Azienda Ospedaliera Universitaria
Università degli Studi della Campania Luigi Vanvitelli

Preg.ssimo Sig.
c/o …….

Data,…

Oggetto: D.Lgs. 196/03 in materia di "privacy"

- trattamento dei dati a cura del personale "incaricato"
- formalizzazione di indicazioni operative

A) PREMESSA

1. Il D.Lgs. 196/03 prevede le regole per le operazioni di trattamento di dati personali, quali

- raccolta
- utilizzo
- registrazione
- elaborazione
- consultazione
- selezione
- raffronto
- blocco
- cancellazione
- conservazione
- comunicazione
- organizzazione
- modificazione
- estrazione
- interconnessione
- diffusione
- distruzione

indifferentemente che questa vengano svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati;

2. Al fine di garantire la debita conoscenza da parte di tutti i dipendenti della disciplina inerente la tutela della riservatezza dei dati la *"A.O.U. "L. Vanvitelli"* ha organizzato corsi mirati anche ad assicurare il rispetto delle norme contenute nella D.Lgs. 196/03, attività didattiche cui la S.V. ha preso parte in data ……

3. La S.V. è già in possesso di copia del provvedimento normativo in questione e, allo scopo di consentirne una costante corretta consultazione, in allegato è riportato un glossario di pratico utilizzo (allegato 1)

B) CONFERIMENTO DELL'INCARICO

4. Considerato che la S.V. rientra tra il personale che effettua il trattamento di dati personali per conto della nostra azienda

a) alla luce di quanto premesso,

b) ai sensi dell'art. 30, comma 1 e dell'art. 30 comma 2 del D.Lgs. 196/03 sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali,

Le comunichiamo che assume il ruolo di incaricato dei seguenti trattamenti:

<segue lista dei trattamenti specificandone la natura dei dati e le eventuali operazioni consentite.

C) INDICAZIONI OPERATIVE

5. Pertanto, nello svolgimento delle Sue mansioni

a) potrà eseguire, per lo svolgimento delle attività del Suo ufficio, il trattamento dei dati personali ai quali ha accesso, ivi compresa la comunicazione alle Aziende o enti:

<segue lista con cui esiste continuativo rapporto di lavoro.

oltre ad eventuali altre organizzazioni che le verranno comunicate di volta in volta in ragione delle esigenze che si verranno a determinare per il perseguimento degli obbiettivi aziendali

6. Nell'espletamento delle funzioni demandate ed in particolare in quelle oggetto dell'incarico la S.V. dovrà usare le massima riservatezza e discrezione nella tenuta dei dati di cui sopra e nella conseguente loro protezione (allegato 3), il cui trattamento deve essere effettuato seguendo principi di correttezza e liceità; la SV ha l'assoluto divieto di comunicare, diffondere, utilizzare i dati in questione in assenza di autorizzazione da parte del titolare e comunque nei casi non consentiti dalla legge. In armonia con gli obblighi che Le derivano, in quanto prestatore di lavoro subordinato, dagli artt. 2104 e 2105 c.c., e in stretta osservanza del regolamento concernente le 'Misure minime di sicurezza' introdotte con l'ALLEGATO B al D.Lgs. 196/03 (allegato 2).

7. qualora la SV dovesse ricevere da un interessato dal trattamento, richiesta di accesso ai propri dati ex art. 7 DLgs 196/03, dovrà darne tempestiva notizia al responsabile e/o al titolare, onde consentirgli di poter espletare i doveri inerenti alla richiesta stessa e dale così idoneo e tempestivo riscontro, nel più breve tempo possibile e comunque nei termini previsti dal decreto di cui sopra, termine che Le si ricorda essere di 15 giorni.

Copia della presente comunicazione - consegnata in due esemplari - dovrà essere restituita debitamente firmata per accettazione.

data _____

IL RESPONSABILE

_____

PER ACCETTAZIONE

L'INCARICATO

data _____ _____

All. 1 alla lettera di incarico: GLOSSARIO

All. 2 alla lettera di incarico: MISURE MINIME

All. 3 alla lettera di incarico: INDICAZIONI OPERATIVE

allegato 1

GLOSSARIO

Sono qui riportati i termini specifici usati nella legge con spiegazioni e commenti facendo riferimento agli specifici articoli in cui sono spiegati o usati.

autorizzazione: autorizzazione formale da parte del Garante, necessaria per i trattamenti riguardanti dati sensibili (art. 40).

comunicazione: messa a disposizione dei dati a individuate terze persone in qualunque forma, invio di tabulati, files, permesso di lettura, (art. 4.l); non costituisce comunicazione l'accesso ai dati da parte del rappresentante privacy, del responsabile del trattamento e degli incaricati del trattamento.

consenso: autorizzazione dell'interessato al trattamento dei dati (art. 23); esso deve essere documentato per iscritto per i dati comuni, rigorosamente sottoscritto dall'interessato per quelli sensibili. Per essere valido il consenso deve essere informato e libero.

dato personale: qualsiasi informazione riconducibile anche indirettamente, ad esempio attraverso codici identificativi, ad una persona fisica (art. 4.b).

dato sensibile: dati particolarmente delicati riguardanti: origine razziale etnica; convinzioni religiose o filosofiche; opinioni politiche; iscrizione o adesione a partiti o sindacati, a movimenti o organizzazioni a carattere religioso, filosofico, politico, sindacale; stato di salute; vita sessuale (art.4.d.).

dato giudiziario: dati personali idonei a rivelare i provvedimenti richiamati dalle lettere da a) a o) e da r) a u) dell'art. 3 comma 1 del DPR 313/02 in materia di casellario giudiziale, anagrafe delle sanzioni amministrative che dipendono da reato e dei relativi carichi pendenti, o la qualità di imputato o indagato ex artt. 60 e 61 del codice di procedura penale.

diffusione: messa a disposizione dei dati a pubblico indistinto mediante, ad esempio, stampa o altri mezzi di comunicazione (art.4.m).

diritti dell'interessato: i diritti dell'interessato in merito al trattamento di dati che lo riguardano sono (art. 7): conoscere con accesso gratuito al registro del Garante l'esistenza di trattamenti che lo riguardano e le relative caratteristiche notificate; chiedere ed ottenere dal titolare notizie sui propri dati, e sui trattamenti, rettifica o cancellazione dei dati, verificandone l'esecuzione; opporsi a specifici trattamenti.

Garante: ente costituito appositamente per controllare praticamente l'applicazione della legge, anche con la gestione operativa delle informazioni relative ai trattamenti (artt.153 e successivi).

incaricato: persona che esegue materialmente le operazioni connesse con il trattamento (art. 4.h), con mansioni delegate dal titolare o dal responsabile.

informativa: serie di notizie che devono essere date all'interessato prima di chiedere il consenso o, in altri casi, prima di iniziare il trattamento (art.13).

interessato: la persona fisica, giuridica o altro ente cui i dati si riferiscono (art. 4.i).

notificazione: comunicazione al Garante dell'apertura di un trattamento e delle sue caratteristiche (art. 37).

responsabile: persona, o ente, che sovrintende al trattamento dei dati, sottoposta al controllo del titolare, assumendo specifiche responsabilità (art. 4.g).

titolare: persona o ente cui competono le decisioni, e quindi tutte le responsabilità, sul trattamento dei dati; è il 'proprietario' dei dati (art. 4.f).

trattamento: qualsiasi forma di utilizzo di dati: raccolta, classificazione, archiviazione, elaborazione manuale o con strumenti automatici o informatici (art. 4.a).

allegato 2

ALLEGATO B
DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Artt. da 33 a 36 del codice)

Trattamenti con strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e

dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Soppresso art. 45 comma 1, lett.d) del d.g.l 9/02/2012, n.5

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. *Soppresso art. 45 comma 1, lett.d) del d.g.l 9/02/2012, n.5*

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e

dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Allegato 3

raccomandazioni di carattere generale

principi di base

1. Il responsabile per il trattamento dei dati personali è tenuto a rispettare e a far rispettare le indicazioni riportate:

a) nella presente circolare,

b) in quelle che successivamente verranno emanate
   I) a completamento di quanto qui definito,
   II) a copertura di sopravvenute esigenze di carattere tecnico, organizzativo o legislativo.

2. Il presente documento dovrà essere illustrato al personale dipendente che effettua operazioni di trattamento di dati personali, o di gestione e manutenzione delle apparecchiature impiegate per il trattamento automatizzato, che – a seguito delle istruzioni preliminarmente impartite – hanno assunto o assumeranno, rispettivamente, i ruoli di "incaricato", "responsabile per la sicurezza", "amministratore di sistema" e, ove necessario, "preposto alla tutela delle password", formalizzati con i modelli di cui agli allegati 2, 3, 4, 5.

3. Il personale dipendente "incaricato del trattamento"

a) sarà destinatario di un modulo didattico di sensibilizzazione, al fine di consentirgli di ottenere i chiarimenti necessari per un corretto e sereno espletamento delle mansioni affidate

b) riceverà un manuale d'istruzioni specifiche che solleva il responsabile dalla redazione di regole e spiegazioni dettagliate.

4. Il responsabile, compilando il modello in allegato 7, deve predisporre un elenco dei soggetti "incaricati" avendo cura di

a) riportare il nominativo e la qualifica/mansione,

b) far apporre la firma per l'avvenuta istruzione preliminare e la presa in visione della presente circolare,

c) conservare ed aggiornare la lista,

d) trasmetterne copia e relativi aggiornamenti al titolare.

5. Il responsabile deve altresì garantire la corretta tenuta del registro degli accessi ai dati da parte di soggetti non incaricati che costituisce l'allegato 8 alla presente circolare.

controllo degli accessi ai dati personali

6. Per quanto concerne il controllo degli accessi "fisici" è disposta l'osservanza delle seguenti disposizioni:

a) i locali in cui sono trattati o custoditi dati personali devono essere adeguatamente protetti e non accessibili al pubblico o a dipendenti non incaricati dello specifico trattamento;

b) la necessità di accesso a dati personali da parte di soggetti esterni al novero degli incaricati (ad esempio per finalità connesse all'esercizio dei diritti di cui alla legge 241 o al D.Lgs. 196/03) deve avvenire sotto la diretta sorveglianza e assistenza di personale incaricato con la registrazione delle operazioni effettuate sull'apposito registro di cui all'allegato 8 alla presente circolare;

c) i documenti contenenti dati personali sensibili o giudiziari – meglio per i dati di ogni natura - devono essere conservati in armadi o scrivanie con la possibilità di chiusura a chiave (Punto 28 ALLEGATO B)
   I) ogni qualvolta non siano sotto il diretto controllo di chi li deve utilizzare per ragioni d'ufficio
   II) quando i locali in cui viene svolta l'ordinaria attività non siano occupati dai dipendenti preposti.

d) le normali procedure di sicurezza hanno validità nel corso del normale orario di servizio, dopo il quale tutte le aree destinate ad ufficio o attività amministrative devono restare chiuse. E' fatto obbligo di identificare e registrare chiunque acceda agli archivi contenenti dati sensibili o giudiziari dopo l'orario di lavoro. Ove non è possibile controllare gli accessi, le persone che accedono a tali archivi sono preventivamente autorizzate (Punto 29 ALLEGATO B).

7. Il controllo degli accessi "logici", vale a dire quello eseguito attraverso computer e/o terminali, dovrà rispettare le seguenti modalità operative:

a) gli strumenti informatici contenenti dati personali devono essere protetti con meccanismi che richiedano la digitazione di una parola chiave o altro sistema di autenticazione (Punti da 1 a 8 ALLEGATO B).
   I. all'atto dell'accensione dell'apparato,
   II. alla richiesta di accesso a determinate risorse,
   attività che al momento della sua introduzione tra le procedure operative fruirà - ove necessario - del supporto di personale tecnico designato allo specifico scopo;
   III. all'avvio di applicativi che prevedono ulteriori funzioni di autenticazione;

b) Le password devono essere sufficientemente robuste e nello specifico:
   I. lunghe almeno 8 caratteri;
   II. composte da lettere minuscole e maiuscole, numeri e simboli;
   III. difficilmente riconducibili alla vita personale dell'incaricato (nome, data di nascita, nomi di parenti…);
   IV. evitando password molto comuni (pippo, topolino, love…)
   V. evitando anche password troppo difficili da ricordare, onde evitare che l'utente possa essere costretto a scriverle su un pezzo di carta, apposto *"magari sul monitor";*
   VI. per comporre password adeguate si potrebbe ricorrere alle iniziali di una frase facile da ricordare per l'incaricato, magari sostituendo di tanto in tanto lettere con simboli (es. "@ "al posto di "a" oppure "][" al posto di "i"), alternando maiuscole e minuscole, aggiungendo numeri;
   VII. le password devono essere sostituite almeno ogni sei mesi (tre per i trattamenti di dati sensibili o giudiziari);

c) le apparecchiature che per limiti di carattere tecnologico non possano essere protette da parole chiave dovranno
   I. visualizzare sullo schermo, all'atto dell'accensione,
   II. riportare in evidenza su pannello o etichetta,
   l'avvertenza che non possono essere impiegate per il trattamento di dati personali.
   Unica eccezione per detti apparati è l'elaborazione dei dati con la memorizzazione dei medesimi su floppy disk e con l'adozione di precauzioni specifiche - quali quelle già specificate per i documenti cartacei - per la conservazione dei supporti magnetici in questione.

d) l'accesso alle risorse deve prevedere entrambe le fasi di
   I. **identificazione** (digitazione del codice identificativo personale, utilizzo di carta magnetica o a microprocessore, o altro sistema di "presentazione")
   II. **autenticazione** (digitazione della parola chiave corrispondente a quella dell'identificativo dichiarato)

dell'utilizzatore, così da assicurare maggiore certezza sul "chi" si avvale delle risorse disponibili sul sistema.

e) i computer a disposizione degli incaricati non possono essere utilizzati per scopi personali, non devono ospitare procedure o programmi che non siano stati rilasciati dalla competente struttura aziendale o installati con precisa autorizzazione

f) quando ci si allontana, anche per cinque minuti dallo strumento impiegato per il trattamento, viene fatto obbligo di terminare la sessione di lavoro. L'elaboratore deve essere sempre custodito (è sufficiente che un collega rimanga nella stanza), o non accessibile (è sufficiente chiudere a chiave la stanza). E' consigliabile impiegare gli screen saver protetti da password.

autorizzazioni all'accesso ai dati

8. Il responsabile del trattamento dei dati personali deve provvedere a garantire il rilascio delle autorizzazioni all'accesso ai dati (Punti 12 e 13 ALLEGATO B).

a) ai soli soggetti che svolgano mansioni per le quali sia necessaria la disponibilità di tali informazioni,

b) per i soli dati pertinenti i compiti affidati,

c) per il solo tempo effettivamente occorrente all'espletamento dell'incarico conferito;

9. Il responsabile deve assicurare l'attualità di tali autorizzazioni (Punti 14 e 27 ALLEGATO B).

a) provvedendo a controllare costantemente la vigenza dei requisiti che sono stati presi in considerazione all'atto del rilascio dell'autorizzazione stessa,

b) verificando quindi la posizione di competenza e coerenza dei singoli soggetti rispetto i trattamenti,

c) bloccando tempestivamente le autorizzazioni del personale che viene trasferito ad altre mansioni o ad altra sede oppure che cessa di prestare servizio presso l'organizzazione;

10. L'accesso in caso di emergenza agli apparati protetti da password dai legittimi assegnatari sarà eseguito (Punto 10 ALLEGATO B).

a) convocando l'utente presso la postazione di lavoro, affinché provveda direttamente a fornire i dati resisi necessari,

b) superando tale protezione nel rispetto della procedura stabilita dall'azienda o ente,
   I. informando l'utente ed eventualmente,
   II. verbalizzando le operazioni svolte con l'assistenza di altro incaricato,
   III. disabilitando l'apparato fino al rientro dell'assegnatario.

11. Il controllo della legittimità delle operazioni di trattamento svolte dagli incaricati deve essere effettuato

a) riscontrando le attività eseguite con il livello di autorizzazione concesso,

b) segnalando al titolare i tentativi di violazione delle misure di sicurezza in essere,

c) assicurando il tempestivo intervento - con l'eventuale segnalazione all'Autorità giudiziaria - in caso di violazione al D.Lgs. 196/03.

raccomandazioni di carattere tecnico

12. Le attività di manutenzione e riparazione degli apparati che contengano dati di tipo sensibile o che abbiano la possibilità di accedere a banche dati attraverso collegamenti in rete, devono essere svolte sotto il diretto controllo del responsabile o dell'amministratore di sistema o persona delegata.

13. Qualora si presenti la necessità di portare un apparato o parte di esso al di fuori dell'infrastruttura, sarà necessario adottare tutte le precauzioni atte ad evitare il diffondersi dei dati sensibili contenuti..

14. Per quanto concerne la rete locale dovranno essere abilitate le sole connessioni necessarie al funzionamento degli uffici

15. Sono assolutamente vietate connessioni attive o attivabili in luoghi non controllati o al di fuori degli uffici

16. Periodicamente il responsabile, coadiuvato se del caso da personale tecnico, dovrà effettuare una ricognizione per verificare l'integrità fisica della rete locale

17. Occorre evitare per quanto possibile di sistemare le stampanti condivise da più utenti in luoghi aperti al pubblico

18. Dovrà essere conservato un log con i dati identificativi di ogni processo di stampa (file, data, ora, utente, quantità ecc..)

19. Le copie di salvataggio dei dati avranno luogo attraverso l'attività di backup che deve essere effettuata (Punto 18 ALLEGATO B).

a) con frequenza giornaliera su tutti i server di rete

b) almeno settimanale per i dati più importanti memorizzati sulle unità di lavoro

Tutte le copie devono essere verificate e devono essere adottate misure per il ripristino in tempi rapidi (comunque non superiori a 7 giorni) in caso di eventi dannosi (Punto 23 ALLEGATO B).

20. Le unità magnetiche, ottiche o altro contenenti i dati di backup dovranno essere conservate in armadi con chiusura a chiave, ignifughi o, possibilmente in luoghi relativamente sicuri da pericoli di incendi (Punto 21 ALLEGATO B).

21. Tutte le postazioni dovranno essere dotate di programmi antivirus, considerando che è fatto assoluto divieto agli utilizzatori di disattivarne anche solo temporaneamente le funzionalità. L'aggiornamento delle firme riconosciute deve essere a cadenza almeno semestrale (Punto 16 ALLEGATO B).

22. Tutti i programmi utilizzati per il trattamento dei dati personali devono essere aggiornati, per prevenire vulnerabilità e risolverne eventuali difetti, almeno a cadenza annuale, per i dati comuni, o semestrale per i dati sensibili e giudiziari (Punto 17 ALLEGATO B).

23. Tutte le apparecchiature di collegamento all'esterno (modem) sono vietate se non esplicitamente autorizzate. I modem presenti necessari per collegamenti remoti o amministrazione di sistema dovranno essere connessi alle linee telefoniche esterne solo per il periodo strettamente necessario e comunque il software di gestione per il collegamento dovrà consentire l'accesso solo dopo la digitazione di password.

24. Tutti i supporti di memorizzazione, già utilizzati per il trattamento di dati, possono essere riutilizzati solo previa formattazione di basso livello, o cancellazione per sovrascrizione, in modo da rendere tecnicamente irrecuperabili le informazioni in essi contenute. In caso contrario i suddetti supporti devono essere distrutti (Punto 22 ALLEGATO B).

25. I supporti cartacei, contenenti dati personali, devono essere "coriandolati" prima di essere cestinati o riciclati.

26. I dati sensibili e giudiziari devono essere protetti contro le intrusioni mediante un firewall. Qualora le circostanze lo richiedano è opportuno impiegare misure aggiuntive per la crittografia e/o la disgiunzione dei dati.