
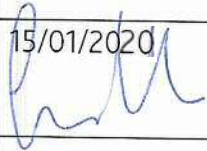




**ISTITUTO
ITALIANO DI
TECNOLOGIA**

Procedura Accessi Logici

Revisione	Descrizione Modifica	Autore	Approvazione	Data
01	Prima emissione	ICTD	SD DG	13/05/2019
02	Prolungamento account per adempimenti post contrattuali	ICTD	SD/ DG 	15/01/2020 



**ISTITUTO
ITALIANO DI
TECNOLOGIA**

Procedura Accessi Logici

Revisione	Descrizione Modifica	Autore	Approvazione	Data
01	Prima emissione	ICTD	SD DG	13/05/2019
02	Prolungamento account per adempimenti post contrattuali	ICTD	SD DG	15/01/2020

SOMMARIO

1. Obiettivi e finalità.....	3
2. Premessa e definizioni.....	3
2.1 Premessa	3
2.2 Definizioni.....	4
3. Principali attori e responsabilità	5
4. Documenti e strumenti	5
5. Attuazione	6
5.1 Principi	6
5.2 Profili Autorizzativi ed Utenze Personali	6
5.3 Gestione dei Profili Autorizzativi	7
5.4 Gestione delle Utenze Personali	8
5.5 Gestione delle Utenze Amministrative	10
5.6 Gestione delle Utenze Tecniche	11
5.7 Elenco e Revisione di tutte le Utenze	12
5.8 Misure di Sicurezza per gli Accessi Logici.....	13
5.9 Attività di controllo	14
5.10 Responsabilità.....	14

1. Obiettivi e finalità

- Oggetto della presente Procedura è la gestione delle utenze che permettono l'accesso, l'utilizzo e la gestione di tutti i sistemi e le dotazioni informatiche e di telecomunicazione (di seguito anche "Sistemi Informatici") di proprietà o nella disponibilità della Fondazione IIT (di seguito, anche "Fondazione" o "IIT").
- Destinatario della presente Procedura è chiunque abbia un rapporto di lavoro dipendente, di collaborazione e il personale esterno affiliato alla Fondazione IIT che svolge attività di ricerca scientifica, professionale o di studio all'interno delle strutture di IIT. Le suddette categorie di soggetti saranno di seguito denominate anche "Utenti".
- Destinatari della presente Procedura sono anche tutte le terze parti, quali fornitori ed enti di ricerca, che gestiscono informazioni della Fondazione IIT tramite sistemi e dotazioni informatiche e di telecomunicazione. Le suddette categorie di soggetti saranno di seguito denominate anche "Terze Parti".
- Finalità della presente Procedura è quella di stabilire norme per la creazione, gestione, assegnazione e rimozione di privilegi e di utenze nei sistemi informatici della Fondazione, allo scopo di garantire che vengano soddisfatte misure di sicurezza tali da mitigare possibili rischi relativi alla Riservatezza, Integrità e Disponibilità delle informazioni e dei sistemi informatici.


Nelle seguenti disposizioni si farà anche riferimento alla normativa vigente applicabile in materia di protezione dei dati personali.

2. Premessa e definizioni

2.1 Premessa


La Fondazione adotta strumenti, processi e procedure utili al fine di garantire la sicurezza delle informazioni e di incoraggiare la responsabilizzazione dei singoli Utenti.

I Sistemi Informatici messi a disposizione degli Utenti dalla Fondazione costituiscono uno dei punti di forza di quest'ultima, ma, allo stesso tempo, possono essere fonte di rischio per la sicurezza delle informazioni trattate e per l'immagine della Fondazione. Per questo motivo, è necessario che la gestione delle utenze che permettono l'accesso ai sistemi informatici della Fondazione, segua procedure che permettano di mitigare i rischi relativi alla Riservatezza, Integrità o Disponibilità delle informazioni e dei sistemi informatici di proprietà o nella disponibilità della Fondazione.

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura Accessi Logici	IO IT 05
--	--------------------------	----------

2.2 Definizioni

Nome	Sigla	Descrizione
Tecnologie dell'Informazione e della Comunicazione	ICT	Le tecnologie dell'informazione e della comunicazione (ovvero "Information and Communications Technology", ICT) sono l'insieme dei metodi e delle tecniche utilizzate nella trasmissione, ricezione ed elaborazione di dati e informazioni usualmente tramite tecniche e strumenti digitali.
Sistema Informatici	S.I.	I sistemi e le dotazioni informatiche e di telecomunicazione di proprietà o nella disponibilità della Fondazione IIT.
Rete di Telecomunicazione	R.T.	Insieme di dispositivi e dei loro collegamenti (fisici o logici) che consentono la trasmissione e la ricezione di informazioni di qualsiasi tipo tra due o più utenti situati in posizioni geograficamente distinte, effettuandone il trasferimento attraverso cavi, sistemi radio o altri sistemi elettromagnetici o ottici.
Dati Personali	D.P.	Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Utente	UT	Un utente è una persona fisica che interagisce con un S.I. accedendovi tramite una utenza.
Utenza	Ut.a	Una utenza è un meccanismo informatico tramite il quale un S.I. mette a disposizione di un utente, individuato da un nome utente, un ambiente di elaborazione possibilmente con contenuti e funzionalità personalizzabili e con un appropriato isolamento dalle altre utenze.
Utenza Tecnica	Ut.T.	Una utenza tecnica è un'utenza che non è associata ad una persona fisica ed è tipicamente utilizzata per la gestione di un S.I..
Utenza Personale	Ut.P.	Una utenza personale è una utenza che è univocamente assegnata ed utilizzata da una sola persona fisica.
Utenza Amministrativa	Ut.A.	Una utenza amministrativa è una utenza che permette l'amministrazione e la gestione, quale l'installazione e l'aggiornamento, di un S.I. e delle sue componenti.
Profilo Autorizzativo	P.A.	Un profilo autorizzativo è un insieme di privilegi che permettono all'utenza a cui sono assegnati di eseguire un insieme coerente di attività su di un S.I..
Active Directory	AD	Active Directory è un insieme di servizi di rete presenti nei sistemi Microsoft che gestiscono in maniera centralizzata le utenze e le risorse dei S.I. tramite delle Politiche di Gruppo.
Dominio AD	D.AD.	Un dominio AD è un gruppo logico di S.I. Microsoft che condividono un database directory AD centralizzato.
Accesso Remoto	AR	Accesso ad un sistema, servizio o applicazione presente od erogato da un dispositivo diverso da quello fisicamente utilizzato dall'utente o direttamente connesso a questo.
Autenticazione Forte (Strong Authentication)	AF	Un metodo di autenticazione che utilizza modalità più sicure del solo controllo della password, tipicamente utilizzando almeno due controlli tra: una cosa che si conosce (quale una password), una cosa che si ha (quale un dispositivo fisico, chiave ecc.), una cosa che si è (quale una caratteristica biometrica dell'utente).


 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura Accessi Logici	IO IT 05
--	--------------------------	----------

3. Principali attori e responsabilità

Attore	Sigla	Maggiori responsabilità
Direzione ICT	ICTD	<p>Lo sviluppo e la gestione della rete interna è affidata alla Direzione ICT che opera conformemente alle delibere degli organi istituzionali della Fondazione ed in stretta collaborazione con GARR.</p> <p>La Direzione ICT gestisce centralmente privilegi e/o utenze dei S.I. in dominio AD.</p>
Utente	UT	<p>Chiunque abbia un rapporto di lavoro dipendente, di collaborazione e il personale esterno affiliato alla Fondazione IIT che svolge attività di ricerca scientifica, professionale o di studio all'interno delle strutture di IIT.</p> <p>Sono utenti della rete della Fondazione in particolare le persone afferenti a tutte le strutture di ricerca e di servizio direttamente connesse alla rete interna della Fondazione. Tutti gli utenti che a qualsiasi titolo utilizzano la rete di Fondazione accettano senza riserve la presente Procedura.</p>
Direttore	DIR	Ogni Direttore/Responsabile di Funzione valida e autorizza la creazione, modifica, chiusura e rimozione di utenze e privilegi sui sistemi per i quali è responsabile.
Principal Investigator/ Facility coordinator	P.I.	Ogni P.I. valida e autorizza la creazione, modifica, chiusura e rimozione di utenze e privilegi sui sistemi per i quali è responsabile.
Amministratore di Sistema	A.d.S.	Particolari utenti dei S.I. con la responsabilità della gestione e amministrazione degli stessi, come anche definiti dal Provvedimento Generale del Garante Privacy del 27 Novembre 2008
Direzione Risorse Umane e Organizzazione	H.R.O.D.	La Direzione Risorse Umane e Organizzazione comunica alla Direzione ICT la richiesta di creazione di una nuova utenza, di modifica di un'utenza (ad esempio per cambio mansione), e la chiusura di un'utenza per cessazione del rapporto di lavoro per i sistemi gestiti dalla Direzione ICT.
Referente ICT	R.ICT	Figura tecnica che ha in carico la gestione di S.I. non gestiti direttamente dalla Direzione ICT.

4. Documenti e strumenti

Tipo	Nome	Utilizzo
Policy	Policy ICT	Stabilire il corretto utilizzo dei Sistemi Informatici nella Fondazione IIT (di seguito, anche "Fondazione" o "IIT") proteggendo IIT e gli Utenti dal rischio di compromissione dei Sistemi Informatici, dalla indebita divulgazione di dati personali e riservati, e dalle relative conseguenze legali.

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura Accessi Logici	IO IT 05
--	--------------------------	----------

Tipo	Nome	Utilizzo
Procedura	Accesso ai dati in caso di emergenza o assenza prolungata	Definire e regolamentare, in accordo con la Policy ICT della Fondazione, le modalità di accesso ai dati aziendali gestiti dagli Utenti localizzati all'interno dei Sistemi Informatici della Fondazione, nei casi di assenza improvvisa o prolungata dell'Utente durante la quale si verifichino improrogabili necessità legate all'attività lavorativa o dalle quali comunque possano derivare conseguenze pregiudizievoli per la Fondazione.

5. Attuazione

5.1 Principi

La gestione delle utenze personali e dei diritti di accesso ai sistemi ed alle applicazioni della Fondazione si basa sui seguenti principi di sicurezza e buon governo dei sistemi:

1. Principio del "Need to know" (ovvero "necessità di sapere"):

Il diritto di accesso ad un sistema od applicazione è concesso solo a chi ne ha la necessità per la gestione del sistema stesso o per la gestione dei processi di business e delle informazioni in esso presenti;

2. Principio del privilegio minimo:

I privilegi concessi per l'accesso ad un sistema od applicazione devono essere limitati solamente a quelli essenziali e necessari a svolgere le attività in carico all'Utente;

3. Principio di separazione dei compiti:


Ad un'utenza personale possono essere assegnati privilegi relativi ad una sola delle seguenti tre funzioni: operativa, autorizzativa, di controllo.

I tre principi devono essere applicati sulla base delle reali necessità della Fondazione, ad esempio può verificarsi che i principi 2 e 3 non si applichino ad alcuni Amministratori di Sistema, e che il principio 3 non si applichi ad alcuni Direttori o P.I.

5.2 Profili Autorizzativi ed Utenze Personali

In ogni sistema e applicazione devono essere definiti dei Profili Autorizzativi, ovvero degli insiemi di privilegi che permettono ad un'utenza personale a cui sono assegnati di eseguire un insieme coerente di attività.

I principali privilegi permettono la creazione, modifica, lettura, cancellazione od esecuzione di un insieme di risorse. Un Profilo Autorizzativo indica, per ogni insieme di risorse del sistema o applicazione, quali privilegi sono concessi. Per impostazione predefinita, ad un profilo non è concesso alcun privilegio a tutte le risorse del sistema o applicazione (in ottemperanza al principio del privilegio minimo). La configurazione di un profilo consiste nell'assegnazione dei soli privilegi necessari alla gestione delle risorse utili ad eseguire un insieme coerente di attività.

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura Accessi Logici	IO IT 05
--	--------------------------	----------

Ad ogni utenza personale sono associati uno o più profili.

Per la gestione di Profili Autorizzativi e delle utenze è necessario specificare la relazione tra il S.I. ed il dominio AD aziendale; sono possibili tre casi:

1. S.I. integrato nel dominio AD aziendale sia per le utenze che per i profili autorizzativi: le utenze ed i profili autorizzativi sono creati nel dominio AD e da questo condivise con il S.I.;
2. S.I. integrato nel dominio AD aziendale solo per le utenze: le utenze sono create nel dominio AD e da questo condivise con il S.I. mentre i profili autorizzativi sono creati e gestiti direttamente nel S.I.;
3. S.I. non integrato nel dominio AD aziendale: sia le utenze che i profili autorizzativi sono creati e gestiti direttamente nel S.I..

Ove tecnicamente possibile devono essere integrate nel dominio AD aziendale sia la gestione delle utenze che dei profili autorizzativi.

Sono possibili 5 fattispecie di utenze personali:

1. Utenze amministrative centrali: utenze utilizzate dagli AdS per gestire sistemi e applicazioni associate al dominio AD aziendale;
2. Utenze amministrative locali: utenze utilizzate dagli AdS per gestire sistemi e applicazioni locali al sistema o applicazione;
3. Utenze personali in dominio AD con profilazione centrale: utenze e profili gestiti tramite il dominio AD aziendale;
4. Utenze personali in dominio AD con profilazione locale: utenze gestite tramite il dominio AD aziendale con profili gestiti localmente sul sistema o applicazione;
5. Utenze personali locali con profilazione locale: utenze e profili gestiti localmente sul sistema o applicazione.

Ove tecnicamente possibile devono essere utilizzate utenze e profili centrali in dominio AD.

5.3 Gestione dei Profili Autorizzativi

Per ogni S.I., la gestione dei profili autorizzativi, sia locali che tramite il dominio AD aziendale qualora integrato, si compone dei seguenti passi operativi.

Creazione, modifica o rimozione di un profilo autorizzativo

- La richiesta di creazione, modifica o rimozione di un profilo autorizzativo è formulata dal responsabile del S.I. in quanto soggetto deputato a valutare l'opportunità e la necessità di un

nuovo profilo o dell'esigenza di apportare modifiche ad un profilo esistente, in modo che il profilo costituisca un insieme di privilegi e risorse utili ad eseguire un insieme coerente di attività;

- Il responsabile del S.I. si coordina con il gruppo di sviluppo per l'implementazione del nuovo profilo o, ove non necessario, con l'AdS per l'implementazione diretta del profilo sul S.I.;
- Il gruppo di sviluppo, o l'AdS, crea, modifica o rimuove il profilo autorizzativo sul S.I..

Elenco dei profili autorizzativi

Il responsabile di un S.I. deve poter fornire l'elenco dei profili autorizzativi esistenti sul S.I., con associato ad ogni profilo la descrizione dello scopo e dei privilegi concessi, anche tramite estrazione dal S.I. stesso effettuata dall'AdS o da altro tecnico di riferimento.

Revisione dei profili autorizzativi

- Per ogni S.I. almeno una volta all'anno viene prodotto l'elenco dei profili autorizzativi e svolta una revisione di tutti i profili autorizzativi esistenti;
- Il responsabile di un S.I. valuta se vi sono profili autorizzativi da modificare nel qual caso si procede secondo quanto descritto precedentemente in questa sezione;
- Il responsabile di un S.I. valuta se vi sono profili autorizzativi da rimuovere, ad esempio se un profilo autorizzativo non è più assegnato ad alcuna utenza e non è previsto che vengano create nuove utenze che ne facciano uso; per la rimozione del profilo autorizzativo si procede secondo quanto descritto precedentemente in questa sezione.

Alcuni sistemi, quali ad esempio SAP e sistemi di analisi e reportistica ad esse correlati, prevedono una gestione dei profili autorizzativi specifica, i cui dettagli sono presentati in apposita procedura che sostituisce la presente sezione.

5.4 Gestione delle Utenze Personali

Ogni utenza personale sui S.I. è individuale e non sono permesse utenze condivise. Ad ogni utenza personale deve corrispondere la formalizzazione di un contratto di lavoro o fornitura.

Un'utenza personale non può superare la scadenza del contratto con la Fondazione dell'utente a cui è assegnata.

Un'utenza può essere prorogata oltre la scadenza per il tempo strettamente necessario all'adempimento di attività che derivino da situazioni contrattuali pregresse con IIT e che abbiano ricadute successive all'estinzione del rapporto di lavoro.

Alla creazione di una nuova utenza personale, l'AdS crea una nuova password, complessa¹ e unica per quell'utenza che comunica all'Utente. Alla prima connessione l'Utente deve cambiare la password.

Ove tecnicamente possibile, i sistemi e applicazioni devono chiedere nuovamente agli utenti l'autenticazione dopo un periodo predefinito di inattività, impostato tipicamente a 15 minuti².

Nel caso all'utenza vengano assegnati profili che permettono l'accesso a dati personali³, prima di abilitare l'accesso dell'utenza al S.I. deve essere verificato che l'utente sia stato nominato ed abbia accettato la nomina a responsabile/incaricato al trattamento dei dati personali.

La gestione delle utenze personali comprende le seguenti attività.

Creazione o modifica di un'utenza personale su S.I. integrati in dominio AD (sistema preferenziale)

- Per i S.I. integrati nel dominio AD della Fondazione la creazione o modifica di un'utenza è svolta in AD; La Direzione Risorse Umane e Organizzazione aggiorna e verifica l'anagrafica condivisa degli utenti della Fondazione specificando la scadenza contrattuale;
- Il responsabile del S.I. o il responsabile dell'utente che chiede la creazione dell'utenza, indica i profili autorizzativi da assegnare all'utenza;
- L'AdS crea l'utenza in AD con i profili indicati e se richiesto assegna all'utenza ulteriori profili locali sui singoli sistemi;

Creazione o modifica di un'utenza personale su S.I. non integrati in dominio AD

- Per i sistemi e applicazioni non integrati nel dominio AD aziendale, il responsabile del S.I., richiesto un parere alla Direzione Risorse Umane e Organizzazione, raccoglie i dati anagrafici dell'utente, la scadenza, la qualifica e le mansioni e indica all'AdS, autorizzandolo, i profili autorizzativi da assegnare o da modificare all'utenza;
- L'AdS del S.I. crea o modifica l'utenza con i profili indicati.

Chiusura di un'utenza personale

Alla scadenza della validità del contratto le utenze sono chiuse automaticamente dai S.I. integrati nel dominio AD aziendale. Per i S.I. non integrati nel dominio AD aziendale, il responsabile del S.I. provvede ad incaricare gli AdS della chiusura dell'utenza alla data di scadenza della stessa.

¹ Si veda la sezione 5.8 "Misure di Sicurezza per gli Accessi Logici".

² Si veda NIST 800-53 (Rev. 4) AC-11 "Session Lock", e Australian Government Information Security Manual Control 0428 "Session and screen locking"

³ Si veda la normativa vigente applicabile in materia di protezione dei dati personali.

Blocco temporaneo di un'utenza

Il responsabile del S.I. può richiedere all'AdS il blocco temporaneo di un'utenza in caso di incidenti, attività sospetta, motivi di sicurezza e di urgenza, dandone comunicazione all'interessato e alla Direzione Risorse Umane e Organizzazione.

Al termine del blocco temporaneo dell'utenza questa può essere chiusa oppure riattivata nel qual caso deve essere valutato se è necessario effettuare un reset della password.

Reset della Password di un'utenza

Ove presente, un utente può utilizzare il servizio di reset autonomo della password erogato da apposito portale, oppure può richiedere il reset della password della propria utenza alla Direzione ICT, o direttamente all'AdS del S.I..

Per ragioni di sicurezza, la Direzione ICT può imporre il reset della password ad alcune o tutte le utenze.

In caso di reset non autonomo della password, un utente fa richiesta di reset per la propria utenza alla Direzione ICT tramite ticket o direttamente all'AdS. L'AdS crea una nuova password, complessa⁴, unica per quell'utenza e che comunica all'utente; al primo accesso l'utente deve cambiare la password.

5.5 Gestione delle Utenze Amministrative

Le utenze amministrative per tutti i sistemi e servizi della Fondazione sono nominali ed individuali, non sono permesse utenze amministrative condivise.

Le utenze amministrative sono distinte dalle utenze personali e devono essere utilizzate unicamente per le attività di amministrazione e gestione dei S.I.

Le utenze amministrative possono essere assegnate solo a personale che ha ricevuto la nomina quale AdS.

Ove tecnicamente possibile, gli accessi alle utenze amministrative devono essere fatti con Autenticazione Forte (vedi sezione 5.8).

Gli accessi e le attività amministrative devono essere tracciati. La tracciatura delle attività deve rispettare la normativa vigente.

Il processo di accesso in emergenza a sistemi e applicazioni è descritto nella procedura apposita.

Per quanto non specificato in questa sezione, la gestione delle utenze amministrative segue il processo descritto nella sezione 5.4.

⁴ Si veda la sezione 5.8 "Misure di Sicurezza per gli Accessi Logici".

5.6 Gestione delle Utenze Tecniche

Le utenze tecniche sono utenze di servizio create sui S.I. tipicamente per svolgere attività di amministrazione, gestione e interfacciamento per permettere l'esecuzione di specifici applicativi o per permettere l'esecuzione di attività tecniche interne ai S.I. stessi.

Alle utenze tecniche possono essere assegnati privilegi amministrativi.

Il responsabile del S.I. è anche responsabile di ogni utenza tecnica presente nel S.I., della loro gestione come qui descritta e dell'adozione delle misure di sicurezza descritte nella sezione §5.8.

Le utenze tecniche non devono essere utilizzate dagli utenti per normali attività sui sistemi IT né per attività non incluse nell'ambito predefinito per ciascuna di esse.

È previsto che gli Amministratori di Sistema accedano localmente ai S.I. (es. attraverso una console di sistema), utilizzando utenze tecniche, nei seguenti casi eccezionali:

- quando non sia disponibile la connettività di rete per l'accesso da remoto ai S.I. da parte degli Amministratori di Sistema mediante le proprie utenze nominali;
- per esigenze legate alla manutenzione ordinaria o straordinaria dei S.I. da parte degli Amministratori di Sistema, laddove non sia possibile effettuare tali attività da remoto, utilizzando le proprie utenze nominali.

L'accesso locale (da console) ai S.I. da parte degli Amministratori di Sistema attraverso utenze tecniche, nei casi eccezionali precedentemente indicati, è subordinato all'adozione di idonee procedure atte ad assicurare:

- l'identificazione certa, anche fisica, dell'Amministratore di Sistema che andrà ad utilizzare l'utenza tecnica;
- le motivazioni giustificative e lo scopo delle attività che richiedono l'uso dell'utenza impersonale;
- la registrazione della data e dell'ora di accesso e l'individuazione univoca del sistema/i interessato/i;
- la registrazione dell'intervallo di tempo (login-logout) durante il quale l'Amministratore ha utilizzato l'utenza impersonale;
- adeguata custodia delle password associate alle utenze impersonali, volta a garantirne la riservatezza e contestualmente la disponibilità nel momento in cui vi sia la necessità di utilizzarle;
- validità temporanea della password utilizzata per l'accesso, limitata ad una singola sessione di intervento.

Le utenze tecniche possono essere:

1. Utenze tecniche in dominio AD: utenze gestite tramite il dominio AD aziendale;
2. Utenze tecniche locali: utenze gestite localmente sul S.I..

Ove tecnicamente possibile devono essere utilizzate utenze tecniche nel dominio AD aziendale.

Creazione di un'utenza tecnica su S.I. integrati nel dominio AD

La creazione di un'utenza tecnica nel dominio AD aziendale è autorizzata dalla Direzione ICT ed è effettuata da un AdS con l'assegnazione dei profili e privilegi necessari sia nel dominio AD aziendale che eventualmente su singoli sistemi.

Creazione di un'utenza tecnica su S.I. non integrati nel dominio AD

La creazione di un'utenza tecnica sui sistemi non integrati nel dominio AD aziendale è autorizzata dal responsabile del S.I. ed è effettuata da un AdS con l'assegnazione dei profili e privilegi necessari.

Gestione delle credenziali per utenze tecniche

La gestione delle credenziali per le utenze tecniche può essere dei seguenti tipi:

- Login bloccato, l'accesso all'utenza è permesso solo agli AdS;
- Login permesso tramite password, la password può essere senza scadenza ma non deve essere utilizzata normalmente dagli utenti per accedere all'utenza, l'accesso all'utenza è permesso solo agli AdS; la password deve essere salvata in modo sicuro, ad esempio in busta chiusa in armadio chiuso.

Ove presenti, le password devono soddisfare le caratteristiche minime di sicurezza descritte nella sezione §5.8, ad eccezione dei requisiti di modifica periodica.

Chiusura e rimozione di un'utenza tecnica

Le utenze tecniche non hanno tipicamente una validità predefinita. Al termine della loro utilità, le utenze tecniche devono essere rimosse automaticamente con la rimozione del servizio, oppure manualmente dall'AdS al momento della rimozione del servizio IT a cui sono assegnate.

5.7 Elenco e Revisione di tutte le Utenze

Elenco di tutte le utenze

Il responsabile di un S.I. deve poter fornire l'elenco di tutte le utenze (personali, amministrative e tecniche) esistenti sul S.I., con associata ad ogni utenza l'elenco dei profili assegnati.

Revisione delle utenze

- Per ogni S.I. almeno una volta all'anno viene prodotto l'elenco di tutte le utenze esistenti e svolta una loro revisione;

- Il responsabile di un S.I. valuta se vi sono utenze che devono essere modificate, ad esempio cambiando i profili autorizzativi assegnati, nel qual caso si procede come descritto nelle precedenti sezioni di questo documento;
- Il responsabile di un S.I. valuta, per le utenze personali e amministrative con il supporto della Direzione Risorse Umane e Organizzazione, se vi sono utenze non utilizzate che devono essere chiuse, nel qual caso si procede come descritto nelle precedenti sezioni di questo documento.

5.8 Misure di Sicurezza per gli Accessi Logici

Nel dialogo via rete tra 2 sistemi distinti, le credenziali di accesso non devono mai essere trasferite in chiaro ma attraverso canali cifrati. Gli accessi a S.I. remoti devono essere eseguiti tramite connessioni cifrate. La cifratura delle credenziali e delle comunicazioni deve adottare protocolli ed algoritmi crittografici considerati sicuri allo stato dell'arte.

La modalità di base per l'identificazione, autenticazione e autorizzazione di un utente presso un S.I. è l'utilizzo come credenziali di una username (o nome utenza) e una password, ove la password è nota al solo utente.


L'accesso, specialmente se da Internet, a S.I. che gestiscono dati personali, riservati, particolari ed in generale con livello di rischio alto, deve essere permesso, ove possibile, tramite Autenticazione Forte (Strong Authentication) degli utenti. Una autenticazione è forte se oltre alla, od al posto della verifica della password, viene verificato almeno uno tra:

- una cosa che si ha (ad esempio un dispositivo fisico, chiave ecc.);
 - di particolare sicurezza sono i sistemi che producono ulteriori password utilizzabili una volta sola ed a tempo limitato (Time-Based One-Time-Password)
- una cosa che si è (ad esempio una caratteristica biometrica dell'Utente).

Caratteristiche minime di sicurezza della password:

- Lunghezza minima 8 caratteri;
- Non deve contenere il nome, cognome, indirizzo email o codice identificativo dell'utente;
- Deve contenere caratteri appartenenti ad almeno tre delle quattro categorie qui di seguito elencate:
 - Lettere maiuscole (da "A" a "Z");
 - Lettere minuscole (da "a" a "z");
 - Numeri (0,1,2...);
 - Caratteri di punteggiatura (,;.:) o speciali (ad esempio: _,-,!,\$, #, %).

La password deve essere modificata al primo utilizzo. In caso di trattamento di dati personali, riservati o particolari, la password è modificata almeno ogni tre mesi.

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura Accessi Logici	IO IT 05
--	--------------------------	----------

5.9 Attività di controllo

La Direzione ICT è autorizzata dalla Fondazione a verificare la congruità della definizione dei profili autorizzativi, dell'assegnazione delle utenze ai profili e la corretta gestione dei profili e delle utenze secondo quanto descritto in questo documento (si veda anche la "Policy ICT").

5.10 Responsabilità

Chiunque non rispetti la presente policy potrà incorrere nell'immediata sospensione dell'accesso ai Sistemi Informatici da parte della Fondazione IIT, che si riserva l'eventuale attivazione di procedure disciplinari, ricorrendone i presupposti.

Inoltre, le violazioni delle norme in materia di sicurezza nella gestione e nell'utilizzo dei Sistemi Informatici e delle norme in materia di protezione dei dati personali possono comportare ulteriori e autonome conseguenze di ordine civile, penale e amministrativo.