Istituto Nazionale di Fisica Nucleare

CCR-01/06/P
30 gennaio 2006
Versione 2.7

S. Arezzini, E. Bovo, R. Cecchini, P. Lo Re, M. Morandin, O. Pinazza, A. Spanu

Note per l'attuazione delle misure antiterrorismo
(Decreto Interministeriale 16 agosto 2005)

1. Considerazioni preliminari

Questo documento contiene le norme pratiche di attuazione degli obblighi previsti dal Decreto del Ministero dell'Interno del 16 agosto 2005, "Misure per il contrasto del terrorismo internazionale", come indicate nella Circolare dell'Amministrazione Centrale e del Servizio Affari Legali e Contenzioso del 2/12/05.

Il Decreto Interministeriale, pensato principalmente per "titolari o gestori di esercizio pubblico o circolo privato", prescrive alcuni obblighi che interessano anche l'INFN in quanto:

a) "fornitore di apparecchi terminali utilizzabili per le comunicazioni telematiche (…) a frequentatori" (art. 3);
b) "soggetto che offre accesso alle reti telematiche utilizzando tecnologie senza fili in aree messe a disposizione del pubblico (art. 4)".

Nel caso a) sono considerati **frequentatori** coloro i quali, pur non essendo dipendenti o associati, in modo più o meno occasionale, hanno accesso alle sedi e possono utilizzare apparecchi terminali per la connessione ad Internet (ad esempio laureandi, studenti, ospiti).

L'art. 3 richiede che l'INFN metta in atto misure idonee a:

- impedire l'accesso ai terminali a soggetti non previamente identificati;
- identificare chi accede mediante acquisizione di dati anagrafici e copia del documento di identità;
- informare il pubblico delle condizioni d'uso;
- rendere disponibili i dati acquisiti alla polizia postale, giudiziaria o all'Autorità Giudiziaria (solo quando queste autorità lo richiedano);
- assicurare il trattamento e la conservazione dei dati fino al 31/12/2007.

Nel caso b) il decreto richiede che siano identificabili gli utilizzatori delle reti wireless in aree messe a disposizione del pubblico. In particolare, si dovrà prestare particolare attenzione alle reti che si estendono in strade, piazze, giardini pubblici, aree universitarie, e alle reti wireless attivate in occasione di convegni, eventi e altre manifestazioni di formazione e promozione scientifica.

Per questi casi, il Decreto specifica che è necessario:

- impedire l'uso di terminali che non consentano l'identificazione dell'utente;
- impedire l'accesso ad utenti che non siano preventivamente identificati.

Anche per l'INFN risulta quindi necessario identificare i soggetti ai quali è consentito l'accesso wireless alla rete. Non è previsto invece il monitoraggio delle attività (art. 2).

2. Misure da realizzare

Nel caso di **frequentatori** devono essere richiesti i seguenti dati identificativi:

1. nome, cognome, data e luogo di nascita (i dati presenti sul documento di identità);
2. estremi del documento di identità;
3. documento di identità (digitalizzato);
4. data di attivazione

Questi dati saranno conservati e trattati secondo le norme previste in materia di tutela dei dati personali. Sono raccolti secondo disposizioni di legge e per fini istituzionali dell'Ente e quindi non è richiesto il consenso dell'utente, che però è opportuno riceva un'informativa, di cui si allega un esempio.

Nel caso di convegni organizzati dell'INFN è importante che il comitato organizzatore si premuri di predisporre il servizio di identificazione degli ospiti.

I dati di cui sopra saranno conservati nel sistema documentale dell'INFN, già predisposto per la gestione di dati sensibili. In questo modo si eviteranno identificazioni multiple di una stessa persona e gli oneri della gestione di un ulteriore database di dati personali per ogni Struttura. Tuttavia, non avendo la certezza che la predisposizione del sistema documentale possa essere effettuata in tempi brevi, ogni sede dovrà per il momento curare l'archiviazione in modo autonomo.

Si ritiene inoltre opportuno che queste informazioni, per la loro natura e le conseguenti misure di sicurezza da adottare, siano gestite dal personale incaricato per il trattamento di dati personali appartenente agli uffici amministrativi preposti.

Il Decreto non disciplina il caso di dipendenti ed associati, per i quali l'identificazione è già stata fatta dagli uffici appositi e che sono già responsabili per l'uso delle risorse messe loro a disposizione per motivi di lavoro, incluso l'accesso ad Internet.

Nel caso di macchine non gestite dal Servizio Calcolo, i responsabili non devono fornire accesso a terzi (ad esempio tramite l'apertura di account) senza l'esplicita autorizzazione del Servizio Calcolo e, nel caso di frequentatori, sono comunque tenuti a verificarne l'avvenuta preventiva identificazione.

È indispensabile restringere l'accesso wireless ai soli utenti autenticati con metodologie basate su algoritmi crittografici "forti", ad es. WPA 1.0 con chiavi di almeno 25 caratteri, rimuovendo quindi accessi liberi, che non richiedono alcuna autorizzazione, e, per quanto possibile, forme di restrizione basate sul solo indirizzo hardware (mac-address) del client.

Si allega un documento con le condizioni d'uso delle risorse informatiche dell'INFN, da consegnare ai frequentatori, come richiesto dal Decreto.

3. Ulteriori misure

Il paragrafo precedente contiene gli adempimenti minimi richiesti dal Decreto. Riteniamo però indispensabile, alla luce di passate esperienze e per aumentare la sicurezza delle Strutture, conservare le seguenti altre informazioni, molte delle quali vengono sicuramente già salvate, in modo poter ricostruire i dettagli di eventuali incidenti:

- log degli MTA;
- log dei server DHCP;
- log di gateway VPN;
- log di modem/RAS;
- file di configurazione dei server DHCP;
- file di configurazione del server DNS (con le informazioni che permettano di risalire all'utente),
- log dei server utilizzati per l'accesso wireless (ad es. RADIUS).

Tutte le macchine di cui si conservano i log devono essere sincronizzate ad un *time server* (un **ntpdate** lanciato ogni ora via **cron** è più che sufficiente).

I file di log, in linea di massima, vanno ruotati ogni giorno.

I dati vanno salvati periodicamente (la periodicità è ovviamente funzione del volume dei dati) su supporti ottici non riscrivibili, da conservare fino al 31/12/2007 in un contenitore chiuso a chiave.

Allegato n. 1

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'art. 13 del Decreto Legislativo 30 giugno 2003 n. 196 si informa che l'Istituto Nazionale di Fisica Nucleare effettua il trattamento dei dati personali esclusivamente in adempimento di norme di legge e di regolamento ed in relazione al raggiungimento dei propri fini istituzionali. In particolare, l'acquisizione dei dati diretta alla concessione di credenziali di accesso per le comunicazioni telematiche, è effettuata in relazione a quanto disposto dalla disciplina in materia di contrasto al terrorismo internazionale.

Modalità del trattamento

I dati personali sono trattati in modo lecito e secondo correttezza, anche con strumenti automatizzati e per il solo tempo necessario a conseguire gli scopi per cui sono stati raccolti. Il trattamento avviene nel rispetto dell'art. 11 ed in considerazione dell'art. 100 del D.Lgs.n.196/03.

Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

Il titolare ed i responsabili del trattamento

Il titolare del trattamento dei dati personali è l'Istituto Nazionale di Fisica Nucleare con sede in Frascati, Roma (Italia), via E. Fermi, 40.

Responsabili del trattamento sono i soggetti individuati con Deliberazione del Consiglio Direttivo dell'INFN n. 8335/03 ed in particolare i Direttori delle Strutture INFN presso i quali vengono conferiti i dati personali.

Facoltatività del conferimento dei dati

L'utente è libero di fornire i propri dati personali. Si informa, tuttavia, che il loro mancato conferimento comporterà l'impossibilità di raggiungere le finalità cui il trattamento è connesso.

Diritti degli interessati

Ai soggetti cui si riferiscono i dati personali è garantito l'esercizio dei diritti di cui all'art. 7 del D.Lgs. n.196/03, nel rispetto della disciplina dettata per il contrasto al terrorismo internazionale.

Le eventuali istanze per l'esercizio dei diritti di cui sopra vanno rivolte al titolare del trattamento.

Allegato n. 2

CONDIZIONI D'USO DELLE RISORSE INFORMATICHE DELL'INFN

Uso delle risorse di calcolo e dei servizi di rete

Le risorse di calcolo ed i servizi di rete dell'INFN sono risorse essenziali, che l'Ente mette a disposizione esclusivamente per il conseguimento delle proprie finalità istituzionali di ricerca scientifica e tecnologica. Il contributo di tutti gli utenti autorizzati a servirsene è essenziale affinché ne venga preservata la integrità e garantito il buon funzionamento.

È pertanto vietato l'utilizzo di tale risorse finalizzato a:

- attività contrarie alla legge o proibite dai regolamenti;
- attività commerciali non autorizzate;
- attività comunque idonee a compromettere la sicurezza delle risorse di calcolo dell'Ente o dirette a cagionare danno a terzi;
- attività comunque non conformi agli scopi dell'Ente.

L'INFN promuove atteggiamento collaborativo degli utenti e raccomanda il rispetto di civili consuetudini di comportamento e della "netiquette" (http://www.rfc-editor.org/rfc/rfc1855.txt).

Accesso alle risorse di calcolo e ai servizi di rete

L'accesso alle risorse di calcolo ed ai servizi di rete dell'INFN è consentito ai dipendenti, agli associati, nonché ai collaboratori, ospiti, dottorandi, specializzandi, assegnisti, borsisti e laureandi autorizzati dai relativi responsabili.

L'accesso alle risorse di calcolo che consentono la connessione ad Internet è consentito soltanto previa identificazione degli utenti. Gli utenti le cui generalità non siano già state formalmente accertate in relazione alla stipula di un contratto di lavoro o collaborazione, o all'assegnazione di incarico di associazione, borsa di studio o assegno di ricerca, sono identificati mediante riproduzione di copia del documento di identità ed acquisizione dei dati ivi riportati.

L'accesso è personale, non può essere condiviso o ceduto ed è consentito a ciascun utente soltanto in conformità alle norme del presente regolamento. Non è permesso fornire accesso a terzi senza previa autorizzazione del Servizio Calcolo e Reti.

Al fine di garantire la sicurezza delle risorse di calcolo è vietato:

- accedere senza autorizzazione ai locali dei Servizio di Calcolo e Reti dell'INFN, nonché ai locali ed alle aree riservate alle apparecchiature di rete;
- connettere risorse di calcolo alla rete locale senza l'autorizzazione del competente Servizio di Calcolo e Reti INFN;
- cablare, collegare o modificare apparati di rete senza l'autorizzazione del competente Servizio di Calcolo e Reti INFN;
- utilizzare indirizzi di rete e nomi non espressamente assegnati all'utente;
- installare modem configurati per l'accesso remoto dall'esterno delle Strutture INFN in assenza di preventiva autorizzazione del Direttore di Struttura;
- divulgare informazioni sulla struttura e configurazione delle risorse informatiche, con particolare

riferimento all'ubicazione degli apparati wireless, ai numeri telefonici e alle password dei modem gestiti dal Servizio di Calcolo e Reti INFN;
- intraprendere ogni altra azione diretta a degradare le risorse del sistema, impedire agli utenti autorizzati l'accesso alle risorse, ottenere risorse superiori a quelle già allocate ed autorizzate, accedere alle risorse di calcolo violandone le misure di sicurezza.

Norme di comportamento degli utenti

Gli utenti:

- sono tenuti ad agire in conformità alla legge e nel rispetto delle politiche dell'Ente in materia di sicurezza, garantendo la riservatezza nel trattamento dei dati personali anche mediante la puntuale osservanza delle Norme di condotta dettate dall'INFN in materia di trattamento dei dati personali;
- sono responsabili del software che installano sui computer loro affidati: procedono ad un'attenta valutazione preliminare del software da installare e non installano software privi delle regolari licenze;
- sono tenuti a proteggere da accessi non autorizzati i dati utilizzati e/o memorizzati nei propri computer e nei sistemi cui hanno accesso;
- sono tenuti a seguire le indicazioni fornite dal Servizio di Calcolo e Reti per il salvataggio periodico dei dati utilizzati e/o memorizzati;
- sono tenuti a proteggere il proprio account mediante password variate periodicamente e non banali;
- non devono utilizzare la stessa password su sistemi diversi, né diffonderla o comunicarla, ovvero concedere ad altri l'uso del proprio account;
- sono tenuti a segnalare immediatamente al Servizio di Calcolo e Reti incidenti, sospetti abusi e violazioni della sicurezza;
- per i sistemi operativi che lo prevedono, sono tenuti ad utilizzare programmi antivirus aggiornati, avendo cura di sottoporre a scansione i file scambiati via rete e i supporti rimovibili utilizzati;
- non devono mantenere connessioni remote inutilizzate né lasciare la postazione di lavoro con connessioni aperte non protette.

Violazione delle norme

Ogni condotta contraria a norme di legge o posta in essere in violazione di quanto indicato nel presente documento determinerà la sospensione dell'accesso alle risorse informatiche, previa informazione del Direttore di Struttura, oltre a produrre eventuali conseguenze civili e penali.

Allegato n. 3

INFORMATION ABOUT THE TREATMENT OF PERSONAL DATA

Under Article 13 of the Legislative Decree of 30th June 2003 no. 196, it is noted that the National Institute of Nuclear Physics (INFN) will treat personal data exclusively in execution of the norms of law and regulations and relative to pursuing the specific aims of the institution itself. In particular, the acquisition of data required to grant access to telecommunication services, is performed as provided for by the law as a response to international terrorism.

Conditions of Data Treatment

Personal data will be treated legally and fairly, including the use of automatic tools and only for the time necessary to complete the goals for which the data is being collected. Treatment comes under Article 11 and with consideration of Article 100 of the D.Lgs. 196/03.

Specific security measures are observed to prevent the loss of data, illicit or unfair use and non-authorised access.

The principals and those responsible for data treatment

The principal of personal data treatment is the National Institute of Nuclear Physics, which has its head office in Frascati, Rome (Italy), via E. Fermi, 40.

Those responsible for data treatment are the persons selected with Deliberation of the Directive Council of the INFN no. 8335/03 and in particular the Directors of INFN Centres where the personal data is collected.

The giving of data is non-obligatory

The user is free to supply his own personal data. It is to be noted, however, that the absence of data will make it impossible to achieve the goals related to the treatment of data.

Rights of the parties

The subjects to whom the data refers to are guaranteed the exercise of their rights as specified by the Article 7 of the D.Lgs. no. 196/03, in accordance with the aforementioned rules against international terrorism.

Applications aimed at exercising these rights must be addressed to the principal of the treatment.

Allegato n. 4

CONDITIONS OF USE FOR INFN'S COMPUTING RESOURCES

Use of computing resources and network services

The computing resources and and network services of INFN represent very important resources that INFN makes available exclusively to achieve its institutional scientific and technological research goals. The cooperation of those authorised to use them is essential for preserving their integrity and for guaranteeing their performance.

The following is forbidden:

- Activities contrary to the law or prohibited by regulations;
- Unauthorized commercial activities;
- Any activity which compromises the security of the data resources of the Organisation or intended to cause damage to third parties;
- Any activity not related to the goals of the Organisation.

Access to data resources and network services

Access to the data resources and network services of INFN is permitted to employees, associates, as well as partners, guests, research students, undergraduate students, PhD students and grant holders authorised by their supervisors.

Access to the computing resources that provides Internet connection is allowed only through user identification. Users who have not been formally identified as a consequence of their position as INFN employees, or affiliated to INFN as holder of associates status, INFN research grant or post-doc contract, are identified by presenting a copy of a document of identity and registration of date reported therein.

Access is personal, cannot be shared or passed on and is permitted to each user solely in respect of the provisions of these regulations. Providing access to a third party is forbidden without prior authorisation from the local Computing Service.

In order to guarantee the security of the data resources, the following is forbidden:

- Unauthorised access to the computing rooms, as well as to reserved places and areas where network equipment is located;
- To connect computing resources to the local network without proper authorisation from the local INFN Computing and Network Service;
- To wire, connect or modify network apparatus without the relevant authorisation from the local INFN Computing and Network Service;
- To use network addresses and names other than those explicitly assigned to the user;
- To install modems configured for remote access without preventive authorisation from the Director of center;
- To divulge information about the structure and configuration of IT resources, particularly for what

concerns the location of wireless equipment, telephone numbers and the passwords of modems managed by the local INFN Computing and Network Service;

- To undertake any other direct action intended to degrade the system's resources, to prevent authorised users from accessing resources, to obtain superior resources to those already allocated and authorised, to access the data resources in violation of security measures.

Behavioural rules for users

Users:

- Are bound to act in conformity with the law and in respect of the policies of the Organisation on subjects of security, guaranteeing the confidentiality of the treatment of personal data, also through the strict observance of the rules of conduct laid down by the INFN on the treatment of personal data;
- Are responsible for software packages that are installed on computers by those whom they allow access: originating with a detailed preliminary evaluation of software to be installed that does not have a regular license;
- Are bound to protect from unauthorised access the data used and/or stored in the computer and in the system to which they have access;
- Are bound to follow the instructions provided by the local INFN Computing and Network Service for regularly backing up their data;
- Are bound to protect their own account by choosing a sufficiently complex password and changing it periodically;
- Must not use the same password on different systems, nor communicate it or pass it on, nor give others the use of their account;
- Are bound to immediately inform the local INFN Computing and Network Service of any incident, suspected abuse or violation of security;
- Are bound, for the operating systems which they foresee using, to use updated antivirus programs, taking care to scan files that have been exchanged on the network and any removable storing media;
- Must not maintain unused remote connections nor leave the work station with unprotected open connections.

Violation of the rules

Any conduct contrary to legal norms or in violation of the rules set out in this document will result in the suspension of access to IT resources, following the communication of the the Director of the INFN center, and may have civil and penal consequences.