.lgs. 30 giugno 2003, n. 196 (c.d. Codice in materia di trattamento dei dati personali)[2]. Le presenti istruzioni

[1] 5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

[2] art. 29
*(Responsabile del trattamento)*

1. Il responsabile e' designato dal titolare facoltativamente.
2. Se designato, il responsabile e' individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

intendono quindi corroborare l'azione dirigenziale, lasciando comunque intatta l'autonomia dirigenziale per individuare ulteriori modalità operative che rafforzino la sicurezza dei trattamenti, senza, tuttavia, appesantire l'azione amministrativa.

### 1.1. Riferimenti normativi e alle disposizioni aziendali.

In relazione al trattamento dei dati deve garantirsi la puntuale applicazione del:
* Codice in materia di protezione dei dati personali, decreto legislativo 30 giugno 2003, n. 196 e relativi allegati[3].
* Documento Programmatico della Sicurezza[4]
Nell'elaborazione delle presenti istruzioni si è tenuto conto:
- delle pronunce del Garante per la protezione dei dati personali:
- della Direttiva del Dipartimento della Funzione Pubblica dell'11 febbraio 2005, n. 1[5] – recante misure finalizzate all'attuazione nelle pubbliche amministrazioni delle disposizioni contenute nel decreto legislativo 30 giugno 2003, n. 196 che, seppur non direttamente applicabile nei confronti delle amministrazioni regionali e degli enti sanitari regionali, integra comunque, la più aggiornata elaborazione ministeriale in materia di trattamento dei dati personali.

3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.
4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.
5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

[3] Si rimanda al sito aziendale www.asl.fr.it/privacy.htm - Allegato M
[4] Si rimanda al sito aziendale www.asl.fr.it/privacy.htm
[5] Si rimanda al sito aziendale www.asl.fr.it/privacy.htm

### 1.2. Organizzazione del documento

Il documento è suddiviso in quattro parti:

- **Misure di sicurezza**: l'insieme delle misure di carattere tecnologico e di natura procedurale ed organizzativa per garantire un adeguato livello di sicurezza dei dati e delle informazioni;
- **Istruzioni per il trattamento dei dati**: indicazioni utili per la corretta gestione e custodia degli account di accesso ai sistemi informatici utilizzati per il trattamento dei dati;
- **Sicurezza del software e dell'hardware**: norme per la corretta gestione degli apparati informatici e del software installato su di essi.
- **Sanzioni per inosservanza delle norme**: sanzioni a carico dell'incaricato in caso di violazioni delle istruzioni operativa.

## 2. Misure di sicurezza

Per misure di sicurezza deve intendersi l'insieme delle prescrizioni di carattere tecnologico, procedurale ed organizzativo finalizzate all'implementazione di un adeguato livello di sicurezza nel trattamento dei dati.

### 2.1. Criteri tecnici ed organizzativi per la protezione delle aree e dei locali.

I dati e le informazioni di carattere sensibile e/o giudiziario devono essere trattati in aree protette, anche fisicamente, dall'accesso di persone non autorizzate. Sono perciò individuati

spazi, dotati di un sistema di controllo all'ingresso e di eventuali sbarramenti di sicurezza. Un livello di protezione più elevato deve attivarsi per gli ambiti di trattamento e/o conservazione dei dati sensibili e giudiziari e ove sono ubicati i server di residenza dei dati e delle informazioni. Le barriere fisiche, ove necessario, devono essere configurate in modo tale da impedire l'accesso alle persone non autorizzate. Quando restano vuote, le aree di sicurezza devono restare chiuse e con strumenti di controllo atti ad impedire accessi abusivi.
Il personale in servizio presso l'Azienda ha accesso ai locali esclusivamente per l'adempimento della prestazione lavorativa.
Il personale che espleta servizi strumentali (es.: pulizia dei locali) o si occupa della manutenzione e dei servizi accessori, deve essere espressamente autorizzato ad accedere alle aree di sicurezza.
L'assegnazione degli spazi di lavoro deve avvenire secondo criteri tali da impedire la promiscuità di permanenza e di utilizzazione tra:
> personale incaricato del trattamento di dati personali;
> personale non incaricato di trattamento di dati personali;
> soggetti estranei all'azienda
Il personale dipendente incaricato di trattamento ha accesso ai dati esclusivamente sulla base delle esigenze di servizio, conformemente ai seguenti principi:
> la necessità di trattamento;
> il minimo livello di conoscenza dei dati.

I Responsabili del trattamento devono vigilare affinché venga disciplinato e controllato l'accesso, il transito e la permanenza di persone estranee all'attività lavorativa nelle aree e nei locali adibiti a luoghi di lavoro, con particolare attenzione agli spazi in cui vengono custodite banche di dati o ove vengono trattati dati sensibili o giudiziari. E' altresì compito del Responsabile vigilare sull'introduzione in tali aree di oggetti, apparecchiature, sostanze o materiali che possono favorire il sorgere di rischi.
Devono essere previsti procedure, accorgimenti e strumenti per:
> consentire l'accesso alle aree dove vengono custoditi e trattati i dati al solo personale autorizzato, ivi compresi i locali destinati al personale addetto alla video sorveglianza;
> ostacolare l'accesso abusivo ai dati;
> segnalare la presenza di intrusi;

### 2.1.1. Archivi cartacei temporanei

La gestione degli archivi cartacei temporanei si ascrive alla competenza del Responsabile del trattamento. Lo stesso individua le tipologie dei documenti contenenti i dati sensibili e giudiziari ed i dipendenti incaricati dei relativi trattamenti. Il Responsabile dovrà assicurare che la documentazione venga custodita in armadi dotati di serratura, le cui chiavi dovranno essere conservate in modo appropriato.
I documenti contenenti dati sensibili o giudiziari devono essere conservati secondo modalità che precludano la visione, in occasione della consultazione di documenti di altro genere, mediante creazione di sottofascicoli in busta chiusa, con sottoscrizione dello stesso Responsabile o di un incaricato. Il Responsabile deve garantire l'integrità dei sottofascicoli in occasione dell'accesso all'archivio da parte di soggetti non legittimati alla consultazione dei dati sensibili o giudiziari.

### 2.1.2. Archivi cartacei di deposito

L'archivio cartaceo di deposito deve essere controllato in considerazione della circostanza che l'accesso a siffatta documentazione non è pubblico.

La consultazione potrà avvenire esclusivamente da parte del personale autorizzato o da parte di estranei autorizzati dal Responsabile. Il Responsabile dell'archivio cartaceo deve annotare su apposito registro gli estremi di ogni consultazione, precisando la data, la struttura richiedente, l'identità del soggetto che procede alla consultazione, l'oggetto della consultazione, le operazioni effettuate.
I documenti contenenti dati sensibili o giudiziari devono essere conservati secondo modalità che precludano la visione, in occasione della consultazione di documenti di altro genere, mediante creazione di sottofascicoli in busta chiusa, con sottoscrizione dello stesso Responsabile o di un incaricato. Il Responsabile deve garantire l'integrità dei sottofascicoli in occasione dell'accesso da parte di soggetti non legittimati alla consultazione dei dati sensibili o giudiziari.

### 2.1.3. Selezione e scarto

La selezione e lo scarto della documentazione deve avvenire nel rispetto delle prescrizioni normative vigenti.

### 2.1.4. Altre misure per il rispetto dei diritti degli interessati.

L'azienda al fine di garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale dovrà:
> predisporre appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;
> predisporre soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rilevare lo stato di salute;
> predisporre opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prescrizione di pronto soccorso;

## 3. Istruzioni per il trattamento dei dati

Il Responsabile del trattamento dei dati è tenuto ad effettuare controlli sulle attività degli incaricati del trattamento, al fine di garantire la puntuale applicazione delle disposizioni contenute nel Codice. Ogni Responsabile informa annualmente gli incaricati dell'attivazione di sistemi di controlli legati a criteri in parte statistici in parte casuali.
I responsabili, preferibilmente, precisano le istruzioni per il corretto trattamento dei dati, in forma scritta. E' sempre ammessa la diffusione di istruzioni in forma orale, in particolare allorquando vi sia l'urgenza di salvaguardare i principi in materia di trattamento dei dati personali.
Deve in ogni caso garantirsi l'osservanza delle misure minime di sicurezza, contenute negli artt. 33 – 36 del d.lgs. n. 196 del 2003[6] e nel relativo allegato B, indifferentemente dalla natura del supporto contenente dati.

### *3.1. Trattamenti senza l'ausilio di strumenti elettronici.*

Il trattamento di dati senza strumenti elettronici, coinvolge i dati contenuti in tutti i supporti cartacei o simili che, comunque non richiedano l'uso di elaboratori elettronici. Ove esistano copie o riproduzioni di documenti che contengono dati personali, le medesime devono essere protette con le stesse misure di sicurezza applicate agli originali.

[6] Cfr. Allegato "E"

### 3.1.1. Custodia

* I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili alle persone non incaricate del trattamento, mediante localizzazione presso spazi con accesso riservato (es. armadi o cassetti chiusi a chiave).
* I documenti contenenti dati personali prelevati dagli archivi per l'attività quotidiana, devono essere ivi collocati al termine della giornata.
* I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

### 3.1.2. Comunicazione

* La diffusione dei dati personali deve avvenire in base al principio dello "stretto indispensabile", talché non devono essere condivisi, comunicati o inviati a soggetti o istituzioni che non ne abbiano bisogno per lo svolgimento delle funzioni lavorative, a prescindere dall'eventuale qualifica di responsabili o incaricati di altra struttura. I dati non devono essere comunicati all'esterno della struttura, e comunque a soggetti terzi, se non previa autorizzazione.

### 3.1.3. Distruzione

Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere soppressi mediante apparecchi "distruggi documenti" o, in assenza, attraverso modalità che impediscano qualsiasi ricomposizione.

### 3.1.4. Istruzioni per il trattamento di dati sensibili e/o giudiziari.

* I documenti contenenti dati sensibili e/o giudiziari devono essere sottoposti al controllo dei responsabili i quali, a loro volta, potranno avvalersi degli incaricati per la custodia e/o il trattamento. Il Responsabile deve impedire l'accesso a persone prive di autorizzazione nei luoghi e nei momenti in cui si trattano dati sensibili e/o giudiziari. Conseguentemente, il trattamento di dati sensibili e/o giudiziari contenuti in documenti cartacei deve avvenire per il tempo strettamente necessario al trattamento, con successiva immediata archiviazione dei dati.
* L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.
* Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure procedere all'identificazione su un apposito registro.

## *3.2. Trattamenti con l'ausilio di mezzi elettronici.*

Per trattare i dati mediante dispositivi informatici, deve seguirsi una procedura di autenticazione che consenta l'identificazione del Responsabile o dell'Incaricato, mediante "credenziali di autenticazione". Le "credenziali di autenticazione" consistono in un user-ID, associato ad una parola chiave segreta password.
Le user-ID e password individuali per l'accesso alle applicazioni non devono essere mai condivise con altri soggetti, anche se incaricati del trattamento. Nel caso in cui occorre permettere l'accesso da parte di altri utenti, è necessario richiedere la generazione di una nuova password.
Per i PC collegati in rete, i Responsabili e gli Incaricati devono superare le procedure di identificazione, quali formalità preliminari per accedere alle risorse presenti nella rete aziendale; nel

caso di utilizzo di applicazioni centralizzate, i responsabili e gli incaricati devono provvedere anche alla propria identificazione sul sistema applicativo centrale, secondo le modalità e le regole previste dall'applicativo stesso.
Tutti i Responsabili e gli Incaricati che utilizzano un personal computer per il trattamento di dati personali non collegato in rete, sono tenuti a proteggere l'accesso alla propria postazione di lavoro attivando una password (BIOS del PC e/o del sistema operativo).

### 3.2.1. Gestione delle password

La password è assegnata ai Responsabili ed agli Incaricati mediante sistemi meccanici che consentano l'enucleazione di password conformi alle prescrizioni contenute nell'Allegato B del d.lgs. n. 196 del 2003 (almeno 8 caratteri) e la periodica disattivazione/sostituzione.
I Responsabili devono garantire l'esclusività dell'uso della password, in particolare impedendo che incaricati, o altri, si avvalgano di credenziali di autenticazione a qualunque titolo percepite. Nessuno deve annotare la propria password su supporti facilmente rintracciabili e, soprattutto, in prossimità della postazione di lavoro utilizzata.
I Responsabili devono altresì accertarsi che gli incaricati cambino la password almeno ogni sei mesi, ovvero se trattano dati sensibili e/o giudiziari ogni tre mesi.

### 3.2.2. Custode delle password

In caso di assenza od impedimento dell'incaricato e contestuale esigenza di accedere ai dati detenuti presso banche dati o p.c. in uso all'incaricato, i responsabili devono attivare procedure di accesso temporaneo, mediante generazione di nuove credenziale di autenticazione. Le nuove credenziali di autenticazioni devono essere disattivate al termine della sessione straordinaria di lavoro. Conformemente a quanto previsto nel punto 10 dell'all. "B - Disciplinare tecnico" del Codice, il responsabile deve accertarsi che sia fornita adeguata comunicazione all'incaricato del sopravvenuto accesso al p.c. o alla banca dati da parte di altro incaricato.

### 3.2.3. Presenza di estranei all'azienda

I Responsabili devono garantire che le attività degli incaricati non vengano espletate alla presenza o secondo modalità che consentano ad estranei, di acquisire dati e/o informazioni detenute dall'azienda. A tal fine i Responsabili devono impartire istruzioni finalizzate ad evitare che personale estraneo o visitatori restino negli spazi ove si trattano dati personali. In ogni caso, gli incaricati sono tenuti a riporre i documenti contenenti dati personali secondo modalità che ne impediscano al visione a qualunque soggetto non legittimato i visitatori.
In caso di allontanamento dal p.c. l'incaricato deve attivare la procedura c.d. "salvaschermo", al fine di evitare la visione dei documenti in lavorazione.

### 3.2.4. Istruzioni per il trattamento di dati sensibili e/o giudiziari.

I dati anagrafici devono essere conservati separatamente da quelli sanitari che, invece, se contenuti in elenchi, registri o banche dati devono essere trattati con "tecniche di cifratura o codici identificativi che consentano di identificare gli interessati solo in caso di necessità".

### 3.2.5. Distruzione dei dati

I supporti magnetici od ottici contenenti dati personali devono essere cancellati

prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti secondo modalità che ne impediscano la ricomposizione.

### *3.3. Istruzioni per la regolarizzazione dei rapporti con i fornitori: Informativa*

Ogni struttura Aziendale dovrà regolarizzare i rapporti con ogni fornitore dell'Azienda mediante l'invio dell'informativa prevista dall'art. 13 del D.Lgs 196/03 (allegato D), tramite raccomandata A/R o fax. La ricevuta dell'avvenuto invio deve essere conservata presso la struttura.

#### 3.3.1. Designazione dei Responsabili esterni del trattamento

I Responsabili del trattamento individuati nell'allegato B 2, dovranno farsi carico di designare i soggetti esterni che trattano dati per conto della propria struttura in virtù di un contratto in essere, a Responsabili esterni del trattamento utilizzando lo schema previsto nell'allegato E e F. Allegato E per quanto concerne i contratti di Assistenza/Manutenzione dei sistemi hardware e software e Allegato F per i servizi esternalizzati che prevedono il trattamento di dati comuni/sensibili/giudiziari (es. gestione cartelle cliniche, dignostica in convenzione ecc.).

### *3.4. Istruzioni per regolarizzare il trattamento dei dati dei dipendenti/collaboratori*

La S.C. Risorse Umane dovrà farsi carico di informare il dipendente/collaboratore mediante l'invio allegato alla busta paga dell'informativa prevista dall'art. 13 del D.Lgs 96/03 (allegato G). L'informativa dovrà essere allegata al contratto di assunzione, di collaborazione, di consulenza ecc. di nuova adozione.

### *3.5. Istruzioni per la designazione degli Incaricati del trattamento*

I Responsabili del trattamento individuati nell'allegato B 2, dovranno designare Gli Incaricati del trattamento della propria struttura utilizzando lo schema riportato nell'allegato H. La copia della lettera di designazione dell'Incaricato dovrà essere conservata dal Responsabile e successivamente inviata all'Ufficio Privacy a seguito di richiesta.

### *3.6. Informativa Utenti*

Nell'allegato I è riportato lo schema di Informativa e Consenso da utilizzare al momento della raccolta dei dati dell'Interessato. I Responsabili del trattamento dovranno curare la pubblicazione dell'Informativa e la conservazione del relativo consenso. Il soggetto interessato potrà esercitare i propri diritti in materia di protezione dei dati personali avvalendosi della modulistica presente sul sito internet aziendale www.asl.fr.it/privacy.htm (allegato L).

## 4. Sicurezza del software e dell'hardware

Le norme riportate in questa sezione sono finalizzate ad aumentare la sicurezza dei singoli sistemi informatici utilizzati per il trattamento dei dati. Il rispetto di tali norme garantisce anche che non vengano compromesse le misure di sicurezza del sistema informativo ad opera di un utente

regolarmente autorizzato, che, inconsapevolmente, adotti comportamenti in grado di violare l'integrità del sistema (installazione inconsapevole di virus o di "trojan horse").
**I Responsabili devono assicurare che gli incaricati non installino sulla postazione di lavoro programmi non attinenti alle attività di ufficio, ovvero programmi senza la preventiva autorizzazione.** I Responsabili, qualora non siano in grado di apprezzare l'impatto dei programmi per i quali si è chiesta l'installazione, si coordinano con il titolare del trattamento per concordare la linea di condotta. **Gli incaricati non devono modificare le configurazioni hardware e software, senza l'autorizzazione del Responsabile del trattamento.**
I Responsabili devono garantire che gli incaricati provvedano all'aggiornamento, con cadenza almeno mensile, del software riferito alla sicurezza applicabile alla versione di sistema operativo.

## *4.1. Protezione da virus informatici*

I virus informatici rappresentano una delle minacce principali per la sicurezza dei sistemi informativi e dei dati in esso presenti. Un virus informatico, come è noto, può modificare e/o cancellare i dati in esso contenuti, compromettere la sicurezza e la riservatezza di un intero sistema informativo, rendere indisponibile tutto o parte del sistema, compresa la rete di trasmissione dati.
Al fine di non aumentare il livello di rischio di contaminazione da virus è opportuno che Responsabili ed incaricati provvedano a:
1. accertarsi che sul computer sia sempre operativo il programma antivirus aggiornato e con la funzione di monitoraggio attiva;
2. sottoporre a controllo con il programma installato sul proprio p.c., tutti i supporti di provenienza esterna prima di eseguire files in esso contenuti;
3. accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; nel caso che il mittente dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati
4. non condividere con altri computer il proprio disco rigido o una cartella di files senza password di protezione in lettura/scrittura;
5. proteggere in scrittura i propri floppy disk contenenti programmi eseguibili e/o file di dati;
6. limitare la trasmissione tra computer in rete di file eseguibili e di sistema;
7. **non scaricare da Internet programmi o file non inerenti l'attività lavorativa o comunque sospetti.**

## *4.2. Backup dei dati*[7]

Gli incaricati che trattano i dati sui propri p.c. non collegati in rete, o per i quali non sono previsti back-up centralizzati, devono provvedere al back-up dei dati almeno settimanalmente. I supporti di back-up devono essere custoditi in luogo sicuro e ad accesso controllato. In occasione di ogni back-up, deve preliminarmente accertarsi l'esito positivo della procedura nonché disporsi la distruzione del precedente supporto. Tutti i Responsabili verificano la puntuale osservanza di siffatta prescrizione.

## *4.3. Utilizzo della rete Internet*

Il sistema informativo ed i dati in esso contenuti possono subire gravi danneggiamenti per un utilizzo improprio della connessione alla rete Internet, anche in conseguenza della

[7] Per Backup si intende il salvataggio dei dati di interesse in copie di sicurezza da effettuarsi periodicamente su CD o altri supporti.

diffusione di virus informatici o accessi non autorizzati. I Responsabili vigilano che gli incaricati utilizzino la connessione Internet esclusivamente per lo svolgimento dei propri compiti istituzionali, non diffondano messaggi di posta elettronica di provenienza dubbia, non utilizzino la casella postale assegnata per fini privati e personali, non si avvalgano di servizi di comunicazione e condivisione di files (condivisione P2P "peer-to-peer"[8]).

Il Responsabile è tenuto a ricordare, a tutto il personale addetto alla propria struttura, il divieto di violare le prescrizioni di cui agli articoli 615 ter – "Accesso abusivo ad un sistema informatico e telematico"[9], 615 quater – "Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematica"[10], 615 quinquies – "Diffusione di programmi diretti a danneggiare ed interrompere un sistema informatico"[11] del codice penale, nonché del Decreto Legge 22 Marzo 2004 n. 72[12], convertito in legge con modificazioni, dalla Legge 21 Maggio 2004 n. 128 (c.d. "Legge Urbani") diretta a sanzionare la condivisione e/o fruizione di file relativi ad un'opera cinematografica, od assimilata, protetta da diritti d'autore.

È pertanto vietato effettuare il download[13] e l'installazione di programmi dalla rete Internet, a meno che non si abbia l'esplicita autorizzazione da parte del Responsabile del trattamento.

## 5. Sanzioni per inosservanza delle norme

Le presenti istruzioni integrano elementi di valutazione della condotta del lavoratore. La violazione delle prescrizioni contenute può generare, oltre che responsabilità penali e civili, l'irrogazione di sanzioni disciplinari, in considerazione della gravità della condotta.

[8] Due computer effettuano una "condivisione peer to peer" quando scambiano file tra di loro senza ricorrere ad un server centrale che ne traccia il percorso.

[9] L'art. 615 ter c.p., rubricato "accesso abusivo ad un sistema informatico o telematico", punisce chiunque si introduca senza autorizzazione in un sistema informatico o telematico protetto da misure di sicurezza o vi si mantenga contro la volontà esplicita o tacita di chi ha il diritto di escluderlo. La norma recita testualmente : "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero si mantiene contro la volontà di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni"

[10] L'art. 615 quater Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a lire 10 milioni. La pena è della reclusione da uno a due anni e della multa da lire 10 milioni a 20 milioni se ricorre taluna delle circostanze di cui ai nn. 1) e 2) del quarto comma dell`art. 617 quater.

[11] art. 615 quinquies Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, e' punito con la reclusione sino a due anni e con la multa sino a lire venti milioni(1).
*(1)Articolo aggiunto dall'art. 4, L. 23 dicembre 1993, n. 547.*

[12] Si rimanda al sito aziendale www.asl.fr.it/privacy.htm

[13] Il "download" è l'azione di scaricare o prelevare dalla rete (ad esempio da un sito web) un file (audio, mp3, video, materiale pornografico, ecc.), trasferendolo sul proprio disco rigido