Accordo riguardante la policy per l'utilizzo dei sistemi informatici della Fondazione Bruno Kessler.

La Fondazione Bruno Kessler rappresentata Alessandro Dalla Torre, responsabile del Servizio Risorse Umane e da Marco De Rosa, responsabile del Servizio Innovazione Tecnologica e Sistemi Informativi,

e

i delegati sindacali Michele Fedrizzi (CISL), Alberto Lavelli (CGIL) e Francesco Rocca (UIL)

si sono incontrati allo scopo di sottoscrivere un accordo riguardante la policy per l'utilizzo dei sistemi informatici della Fondazione Bruno Kessler .

Premesso che:

- le risorse informatiche e telematiche messe a disposizione dalla Fondazione costituiscono uno dei punti di forza dei centri di ricerca di FBK, ma, nello stesso tempo, possono essere fonte di rischio per la sicurezza delle informazioni trattate e per l'immagine di FBK stessa;
- l'individuazione di regole precise e chiare per l'utilizzo degli strumenti informatici di FBK da parte dei dipendenti e dei collaboratori è un passaggio obbligato nel percorso che porta all'ottimizzazione del funzionamento della Fondazione;
- si conviene sull'importanza di condividere regole atte a definire i rapporti fra FBK e il personale interno ed esterno utilizzatore degli strumenti informatici messi a disposizione dalla Fondazione;
- tali regole devono contenere garanzie reciproche tra le parti, al fine di gestire le problematiche legali e gestionali che derivano dall'esercizio dell'attività e dai comportamenti inconsapevoli che possono innescare problemi o minacce alla sicurezza nel trattamento dei dati;

tutto ciò premesso

- Le parti condividono quanto riportato nell'unito allegato "policy per l'utilizzo dei sistemi informatici della Fondazione Bruno Kessler" di cui sottoscrivono il contenuto ed invitano il responsabile del Servizio Innovazione Tecnologica e Sistemi Informativi a proseguire nell'iter di formalizzazione del documento.

Letto, confermato e sottoscritto
Povo, 2 maggio 2013

I rappresentanti della Fondazione Bruno Kessler

Alessandro Dalla Torre,
responsabile del Servizio
Risorse Umane

Marco De Rosa, responsabile del Servizio
Innovazione Tecnologica e Sistemi
Informativi

FIRMATO IN ORIGINALE

I rappresentanti delle Organizzazioni sindacali:

Alberto Lavelli per la C.G.I.L.

Michele Fedrizzi er la C.I.S.L.

Francesco Rocca per la U.I.L.

POLICY PER L'UTILIZZO DEI SISTEMI INFORMATICI

Letto e approvato il 21 luglio 2008 – Modificato in data 24 maggio 2010

Versione aggiornata al 28 novembre 2011, Versione aggiornata al 17.05.2013.

Premessa

Le risorse informatiche e telematiche messe a disposizione dalla Fondazione costituiscono uno dei punti di forza dei centri di ricerca di FBK, ma, nello stesso tempo, possono essere fonte di rischio per la sicurezza delle informazioni trattate e per l'immagine di FBK stessa. Per questo motivo il loro utilizzo deve sempre ispirarsi ai comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro quali diligenza e correttezza.

L'individuazione di regole precise e chiare per l'utilizzo degli strumenti informatici di FBK da parte dei dipendenti e dei collaboratori è un passaggio obbligato nel percorso che porta all'ottimizzazione del funzionamento della Fondazione. Solo attraverso la creazione di un codice etico atto a regolare i rapporti con il personale interno e contenente garanzie reciproche tra le parti è possibile gestire le problematiche legali e gestionali che derivano dall'esercizio dell'attività e dai comportamenti inconsapevoli che possono innescare problemi o minacce alla sicurezza nel trattamento dei dati.
Sono proprio questi gli elementi che hanno ispirato la Fondazione nella stesura delle norme di comportamento conformi alle leggi ed ai principi di giustizia e garanzia dei diritti del singolo. È la comprensione delle ragioni che animano le regole di comportamento che porta al loro rispetto spontaneo.

Tali prescrizioni integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del Decreto Legislativo 196/03 e ss. mm. in materia di trattamento dei dati personali e misure minime di sicurezza e sono coordinate con quanto previsto dal Provvedimento del garante della Privacy dell'1 marzo 2007.

Tutela del Lavoratore

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati in modo da garantire, in una cornice di reciproci diritti e doveri, l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali.

Diritti alla protezione dei dati personali

Nell'impartire le seguenti prescrizioni la Fondazione Bruno Kessler tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (artt. 1 e 2, D.Lgs. 196/03 e ss. mm. – Codice in materia di protezione dei dati personali). Le prescrizioni potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica. I trattamenti rispettano le garanzie in materia di protezione dei dati e si svolgono nell'osservanza dei principi di necessità, correttezza, per finalità determinate, esplicite e legittime osservando il principio di pertinenza e non eccedenza e nella misura meno invasiva possibile.

Principio di trasparenza

In base al richiamato principio di correttezza, la Fondazione Bruno Kessler ispira le presenti policy ad un canone di trasparenza, come prevede anche la disciplina di settore (art. 4, secondo comma, Statuto dei lavoratori; D.lgs n. 81/08 e successive integrazioni e modificazioni in materia di "uso di attrezzature munite di videoterminali").

FIRMATO IN ORIGINALE

POLICY PER L'UTILIZZO DEI SISTEMI INFORMATICI

I- Premessa

I sistemi informatici affidati ai dipendenti e collaboratori sono strumenti di lavoro di proprietà della Fondazione Bruno Kessler.

II- Scopo

Lo scopo di queste policy è quello di stabilire il corretto utilizzo dei sistemi informatici in FBK. Queste regole hanno lo scopo di proteggere FBK, i suoi dipendenti e i suoi collaboratori, dal rischio di compromissione dei sistemi e dei servizi di rete, dalla divulgazione di dati personali e riservati, e dalle relative conseguenze legali, oltre che di rendere più efficace l'utilizzo dei sistemi informatici.

III- Destinatari

Destinatario di queste policy è chiunque sia titolato di un rapporto formalizzato con la Fondazione (dipendente, collaboratore, borsista, tesista, ecc.) e che abbia necessità di utilizzare qualunque sistema informatico di proprietà o in disponibilità alla Fondazione. Tali persone saranno di seguito denominate anche "utenti".
Nelle seguenti disposizioni si farà anche riferimento alle figure previste dal D.Lgs. 196/03 e ss. mm., ovvero Titolare, Responsabile ed Incaricato del trattamento dei dati personali individuati nel Documento Programmatico per la Sicurezza.

IV- Modalità operative

A - Uso degli Strumenti

1. L'utilizzo degli strumenti in dotazione è di carattere professionale. In deroga a tale principio la Fondazione Bruno Kessler autorizza un moderato e ragionevole utilizzo privato. Tale utilizzo deve essere limitato ed ispirato a criteri di buon senso e non dovrà ostacolare l'utilizzo professionale. Lo spazio della risorsa affidata utilizzato a fini "privati" (ad esempio dislocazione di file dati, foto o filmati), dovrà perciò essere limitato e non dovrà precludere e limitare quello dedicato all'utilizzo professionale.
2. Le unità di rete, ad esempio i file server, 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, su cui vengono svolte regolari attività di controllo, amministrazione e backup da parte degli Amministratori di Sistema.
3. Ai fini di tutela della privacy, l'utente dovrà creare all'interno della propria casella di posta elettronica una cartella denominata "posta personale" nella quale dovrà spostare tutti i messaggi ritenuti "privati". Tale cartella non verrà in alcun modo sottoposta a controlli da parte degli Amministratori di Rete.
4. L'accesso attraverso strumenti informatici personali, per le reti che lo prevedono (si veda il punto 1 della parte E - Implementazione), può avvenire a condizione che sia integralmente rispettato quanto previsto al successivo punto B – Conformità alle disposizioni di Legge
5. La Fondazione, all'interno delle politiche per la tutela dell'ambiente, è da sempre impegnata in programmi di risparmio energetico e il corretto utilizzo degli strumenti informatici contribuisce al raggiungimento degli obiettivi in questo senso. A tal fine gli utenti dovranno adoperarsi perché gli strumenti informatici da loro utilizzati all'interno dei locali della Fondazione siano configurati in modo conforme alle regole seguenti:
   a. i Personal Computer dovranno essere automaticamente spenti o messi in modalità di stand-by o ibernazione se non usati per più di un'ora a meno di motivate esigenze di ricerca;
   b. i monitor dovranno essere automaticamente spenti o messi in modalità di stand-by se non usati per più di 5 minuti.

B - Conformità alle disposizioni di Legge

1. L'utilizzo delle apparecchiature della Fondazione è soggetto a restrizioni derivanti dalla Legge e dalle disposizioni contenute nelle presenti policy. In particolare non è consentito utilizzare i sistemi informatici:
   a. in modo difforme da quanto previsto dalle leggi penali, civili e amministrative;

b. per scopi incompatibili con le finalità e con l'attività istituzionale di FBK;
c. per conseguire l'accesso non autorizzato a risorse di rete interne od esterne a FBK;
d. per attività che violino la riservatezza di altri utenti o di terzi;
e. per attività che influenzino negativamente la regolare operatività della rete o delle risorse (p.e., persone, capacità, elaborazione) o che ne compromettano utilizzabilità e prestazioni;
f. per attività che provochino trasferimenti non autorizzati di informazioni;
g. per attività che violino le leggi a tutela delle opere dell'ingegno;
h. in modo difforme dalla Accettable use policy della rete GARR (all. D);

e comunque in modo difforme da quanto previsto nelle presenti policy.

2. Tutte le postazioni di lavoro connesse alle reti FBK devono essere conformi alle misure di sicurezza previste dagli Artt. 31, 33 – 36 del D. Lgs 196/03 e ss. mm. (codice della privacy), e in particolare dalle misure minime previste dall'Allegato B. Si veda per questo l'appendice B

C - Gestione e protezione dei dati

1. Il backup dei principali server di rete viene effettuato dagli Amministratori di Sistema, come descritto nel Documento Programmatico sulla Sicurezza e nella Carta dei Servizi. Gli utenti che trattengono dati della Fondazione Bruno Kessler in aree per cui il DPS non prevede backup sono responsabili del salvataggio degli stessi e di eventuali danni alla Fondazione o a terzi anche di natura civilistica causati dalla loro perdita o sottrazione.
2. Fermi restando i vincoli esistenti a tutela della privacy per il proprio personale, gli utenti devono essere consapevoli che i dati da loro trattati sui sistemi informatici della Fondazione possono essere di proprietà della Fondazione o comunque sotto la responsabilità della stessa. Proprio per garantire la sicurezza e l'integrità delle informazioni presenti sui sistemi informatici di FBK, la Fondazione non può garantire in maniera assoluta, in caso di controlli, la segretezza delle informazioni.
3. L'apertura di caselle di posta, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, viene gestita con delega di FBK fornita a soggetti "Fiduciari" atti a verificare il contenuto dei messaggi e a inoltrare al Titolare del Trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. La Fondazione Bruno Kessler ha identificato come fiduciari per tutta l'organizzazione i Responsabili del Trattamento (in relazione al settore di appartenenza) e gli Amministratori di Sistema. Tale identificazione è conforme a quanto previsto dal Provvedimento del Garante della Privacy del 1 marzo 2007 in tema di utilizzo di Internet e Posta Elettronica. Ai soggetti fiduciari è fatto assoluto divieto di accedere alla casella di posta personale creata dall'utente assente.
4. Ai fini di tutela della privacy, l'utente potrà avvisare i propri destinatari della natura potenzialmente non riservata del messaggio attraverso il seguente disclaimer: "Il presente messaggio ha natura non personale ed eventuali risposte potranno essere conosciute da FBK".
5. In caso di perdita delle condizioni di incaricato al trattamento o di cessazione del rapporto con la Fondazione, valgono le seguenti regole operative:
   a. Le credenziali per l'accesso ai sistemi e alla posta elettronica vengono disattivate.
   b. La casella postale rimane attiva in ricezione per un periodo di circa 4 mesi
   c. È facoltà della Fondazione effettuare eventuali operazioni di conservazione di mail di carattere professionale di utenti non più appartenenti all'organizzazione. Le mail della "Posta personale" saranno, al contrario, cancellate.

   Tali attività sono effettuate dagli Amministratori di Sistema autorizzati alla gestione della posta elettronica, che potranno pertanto avere accesso, per esclusive ragioni di carattere tecnico e solo ove non sia evitabile, a dati personali conservati all'interno delle caselle di posta.

D - Attività di Controllo

1. Come previsto dal Provvedimento del Garante della Privacy dell'1 marzo 2007, gli Amministratori di Sistema sono incaricati dal Titolare del Trattamento a effettuare forme di controllo di carattere impersonale sulla rete e su tutti i dispositivi che la compongono. I dettagli relativi ai controlli effettuati sono disponibili nell'appendice E.
2. Al fine della corretta manutenzione dei sistemi e per garantirne la sicurezza, gli Amministratori di Sistema potranno monitorare strumenti, sistemi, traffico di rete ed in generale l'utilizzo delle risorse

in qualunque momento, anche su base periodica, ponendo la massima attenzione alla salvaguardia della privacy degli Utenti.

3. In nessun caso saranno effettuati controlli puntuali occulti. Controlli iniziali, riferibili a operazioni ritenute dannose e comunque non autorizzate, saranno riferiti solo alla totalità degli utenti. Il perdurare delle attività non consentite autorizzano la Fondazione a scendere ulteriormente nel particolare effettuando controlli al livello di gruppi omogenei. Qualora si rilevino ulteriori abusi e comportamenti che possano precludere la sicurezza dei sistemi informativi, siano lesivi del patrimonio aziendale o identifichino reati di natura penale, l'attività di controllo sarà effettuata con modalità di identificazione personale.
4. La Fondazione è tenuta comunque a denunciare all'autorità giudiziaria tutti i comportamenti contrari alla legge, anche rilevati da analisi di tipo impersonale.
5. Gli Amministratori di Sistema possono in qualunque momento procedere alla rimozione puntuale di ogni file o applicazione ritenuto pericoloso per la sicurezza, sia sulle postazioni di lavoro, sia sulle unità di rete.

E - Implementazione

1. La Fondazione mette a disposizione degli utenti diversi tipi di rete:
   a. *Trusted*, riservata ai computer di proprietà della Fondazione gestiti centralmente;
   b. *Untrusted*, riservata ai computer privati o a quelli di FBK non gestiti centralmente;
   c. *DMZ*, riservata ai server gestiti centralmente che devono offrire servizi all'esterno.
2. La prima connessione di qualsiasi apparecchiatura alle reti FBK richiede l'esplicita autorizzazione degli Amministratori di Sistema.
3. Gli Amministratori di Sistema sono gli unici ad avere accesso ai sistemi informatici gestiti collegati alle reti *trusted* e *DMZ* FBK con privilegi di Amministratore o "root", sia locale che di rete. Durante determinati periodi in cui un utente si allontana dalla Fondazione è possibile alzare i privilegi locali dello stesso sulla postazione di lavoro portatile in dotazione. Lo strumento sul quale vengono modificati i privilegi di accesso dovrà essere, senza eccezioni, inizializzato e reinstallato.
4. Per assicurare la massima flessibilità alla ricerca, è possibile, su esplicita richiesta dell'utente e su specifica autorizzazione del suo responsabile di unità, la completa delega della gestione di PC portatili di proprietà di FBK. Il PC così configurato non potrà essere collegato alle reti *trusted* FBK. L'utente, al momento della scelta di questa particolare modalità di utilizzo, dovrà sottoscrivere un documento (Appendice A) in cui viene designato Responsabile del Trattamento dei Dati con la conseguente presa in carico delle responsabilità civili e penali che la legge mette a carico di tale figura, in particolare riguardo al D. Lgs. 196/03 e ss. mm. (Codice della Privacy). Per tali soggetti responsabili viene prevista una attività propedeutica e periodica di formazione, come previsto dalle leggi vigenti, con il fine ultimo di fornire concetti di base riguardanti le misure minime di sicurezza (Appendice B) e i generali obblighi previsti dal Codice della Privacy.
5. Sulle reti *trusted* FBK e sulle postazioni di lavoro gestite centralmente, non è consentito modificare in alcun modo il sistema operativo o le applicazioni installate dagli Amministratori di Sistema.
6. Gli Utenti devono mantenere riservate le proprie password e non possono condividere gli account. Ogni utente è responsabile della sicurezza e di qualunque operazione effettuata utilizzando le proprie credenziali. È proibito accedere alla rete e ai programmi con credenziali diverse dalle proprie o in maniera anonima.
7. Le password degli Utenti devono essere cambiate almeno ogni sei mesi. Le password degli Incaricati al trattamento di dati sensibili devono essere cambiate almeno ogni tre mesi. Le password con privilegi di alto livello (root, administrator, sa, ecc.) devono essere cambiate almeno ogni tre mesi. Fanno eccezione le password che sono state preventivamente autorizzate per soli scopi di gestione tecnica il cui utilizzo assume generalmente caratteristiche di sporadicità.
8. L'accesso dall'esterno alla rete della Fondazione è consentito esclusivamente attraverso precise modalità di connessione sicura, indicate dagli Amministratori di Sistema nella Carta dei Servizi. Ogni altro accesso è espressamente vietato.
9. L'uso dei Sistemi High Performance Computing (HPC) è soggetto alle regole addizionali descritte nell'Appendice C.

V- Responsabilità

FIRMATO IN ORIGINALE

Chiunque non rispetti le presenti policy potrà essere soggetto all'immediata sospensione dell'accesso ai sistemi informatici da parte degli Amministratori di Sistema, che ne daranno comunicazione al Responsabile di riferimento. Gli Amministratori di Sistema sono inoltre obbligati ad informare della violazione il responsabile del servizio HR Business Partner, al fine di valutare l'eventuale attivazione di procedure disciplinari.
Si ricorda che le violazioni alle regole di sicurezza imposte dal D.Lgs. 196/03 e ss. mm. possono comportare ulteriori e autonome conseguenze di ordine civile e penale.

APPENDICE A
Lettera di Responsabilità al Trattamento dei Dati Personali

Oggetto: Nomina Responsabile del trattamento dei dati personali (ex art. 29 D.Lgs. 196/03)

Sig./Sig.ra _____

La Fondazione Bruno Kessler, in qualità di Titolare del trattamento dei dati ai sensi del D.Lgs. 196/03 "Codice in materia di protezione dei dati personali" (di seguito "Codice"), rilevata la Sua funzione e considerata la Sua esperienza, capacità ed affidabilità dimostrata, visto l'art. 29 del Codice, con la presente Le conferisce la nomina di

Responsabile del trattamento dei dati personali

affidandole, fino a revoca, i compiti che la legge pone a carico di questa figura.
Tale nomina si riferisce al trattamento dei dati personali contenuti negli strumenti elettronici a lei consegnati, come da lista allegata, affidandole i compiti che la legge pone a carico di questa figura, ivi compreso il profilo della sicurezza e le relative misure previste dalla legge.
Nell'ambito dell'incarico ricevuto, vorrà attenersi alle seguenti istruzioni, che vengono impartite ai sensi dell'art 29, comma quarto, del Codice:

- La raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati personali dovranno avvenire in modo da garantire il rispetto dei diritti, delle libertà fondamentali e delle dignità delle persone fisiche, con particolare riferimento alla riservatezza ed all'identità personale, nonché nel rispetto dei diritti delle persone giuridiche e di ogni altro ente o associazione;
- In particolare i dati personali devono essere:
  - trattati in modo lecito e secondo correttezza;
  - raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di trattamento in termini non incompatibili con tali scopi;
  - esatti e, se necessario, aggiornati;
  - pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
  - conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Per quanto attiene la tutela degli "interessati", ossia dei soggetti cui i dati si riferiscono, è compito del Responsabile:

- curare che la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali, nonché la persona presso la quale sono raccolti i dati personali siano previamente informati di finalità, modalità, significato del trattamento dei dati che la riguardano secondo le prescrizioni di cui all'art. 13 del Codice, nonché abbiano validamente espresso valido consenso, quando previsto, ai sensi dell'art. 23 del medesimo Codice;
- consentire agli interessati l'esercizio dei seguenti diritti che il Codice riconosce loro:
  - ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile;
  - ottenere l'indicazione:
    - dell'origine dei dati
    - delle finalità e modalità di trattamento
    - della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici
    - degli estremi identificativi del titolare e dei responsabili
    - dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati.
  - ottenere l'aggiornamento, la rettifica ovvero, qualora vi abbia interesse, l'integrazione dei dati;

FIRMATO IN ORIGINALE

- ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- ottenere l'attestazione che le operazioni descritte nei due punti precedenti sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato

Il Responsabile deve garantire, inoltre, il diritto dell'interessato ad opporsi, in tutto o in parte:
- per motivi legittimi al trattamento dei dati che lo riguardano, ancorché pertinenti alla raccolta;
- al trattamento dei dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o comunicazione commerciale.

In qualità di Responsabile, vorrà rispettare le previsioni di cui agli artt. 26 e 27 in materia di dati sensibili e giudiziari, ed onorare, comunque, le prescrizioni date dal Garante o dall'Autorità Giudiziaria in merito al trattamento dei dati personali, informando prontamente il Titolare di ogni questione rilevante ai fini della legge.

Per quanto concerne l'esigenza fondamentale di garantire la sicurezza dei dati trattati vorrà adottare le misure previste dall'Allegato B del Codice onde evitare che i dati non vengano dispersi o distrutti e, soprattutto, che agli stessi non possano accedere persone diverse da quelle autorizzate o che, anche da parte del personale autorizzato all'accesso, non ne venga fatto un trattamento non consentito o difforme rispetto alle finalità della raccolta.
Vorrà, ad ogni modo, garantire che venga conservato e, in ogni caso, non abbassato l'attuale standard di sicurezza in relazione alle finalità sopra indicate.

La società, quale Titolare del trattamento, è a disposizione per fornire ogni ulteriore informazione, istruzione, documentazione e supporto utile per l'adempimento dei compiti sopra specificati.
Si rappresenta, inoltre, che, ai sensi dell'art. 29 del Codice, il Titolare ha il dovere di vigilare, anche attraverso verifiche periodiche, affinché i responsabili nominati osservino le istruzioni impartite, salve le norme poste a tutela della dignità del lavoratore.
La firma della presente comporta accettazione dell'incarico nonché presa visione e conoscenza delle istruzioni impartite (Policy per l'utilizzo dei sistemi informatici - punto IV modalità operative - lettera E implementazione - punto n. 4).

Trento, lì _____

Num. Inv. _____

Il Titolare del trattamento

Il Responsabile del Trattamento

_____

Il Responsabile di Unità/Direttore

_____

Appendice B
Misure di Sicurezza previste dal "Codice della Privacy" (Decreto legislativo 30 giugno 2003, n. 196)

Art. 31. Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 33. Misure minime

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34. Trattamenti con strumenti elettronici

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g) [soppressa] (1);

h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

1-bis. [abrogato] (2)

1-ter. Ai fini dell'applicazione delle disposizioni in materia di protezione dei dati personali, i trattamenti effettuati per finalità amministrativo-contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro. (3)

Art. 35. Trattamenti senza l'ausilio di strumenti elettronici

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

(1) Lettera soppressa dall'art. 45, comma 1, lett. c), del decreto legge 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35. Si riporta, per completezza, il testo originale: "tenuta di un aggiornato documento programmatico sulla sicurezza".
(2) Comma aggiunto dall'art. 6, comma 2, lett. a), numero 5), del decreto legge 13 maggio 2011, n. 70, convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106 (in sostituzione del precedente comma 1-bis aggiunto dall'art. 29, comma 1, del decreto legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133), e successivamente abrogato dall'art. 45, comma 1, lett. c), del decreto legge 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35.
(3) Comma aggiunto dall'art. 6, comma 2, lett. a), numero 5), del decreto legge 13 maggio 2011, n. 70, convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106, in sostituzione del precedente comma 1-bis aggiunto dall'art. 29, comma 1, del decreto legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133.

Allegato B del D. Lgs. 196/03
(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] (1)

19.1. [soppresso](1)
19.2. [soppresso](1)
19.3. [soppresso](1)
19.4. [soppresso](1)
19.5. [soppresso](1)
19.6. [soppresso](1)
19.7. [soppresso](1)
19.8. [soppresso](1)

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] (1)

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.

(1) Paragrafi soppressi dall'art. 45, comma 1, lett. d), del decreto legge 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35.

Per completezza, si riporta di seguito il testo dei paragrafi soppressi.

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
19.3. l'analisi dei rischi che incombono sui dati;
19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonchè in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Nota: La fondazione ha deciso di mantenere il Documento Programmatico sulla Sicurezza, nonostante la sua formale abrogazione da parte della legge 4 aprile 2012 n. 45, tenuto conto che in esso si elencano le misure di sicurezza adottate ai sensi degli articoli di legge indicati nella presente appendice.

FIRMATO IN ORIGINALE

Appendice C
Regole addizionali per l'uso dei Sistemi HPC

I – Utenti dei Sistemi HPC

1. Tutte le unità operative di ricerca che hanno contribuito alla realizzazione dei sistemi HPC possono utilizzarli senza costi aggiuntivi. Gli utenti delle suddette unità possono richiedere l'accesso o il supporto scrivendo a gsc@fbk.eu.
2. I responsabili delle suddette unità operative faranno parte di un tavolo chiamato "Cluster-Strategic". Questo tavolo prenderà decisioni strategiche a proposito dei Sistemi HPC.
3. I responsabili delle suddette unità operative eleggeranno uno o più utenti di un secondo tavolo chiamato "Cluster-Technical". Questo tavolo prenderà decisioni tecniche a proposito dei Sistemi HPC.
4. Tutte le altre richieste dovranno essere indirizzate a Cluster-Strategic.

II – Utilizzo dei Sistemi HPC

1. Gli utenti devono utilizzare Secure Shell (ssh) per collegarsi ai Sistemi HPC e Secure Copy Protocol (SCP) per traferire file all'interno o all'esterno dei Sistemi HPC. I sistemi non accetteranno connessioni da altri protocolli. Dall'interno dei sistemi HPC, per motivi di sicurezza, non saranno consentite connessioni verso l'esterno.
2. I computer che accettano connessioni ssh, chiamati "Logon Server", agiranno come dei front-end. Potranno essere usati per editing, compiling/debugging di piccole applicazioni e per la preparazione e la sottomissione di esecuzioni batch.
3. Non è consentita l'esecuzione di programmi che utilizzano pesantemente la CPU dei logon server. Gli applicativi di questo tipo (targz, compile e debug sessions, ect.) devono essere eseguiti attraverso il sistema di code.
4. Il trasferimento dei dati da e verso i Sistemi HPC sarà possibile utilizzando SCP da file server esterni verso file server interni.
5. Tutti i job devono essere eseguiti attraverso il sistema di code. Saranno disponibili diversi tipi di code per diversi scopi.
6. Non sarà possibile connettersi direttamente ai nodi di calcolo dai Logon Server: sessioni interattive su nodi specifici potranno essere effettuate attraverso il sistema di code.
7. Il debug dovrà essere eseguito su una coda.
8. Ogni nodo ha un disco che potrà essere usato come scratch locale per memorizzare file temporanei durante l'esecuzione di job. Le dimensioni dello spazio variano da nodo a nodo. I dati memorizzati in questo spazio non saranno visibili dagli altri nodi o dai logon server. Gli utenti sono incoraggiati a copiare i propri dati dai file server sullo scratch locale e a riportarli indietro alla fine del job. **Tutti i dati più vecchi di una settimana, presenti nelle aree di scratch, saranno cancellati dopo un avvertimento.**

III – Allocazione delle risorse dei Sistemi HPC

1. Normalmente i nodi sono utilizzati in modalità condivisa. Gli utenti con la necessità di utilizzare nodi in modo esclusivo per un lungo periodo di tempo dovranno effettuare una prenotazione specificando sul calendario condiviso il tempo e il numero stimato. Ogni unità potrà prenotare in modo esclusivo una quantità limitata di nodi. Questi saranno riservati al più presto possibile a partire dalla data richiesta.
2. Al momento della sottomissione dei job l'utente dovrà specificare l'utilizzo massimo di RAM. Un GByte di RAM dovrà essere riservato per il sistema operativo. Tutti i job che eccedono i suddetti limiti saranno terminati.
3. È consigliato l'uso di job checkpointed.
4. Le quote di spazio disco sui file server sono gestite a livello di Unità. Ogni Unità potrà avere riservate diverse quantità di spazio.
5. Le unità che hanno necessità di job con particolari caratteristiche potranno farne richiesta a Cluster-Technical.

IV – Job monitoring

1. Il sistema avvertirà gli utenti quando un loro job è:
    a. terminato (specificando il motivo);
    b. sospeso (specificando il motivo);
    c. ripreso;

d. in esecuzione da lungo tempo.

2. Il sistema può essere configurato dagli utenti per ricevere anche i seguenti avvertimenti:
    a. Job partito
    b. Job finite

FIRMATO IN ORIGINALE

Appendice D
Acceptable Use Policy della rete GARR

1. La Rete Italiana dell'Università e della Ricerca, denominata comunemente "Rete GARR", si fonda su progetti di collaborazione di ricerca ed accademica tra le Università, le Scuole e gli Enti di Ricerca pubblici italiani. Di conseguenza il servizio di Rete GARR è destinato principalmente alla comunità che afferisce al Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR). Esiste tuttavia la possibilità di estensione del servizio stesso anche ad altre realtà, quali quelle afferenti ad altri Ministeri che abbiano una Convenzione specifica con il Consortium GARR, oppure realtà che svolgono attività di ricerca in Italia, specialmente, ma non esclusivamente, in caso di organismi "no-profit" impegnati in collaborazioni con la comunità afferente al MIUR. L'utilizzo della Rete è comunque soggetto al rispetto delle Acceptable Use Policy (AUP) da parte di tutti gli utenti GARR.
2. Il "Servizio di Rete GARR", definito brevemente in seguito come "Rete GARR", è costituito dall'insieme dei servizi di collegamento telematico, dei servizi di gestione della rete, dei servizi applicativi e di tutti quelli strumenti di interoperabilità (operati direttamente o per conto del Consortium GARR) che permettono ai soggetti autorizzati ad accedere alla Rete di comunicare tra di loro (Rete GARR nazionale). Costituiscono parte integrante della Rete GARR anche i collegamenti e servizi telematici che permettono la interconnessione tra la Rete GARR nazionale e le altre reti.
3. Sulla rete GARR non sono ammesse le seguenti attività:
   - fornire a soggetti non autorizzati all'accesso alla Rete GARR il servizio di connettività di rete o altri servizi che la includono, quali la fornitura di servizi di housing, di hosting e simili, nonchè permettere il transito di dati e/o informazioni sulla Rete GARR tra due soggetti entrambi non autorizzati all'accesso sulla Rete GARR (third party routing);
   - utilizzare servizi o risorse di Rete, collegare apparecchiature o servizi o software alla Rete, diffondere virus, hoaxes o altri programmi in un modo che danneggi, molesti o perturbi le attività di altre persone, utenti o i servizi disponibili sulla Rete GARR e su quelle ad essa collegate;
   - creare o trasmettere (se non per scopi di ricerca o comunque propriamente in modo controllato e legale) qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno, indecente, o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza o il credo;
   - trasmettere materiale commerciale e/o pubblicitario non richiesto ("spamming"), nonché permettere che le proprie risorse siano utilizzate da terzi per questa attività;
   - danneggiare, distruggere, cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di parole di accesso (password), chiavi crittografiche riservate e ogni altro "dato personale" come definito dalle leggi sulla protezione della privacy;
   - svolgere sulla Rete GARR ogni altra attività vietata dalla Legge dello Stato, dalla normativa Internazionale, nonchè dai regolamenti e dalle consuetudini ("Netiquette") di utilizzo delle reti e dei servizi di Rete cui si fa accesso.
4. La responsabilità del contenuto dei materiali prodotti e diffusi attraverso la Rete è delle persone che li producono e diffondono. Nel caso di persone che non hanno raggiunto la maggiore età, la responsabilità può coinvolgere anche le persone che la legge indica come tutori dell'attività dei minori.
5. I soggetti autorizzati (S.A.) all'accesso alla Rete GARR, definiti nel documento "Regole di accesso alla Rete GARR", possono utilizzare la Rete per tutte le proprie attività istituzionali. Si intendono come attività istituzionali tutte quelle inerenti allo svolgimento dei compiti previsti dallo statuto di un soggetto autorizzato, comprese le attività all'interno di convenzioni o accordi approvati dai rispettivi organi competenti, purchè l'utilizzo sia a fini istituzionali. Rientrano in particolare nelle attività istituzionali, la attività di ricerca, la didattica, le funzioni amministrative dei soggetti e tra i soggetti autorizzati all'accesso e le attività di ricerca per conto terzi, con esclusione di tutti i casi esplicitamente non ammessi dal presente documento.
   Altri soggetti, autorizzati ad un accesso temporaneo alla Rete (S.A.T.) potranno svolgere solo l'insieme delle attività indicate nell'autorizzazione.
   Il giudizio finale sulla ammissibilità di una attività sulla Rete GARR resta prerogativa degli Organismi Direttivi del Consortium GARR.
6. Tutti gli utenti a cui vengono forniti accessi alla Rete GARR devono essere riconosciuti ed identificabili. Devono perciò essere attuate tutte le misure che impediscano l'accesso a utenti non identificati. Di norma

gli utenti devono essere dipendenti del soggetto autorizzato, anche temporaneamente, all'accesso alla Rete GARR.

Per quanto riguarda i soggetti autorizzati all'accesso alla Rete GARR (S.A.) gli utenti possono essere anche persone temporaneamente autorizzate da questi in virtù di un rapporto di lavoro a fini istituzionali. Sono utenti ammessi gli studenti regolarmente iscritti ad un corso presso un soggetto autorizzato con accesso alla Rete GARR.

7. È responsabilità dei soggetti autorizzati all'accesso, anche temporaneo, alla Rete GARR di adottare tutte le azioni ragionevoli per assicurare la conformità delle proprie norme con quelle qui esposte e per assicurare che non avvengano utilizzi non ammessi della Rete GARR. Ogni soggetto con accesso alla Rete GARR deve inoltre portare a conoscenza dei propri utenti (con i mezzi che riterrà opportuni) le norme contenute in questo documento.
8. I soggetti autorizzati all'accesso, anche temporaneo, alla Rete GARR accettano esplicitamente che i loro nominativi (nome dell'Ente, Ragione Sociale o equivalente) vengano inseriti in un annuario elettronico mantenuto a cura degli Organismi Direttivi del Consortium GARR.
9. In caso di accertata inosservanza di queste norme di utilizzo della Rete, gli Organismi Direttivi del Consortium GARR prenderanno le opportune misure, necessarie al ripristino del corretto funzionamento della Rete, compresa la sospensione temporanea o definitiva dell'accesso alla Rete GARR stessa.
10. L'accesso alla Rete GARR è condizionato all'accettazione integrale delle norme contenute in questo documento.

FIRMATO IN ORIGINALE

Appendice E
Dettagli relativi alle attività di controllo svolte dagli Amministratori di Sistema

La Fondazione gestisce i sistemi informatici e le reti anche attraverso strumenti che possono memorizzare temporaneamente dati relativi alla navigazione internet e al traffico telematico. In particolare si elencano:

1. Posta Elettronica – corretto funzionamento del sistema di consegna dei messaggi e controlli di sicurezza anti-malware e antispam – dati conservati:
    a. log del traffico SMTP generato dai server di posta elettronica;
    b. log dei messaggi non correttamente inoltrati (ritardi e/o mancate consegne);
    c. log dei messaggi intercettati dal sistema antispam;
    d. log dei messaggi intercettati dal sistema antivirus e sottoposti a quarantena di 30 giorni.
2. Traffico WEB – corretto funzionamento del sistema, monitoraggio SLA, controlli di sicurezza:
    a. Log del traffico http/https generato sui dispositivi firewall. Tale log comprende anche dati puntuali di navigazione riferibili all'indirizzo IP interno di provenienza della richiesta. I dati sono conservati per circa 26 settimane in un sistema accessibile solo dagli amministratori di sistema autorizzati, e non utilizzato normalmente per altre attività della Fondazione. Tuttavia potranno essere conservati per tempi superiori per giustificate ragioni tecnico/organizzative, per garantire l'esercizio o la difesa di un diritto in sede giudiziarie e in tutti i casi in cui sia richiesto dall'autorità giudiziaria.
3. Telefonia – corretto funzionamento del sistema:
    a. Log delle chiamate (numero chiamante, numero chiamato, durata).
4. Accesso alle reti- corretto funzionamento del sistema, monitoraggio SLA e controlli di sicurezza:
    a. Log di accesso alle reti dall'esterno.

La Fondazione adotta procedure di backup che proteggono da possibili perdite di dati. Allo stato attuale le copie di backup possono contenere:

dati della cartella "Posta Personale" eventualmente creata dall'utente, fatte salve le garanzie descritte nel paragrafo C - Gestione e protezione dei dati.

Le copie attualmente conservate permettono di risalire ai dati conservati sui sistemi FBK negli ultimi 5 anni.

Come indicato nelle Linee Guida del Garante per posta elettronica e internet, la Fondazione non procederà in nessun caso a controlli non consentiti, quali:

lettura e registrazione puntuale di messaggi di posta;
riproduzione e memorizzazione delle pagine internet visitate;
cattura dei caratteri digitati attraverso tastiera (fisica o virtuale);
analisi occulta dei pc affidati in uso.