Procedura di Accreditamento degli utenti sul sistema IdeA dell'Istituto di Fisiologia Clinica del CNR

R. Conte

20.1.2010

1. Revisioni

Rev.	Data	Autore
1.0	20.01.2010	R. Conte

Introduzione

L'istituto di Fisiologia Clinica (in seguito IFC), in funzione della sensibilità dei dati trattati, ha dedicato grande attenzione al sistema di accesso agli stessi dedicando particolare attenzione alle modalità ed alle diverse figure che vi possono accedere. Nel corso del tempo però l'intera attività dell'Istituto ha subito pesanti modifiche in seguito alla nascita della Fondazione CNR/ Regione Toscana "G. Monasterio" che ha preso in carico l'attività clinico-assistenziale. Di conseguenza anche la stessa procedura di accreditamento degli utenti ha subito diverse variazioni. Il presente documento ha quindi l'obiettivo di descrivere le procedure attualmente in atto per rilasciare un account per l'utilizzo dei servizi di rete ed al tempo stesso definire quella che saranno la procedura e le regole a regime.

1. Descrizione del sistema

Il sistema di gestione delle identità digitali (Identity Management System) è denominato **IdeA** (Identity and Authentication System). Il sistema si compone di tre macchine utilizzate per ospitare un server LDAP master e due repliche. Il server master è utilizzato esclusivamente per le operazioni di modifica dei dati mentre le repliche vengono utilizzate per la consultazione e l'autenticazione.
Al sistema si aggiunge un server sul quale, tramite il software Shibboleth, si implementa un Identity Provider utilizzato per l'autenticazione ed il Single Sign-On per l'utilizzo di risorse disponibili via World Wide Web, siano esse locali o remote, in quest'ultimo caso rese disponibili dalla Federazione IDEM.

2. Procedure e responsabilità dell'accreditamento utenti

L'accreditamento degli utenti viene gestito dall'Ufficio del Personale. È infatti questo ufficio ad essere autoritativo relativamente alle informazioni sul personale stesso afferente, nelle diverse forme, all'IFC. La procedura prevede che un account venga rilasciato successivamente all'espletamento delle operazioni di seguito descritte:

- l'utente sottoscrive il "Modulo di assunzione di responsabilità individuale nell'utilizzo dei servizi informatici" (all. A, MS001, ***attualmente in corso di aggiornamento***), disponibile sul sito Intranet d'Istituto e per il quale non è necessaria autenticazione se il sito stesso è raggiunto da rete locale. Il modulo è anche disponibile direttamente presso l'Ufficio del Personale;
- il modulo MS001, firmato e datato viene consegnato, personalmente, all'Ufficio del Personale contestualmente alla documentazione necessaria per la formalizzazione del rapporto con IFC (modulo copertura assicurativa, contratto ecc.);

- l'account dell'utente, con i relativi attributi viene creato sul sistema IdeA; la password assegnata all'account viene generata automaticamente ed è composta da 8 cifre alfanumeriche casuali;
- all'utente è consegnato un modulo che riporta i dati relativi al proprio account, con relativa password, eventuale data di scadenza e url tramite cui modificare la password stessa.

Lo username assegnato all'utente può essere scelto dall'utente stesso purché non già utilizzato dagli utenti attivi e disattivati (vedi par. 4).

2.1 Utenti sezioni distaccate

Per le sezioni remote (Massa, Lecce, Roma, Milano, Siena) viene identificato un'incaricato dall'Ufficio del Personale alla ricezione della documentazione, al riconoscimento dell'utente ed al relativo inserimento dei dati nel sistema IdeA.

2.2 Utenti a tempo indeterminato

La procedura sopra descritta si applica a tutti gli utenti a tempo indeterminato per i quali non è prevista nessuna scadenza relativa all'account.

2.3 Utenti a tempo determinato

La procedura di rilascio di un account al personale dipendente a tempo determinato prevede che l'account abbia durata annuale ma che sia rinnovabile senza limiti purché subordinatamente al rinnovo del contratto o di altro rapporto formale con l'Istituto.

2.4 Studenti

Per gli studenti (tirocinanti, tesisti, dottorandi, specializzandi) la durata dell'account è pari alla durata del proprio impegno con l'IFC.

2.5 Utenti Fondazione G. Monasterio

Per gli utenti della Fondazione G. Monasterio l'account, della durata di un'anno rinnovabile senza limiti, viene rilasciato solo se lo stesso utente ha un rapporto di "associatura" con IFC.

2.6 Utenti altri Enti convenzionati

A gli utenti dipendenti di organizzazioni convenzionate con IFC l'account ha durata un anno (in questo caso da parte dell'IFC non è noto il rapporto formale fra l'utente e la propria organizzazione), rinnovabile senza limiti purché al momento del rinnovo sia empre in atto la convenzione fra IFC e l'organizzazione stessa.

2.7 Altri utenti

Tutti gli altri utenti (ospiti, visitatori o altro) possono richiedere un account (è necessario farlo se utilizzano le risorse di rete dell'IFC) per un periodo di durata viariabile purché corrispondente con il periodo di frequenza dell'IFC e di durata non superiore ad un anno. L'account può essere rinnovato senza limiti subordinatamente alla frequenza dell'utente presso l'IFC.

3. Proroga scadenza account

Il rinnovo degli account con scadenza avviene semplicemente con una richiesta tramite posta elettronica all'Ufficio del Personale. Sarà cura di quest'ultimo verificare che il richiedente ne abbia diritto in funzione della validità del proprio rapporto con IFC.

4. Disabilitazione account

La disabilitazione di un account può avvenire o direttamente per iniziativa dell'Ufficio del Personale, nel momento in cui il rapporto con IFC viene a cessare, o su richiesta dello stesso utente o di altro utente che ne abbia diritto (es. responsabile del contratto dell'utente, responsabile di un servizio per violazione del regolamento definito nel modulo MS001 ecc.). La disabilitazione dell'account, operativamente, viene sempre eseguita dall'Ufficio del Personale. L'operazione viene svolta tramite script eseguiti via pagine WWW che non rimuovono effettivamente l'account ma lo riposizionano, all'interno del server LDAP, nel sottoalbero "peopleRemoved" in modo da conservare gli attributi relativi all'utente ed in particolare il suo username in modo che non possa essere riutilizzato per un altro utente.

5. Password

La password assegnata inizialmente (par. 2) è generata casualmente ed assegnata all'utente. La password non ha scadenza. Il sistema registra la data dell'ultimo aggiornamento della stessa ed è quindi compito dell'applicazione che richiede l'autenticazione e necessita che sia prevista la scadenza delle password, verificare che l'intervallo di tempo dall'ultima modifica sia non superiore al periodo previsto per legge (D. L. 196/'03, tre mesi per dati personali, sei mesi per dati sensibili) e impedire l'accesso notificando il motivo all'utente. L'utente può modificare la propria password tramite interfaccia WWW (il cui indirizzo è indicato sul modulo consegnato nella fase di creazione o rinnovo dell'account; par. 2) per la quale l'accesso non viene mai disabilitato purché l'account sia sempre in corso di validità.

6. Tipologia di utenza

La posizione contrattuale nei confronti dell'IFC è registrata nell'attributo LDAP "EmployeeType" dell'Object Class "inetOrgPerson". L'affiliazione, definita con l'attributo "primaryAffiliation" dell'Object Class "inetOrgPerson" richiesta da IDEM, non è salvata all'interno del database LDAP ma viene comunicata alla controparte (reltramite un "mapping" dinamico eseguito da Shibboleth rispettando le corrispondenze dei valori definiti nel documento "Specifiche tecniche per la compilazione e l'uso degli attributi" della Federazione IDEM.

7. Autorizzazione per l'accesso ai servizi

L'autorizzazione per l'accesso ai servizi offerti dall'Istituto o remotamente, tramite la Federazione IDEM, avviene utilizzando i meccanismi messi a disposizione dal sistema IdeA, o tramite SAML (di conseguenza Shibboleth), per i servizi WWW, o direttamente mediante bind su LDAP, per i servizi che non supportano il protocollo SAML (es. autenticazione sistemi Unix via PAM). È previsto che in futuro venga implementata l'autenticazione via protocollo RADIUS, interfacciato al server LDAP per l'autenticazione di dispositivi di rete.

L'autorizzazione per l'accesso ai servizi, a carico del gestore del servizio, può far uso degli attributi messi a disposizione dal sistema IdeA definendo quindi preventivamente i criteri di accesso al servizio. Laddove non sia possibile dei profili predefiniti di autorizzazione perché non è possibile determinare delle caratteristiche o dei ruoli sui quali determinare la modalità di accesso al servizio (es. Consiglio d'Istituto), è possibile fa uso di gruppi appositamente definiti e modificabili dal gestore del servizio tramite interfaccia WWW. In tal caso l'autorizzazione per l'accesso ad un servizio avviene includendo o escludendo dal gruppo utenti già definiti nel sistema e quindi noti all'Ufficio del Personale.

Allo stato attuale non tutti i servizi offerti da IFC fanno uso del sistema di autenticazione IdeA. In particolare il servizio di posta elettronica, essendo gestito da un fornitore esterno, ha un proprio e distinto sistema di autenticazione e autorizzazione.

Al contrario fra i servizi locali che utilizzano il sistema IdeA vi sono: Sito Web Intranet, Wiki, HelpDesk (RT), accesso a sistemi Unix, Nagios (ed altri servizi di monitoraggio).

Come servizi remoti, oltre quelli offerti tramite Federazione IDEM (www.idem.garr.it/index.php/it/servizi-intro) il sistema è utilizzato anche dal servizio PuMa offerto dall'Istituto di Scienza e Tecnologie dell'Informazione (ISTI).

Allegato A

“Modulo di assunzione di responsabilità individuale nell’utilizzo dei servizi informatici”

Modulo MS001

Modulo di assunzione di responsabilità individuale nell'utilizzo dei servizi informatici

Art. 1 - Oggetto
Il presente modulo di assunzione di responsabilità individuale nell'utilizzo dei servizi di rete (di seguito indicato come **modulo**) regola il rapporto fra l'Istituto di Fisiologia Clinica (di seguito indicato come **IFC**), Ente erogante i servizi informatici e di rete, e l'Utente.

Art. 2 - Categorie di Utenti aventi diritto
Il **modulo** potrà essere direttamente sottoscritto dai soggetti appartenenti alle sotto elencate categorie:
- ricercatori IFC;
- personale tecnico-amministrativo IFC;
- personale di Enti convenzionati e/o operanti presso **IFC** in virtù di apposito protocollo di intesa.

I soggetti appartenenti alle sotto elencate categorie possono sottoscrivere il **modulo** previa esibizione di una lettera di presentazione sottoscritta dal responsabile della struttura IFC (Direttore, Responsabile di ricerca, Capo reparto …) presso la quale svolgono la propria attività:
a) dottorandi di ricerca, specializzandi e perfezionandi;
b) studenti, borsisti, tirocinanti;
c) personale tecnico a contratto;
d) ospiti e/o frequentatori volontari.

Art. 3 - Durata del Rapporto
La durata del Rapporto è regolamentata come segue:
- la fruizione dei servizi termina con il venire meno del titolo in base al quale si é instaurato il rapporto fra l'Utente e **IFC.**
- per il personale soggetto alla richiesta di autorizzazione alla frequenza di cui ai punti a), b), c) e d) dell'art.2, la validità del rapporto é commisurata alla durata indicata nella predetta richiesta e agli eventuali rinnovi concessi.

In caso di cessazione definitiva del rapporto saranno disabilitati tutti i servizi di rete richiesti e rimossi anche gli eventuali documenti pubblicati dall'utente a partire dalla data di scadenza del rapporto.
Il salvataggio di eventuali dati va concordato con i responsabili dei servizi.

Art. 4 - Obblighi dell'Utente
L'Utente si impegna:
- a conservare i propri codici di accesso al sistema e a non consentirne l'uso a terzi;
- a comunicare immediatamente a **IFC** l'eventuale perdita di riservatezza esclusiva dei codici di cui al punto precedente;
- a non consentire a terzi, a nessun titolo, l'utilizzo del servizio assegnato;
- a non accedere al servizio con più connessioni contemporanee;

- a non divulgare eventuali informazioni di cui venisse a conoscenza, relative all'attività di altri Utenti del servizio;
- a non pubblicare, diffondere, divulgare, trasmettere, distribuire o utilizzare in alcun modo informazioni o materiale diffamatorio, osceno, riservato o altrimenti illegale;
- a non immettere, trasmettere, utilizzare, diffondere qualsiasi materiale che non può essere legalmente distribuito;
- ad assumersi la piena responsabilità di tutti i dati da lui inoltrati attraverso il servizio;
- a tenere indenne **IFC** da qualsiasi danno, perdita, costo, responsabilità, dagli oneri di spesa che dovessero derivare da atti, fatti, comportamenti, omissioni posti in essere dall'Utente nell'utilizzare il servizio.

Art. 5 - Leggi vigenti e norme comportamentali

Nel presente articolo si richiama l'insieme della normativa vigente che regola l'utilizzo delle reti telematiche e le norme che regolano l'uso della rete GARR (la rete di ricerca accademica finanziata dal Ministero dell'Istruzione, Università e Ricerca), in particolare:

- la Legge per la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali (L. 675/96) e sue successive modifiche ed integrazioni;
- il Decreto legislativo 22/05/99 n.185 e la corrispondente normativa europea, in cui all'art. 10 vengono dichiarate illegali le tecniche di pubblicità sulla rete senza il preventivo consenso del destinatario;
- il Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59);
- la Legge 22 Aprile 1941 in materia di disposizioni sul diritto di autore, con l'aggiornamento del comma 1/b aggiunto dall'Art. 1 D.Lgs. 29/12/1992, n. 518 (attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore);
- le regole di buon comportamento, che vanno sotto il nome di ***netiquette*** , per l'uso dei servizi di rete di **IFC** e della rete GARR riportate negli allegati **A** e **B**.

Art. 6 - Obblighi di IFC

IFC si impegna a garantire la riservatezza su tutti i dati personali dell'Utente.
Per gli Utenti che abbiano fatto richiesta della casella postale, **IFC** si impegna alla riservatezza circa le informazioni che l'Utente mantiene sulle macchine della rete **IFC** che ospitano la casella postale.
IFC, nei limiti delle risorse disponibili, si impegna affinché tutti i servizi oggetto del presente **modulo** funzionino nel migliore dei modi.

Art. 7 - Limiti di Responsabilità

IFC non è tenuto a fornire consulenza sulle configurazione delle apparecchiature dell'Utente. Attività di supporto verrà erogata compatibilmente con gli impegni e le disponibilità di personale **IFC**.
IFC non si ritiene responsabile di eventuali danni recati all'Utente a causa di guasti e/o malfunzionamenti degli apparati di gestione del servizio.

Art. 8 - Limitazioni all'utilizzazione del servizio
L'Utente non può cedere a terzi alcun tipo di servizio di rete né può utilizzarli in alcun modo per scopi diversi da quelli per cui l'accesso ai servizi viene concesso.
L'utente prende atto che i servizi vengono offerti per essere utilizzati per l'adempimento delle mansioni assegnate e non a scopo personale o comunque estraneo alla attività lavorativa e/o di ricerca svolta. A tal scopo, l'Utente prende atto inoltre che **IFC** potrà svolgere attività di monitoraggio sull'uso fatto dei servizi nel rispetto della normativa vigente.

Art. 9 - Risoluzione del Rapporto
IFC potrà interrompere immediatamente il servizio prestato all'Utente per la mancata osservanza delle disposizioni contenute negli articoli 4, 5 e 8 della presente assunzione di responsabilità, ivi compresa la palese violazione del codice di buon comportamento riportata negli allegati **A** e **B**.

L'Utente dichiara di aver attentamente letto tutte le clausole del presente Modulo e le sottoscrive accettandole in toto e senza riserve compresi gli allegati di seguito elencati:
A) Norme di accesso alla rete GARR;
B) Raccomandazioni di uso;

Data_____ Firma per accettazione _____

Allegato A

Norme di accesso alla rete GARR

La rete GARR non può essere usata per nessuna delle seguenti attività:

1) uso dei servizi o delle risorse in un modo che possa danneggiare o molestare altre persone o attentare alla dignità umana;
2) creazione o trasmissione (se non per scopi di ricerca propriamente controllati e legali) di qualunque immagine, dati o altro materiale offensivo, osceno o indecente;
3) creazione o trasmissione di materiale finalizzato o in grado di arrecare disturbi o produrre ingiustificate preoccupazioni;
4) creazione o trasmissione di materiale diffamatorio;
5) trasmissione di materiale che viola i diritti di autore;
6) trasmissione di materiale commerciale o pubblicitario non richiesto;
7) fornitura deliberata di accessi non autorizzati ai servizi accessibili via GARR;
8) qualsivoglia attività vietata dalle leggi vigenti, con particolare riferimento alla legge sulla privacy;
9) qualsivoglia attività che produca deliberatamente:
   a) spreco di risorse di rete o del personale addetto al suo funzionamento;
   b) danni o distruzione di dati di altri Utenti;
   c) violazione della riservatezza di altri Utenti;
   d) interferenze sul lavoro di altri Utenti.
10) usi che impediscano l'utilizzo del servizio ad altri Utenti (ad esempio il sovraccarico delle linee di accesso o degli apparati di commutazione);
11) mancato adeguamento di apparecchiature o software dopo che il GARR ha determinato che interferiscono con il corretto funzionamento della rete;
12) altri usi impropri, quali l'introduzione di "virus".

Allegato B

Le raccomandazioni che seguono sono rivolte all'Utente per un corretto uso delle risorse assegnate da IFC.

- Qualunque attività che appesantisca il traffico sulla rete, quale per esempio il trasferimento di archivi voluminosi, deteriora il rendimento complessivo della rete. Si raccomanda pertanto di effettuare queste operazioni in orari diversi da quelli di massima operatività (ad esempio di notte), tenendo presenti le eventuali differenze di fuso orario. **IFC** rende disponibile software di utilità, generalmente reperibile presso **ftp.unipi.it** e **www.cnuce.pi.cnr.it/cnuweb/resources/mirrors.html**
  Nota: se un file è disponibile localmente (Pisa), è consigliabile scaricarlo dal server locale evitando così di impegnare la rete per un tempo maggiore.
- Il software reperibile sulla rete può essere coperto da brevetti e/o vincoli di utilizzo di varia natura. E' bene leggere sempre attentamente la documentazione di accompagnamento prima di utilizzarlo, modificarlo o redistribuirlo in qualunque forma.
- Controllate e scaricate la posta ogni giorno, lasciarla sul server significa sprecare spazio disco riducendo le risorse per tutti gli utenti.
- Cancellate i messaggi non più utili; occupano spazio su disco e riducono le risorse a disposizione degli utenti.
- Non date mai il vostro userID o la password a un'altra persona. Gli amministratori di sistema, qualora dovessero accedere al vostro account per manutenzione, lo potranno generalmente fare senza la necessità di conoscere la vostra password (nel rispetto dell' Art. 6 comma 2).

Nell'utilizzo della posta elettronica si tenga presente quanto segue:

- Non inviate mai nulla di particolarmente privato o compromettente.
- Scrivete paragrafi e messaggi corti ed essenziali.
- Focalizzate un argomento per messaggio e indicate sempre il soggetto del messaggio, in modo che gli altri utenti possano localizzarlo velocemente.
- Includete la vostra firma in fondo ai messaggi. La firma dovrebbe includere nome, titolo (se desiderato), eventuale organizzazione di appartenenza e i vari indirizzi di posta elettronica. Il tutto non dovrebbe comunque superare le quattro righe. Informazioni opzionali potrebbero contenere l'indirizzo postale e un recapito telefonico.
- Scrivete con le lettere maiuscole solo per sottolineare un punto importante o per distinguere un titolo o un sottotitolo dal resto del testo. Scrivere in maiuscole intere parole che non sono titoli viene generalmente definito URLARE! *Asterischi* intorno ad una parola posso aiutare a evidenziare un termine.
- Controllate la lunghezza della riga ed evitate i caratteri di controllo.
- Siate professionali e prestate attenzione a ciò che dite riguardo altre persone. La posta elettronica viene inoltrata e citata con facilità.
- Identificate tutte le citazioni, i riferimenti e le fonti delle informazioni che divulgate, rispettate i copyright e gli eventuali accordi per la divulgazione di qualsiasi informazione.
- È considerato estrema maleducazione l'inoltrare comunicazioni personali e/o private a mailing list senza l'esplicita autorizzazione del moderatore e senza che sia di interesse per tutti gli iscritti alla medesima.