ISTITUTO
ITALIANO DI
TECNOLOGIA

Procedura per l'accesso ai dati in caso di assenza improvvisa o prolungata

Revisione	Descrizione Modifica	Autore	Approvazione	Data
01	Prima emissione	ICTD	SD DG	21/12/2018

ISTITUTO
ITALIANO DI
TECNOLOGIA

Procedura per l'accesso ai dati in caso di assenza improvvisa o prolungata

Revisione	Descrizione Modifica	Autore	Approvazione	Data
01	Prima emissione	ICTD	SD DG	21/12/2018

Indice

1. Obiettivi e finalità

Obiettivo della presente procedura è definire e regolamentare, in accordo con la Policy ICT della Fondazione Istituto Italiano di Tecnologia (di seguito, anche "Fondazione" o "IIT"), le modalità di accesso ai dati aziendali gestiti dagli utenti (di seguito: "Utenti") localizzati all'interno dei Sistemi Informatici della Fondazione, quali, a titolo esemplificativo, il servizio di posta elettronica della Fondazione, il PC di lavoro, le directory condivise o i servizi cloud forniti dalla 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. La presente procedura (nel prosieguo, per brevità, anche "Procedura di accesso ai dati in emergenza") assicura la massima trasparenza dell'operato della Fondazione e tutela gli Utenti da accessi che possano essere finalizzati al raggiungimento di obiettivi diversi e ulteriori, con particolare riferimento alla riservatezza degli Utenti stessi nel rispetto della normativa in materia di tutela dei lavoratori. Gli Utenti sono messi a conoscenza della presente procedura e ne devono tenere conto nell'utilizzo deie Sistemi Informatici.
La presente procedura non copre gli eventuali accessi effettuati nell'ambito di attività di approfondimenti o verifiche effettuate dalla Fondazione in caso di sospetti illeciti, di qualsiasi natura, che siano stati perpetrati a suo danno o a danno di terzi, anche in violazione della regolamentazione interna.

2. Premessa e definizioni

a. Premessa

Nell'ambito delle attività svolte per la Fondazione, gli Utenti dei Sistemi Informatici possono risultare temporaneamente in possesso, nei propri spazi dati (quali posta elettronica, PC, directory o servizi in cloud), di informazioni aziendali non reperibili altrove, che possono risultare necessarie per il corretto svolgimento delle attività della Fondazione in momenti in cui gli Utenti stessi non sono in grado di fornirli, in particolare in caso di assenza improvvisa o prolungata. In questi casi, pur nel rispetto dei diritti degli Utenti, la Fondazione si riserva la facoltà di accedere alle risorse affidate ai medesimi per recuperare le suddette informazioni. Tale accesso potrebbe essere necessario al fine di verificare se vi siano in sospeso attività in carico agli Utenti che, se non portate avanti, possano comportare conseguenze pregiudizievoli per la Fondazione. In ogni caso, prima di attivare la Procedura di accesso in emergenza, la Fondazione cercherà di contattare gli Utenti, in tempi e modi compatibili con le esigenze operative, per notificare a questi ultimi l'intenzione di attivare tale procedura, al fine di consentire loro, ove possibile, di fornire personalmente i dati necessari.

b. Definizioni principali

Nome	Sigla	Descrizione
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.
Sistemi Informatici	S.I.	I sistemi e le dotazioni informatiche e di telecomunicazione di proprietà o nella disponibilità della Fondazione IIT
Verbale di accesso in emergenza ai dati	Verbale	Tracciamento delle informazioni utili relative ad un accesso ai dati in emergenza
Policy	Policy ICT	Stabilire il corretto utilizzo dei Sistemi Informatici nella Fondazione IIT proteggendo IIT e gli Utenti dal rischio di compromissione dei Sistemi Informatici, dalla indebita divulgazione di dati personali e/o riservati, e dalle

relative conseguenze legali, rendendo inoltre più efficace l'utilizzo dei Sistemi Informatici.

3. Principali attori e responsabilità

Attore	Sigla	Maggiori responsabilità
Direzione ICT	ICT	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.
Utente	Utente	Chiunque abbia un rapporto di lavoro dipendente o di collaborazione con la Fondazione e il personale esterno affiliato alla Fondazione IIT che svolge attività di ricerca scientifica, professionale o di studio all'interno delle strutture di IIT. 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.
Amministratore di Sistema	AS	Figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. In ambito informatico vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi. L'Amministratore di Sistema, ai sensi del Provvedimento del Garante per il Trattamento dei dati personali del 27 novembre 2008, è selezionato sulla base dell'esperienza, della capacità e dell'affidabilità.
GARR	GARR	GARR è la rete nazionale a banda ultralarga dedicata alla comunità dell'istruzione e della ricerca. Il suo principale obiettivo è quello di fornire connettività ad alte prestazioni e di sviluppare servizi innovativi per le attività quotidiane di docenti, ricercatori e studenti e per la collaborazione a livello internazionale.

4. Procedura: descrizione

La Procedura di accesso ai dati in emergenza è attivata dal Direttore Scientifico quando ravvisi, anche su segnalazione di altro personale afferente alla Fondazione, la necessità di accedere a dati aziendali gestiti da un Utente assente e non in grado di fornire in autonomia i dati stessi. Potrà quindi affidare in qualsiasi momento il prosieguo delle attività a propri delegati. Il soggetto che prosegue le attività, che sia il Direttore Scientifico o un suo delegato, nel seguito è indicato come "Responsabile dell'accesso".
Il Responsabile dell'accesso, prima di proseguire con la Procedura di accesso ai dati in emergenza, valuta:

- l'effettiva necessità di accedere ai dati in tempi tali da non poter attendere il rientro dell'Utente, in termini di impatti potenziali sulle attività della Fondazione e di complessità nel reperire altrimenti i dati, in particolare gli impatti che l'indisponibilità dei dati potrebbe avere sull'attività della Fondazione, pesandola con gli impatti, comunque limitati, che l'accesso alle aree dati dell'Utente potrebbe avere sulla riservatezza dell'Utente stesso.

Il Responsabile dell'accesso provvede quindi a verificare, nei limiti dei tempi e delle risorse disponibili:

- che i dati non siano in possesso di altri soggetti, quali ad esempio colleghi dell'Utente, che possano renderli disponibili autonomamente: in particolare, l'Utente potrà preventivamente comunicare via mail al proprio Responsabile un proprio collega di riferimento, con il quale verificare la possibilità di raccogliere i dati necessari senza attivare la Procedura di accesso ai dati in emergenza;
- che l'Utente non sia effettivamente in grado di renderli disponibili autonomamente in tempo utile, provando in particolare, nei limiti dei tempi e delle risorse disponibili, a contattare l'Utente attraverso i canali disponibili (ad es. telefono) ed informandolo, se reperibile, dell'intenzione di accedere in emergenza ai dati.

Qualora, al termine di queste verifiche e valutazioni, il Responsabile dell'accesso ritenga necessario l'accesso in emergenza ai dati, provvede ad avviare la procedura e riporta nel Verbale le seguenti informazioni:

- la tipologia di dati a cui è necessario accedere e delle aree in cui verranno cercati (es. posta elettronica, PC, ecc.);
- una valutazione della necessità di effettuare l'accesso e dei possibili impatti sulla Fondazione in caso di mancato accesso;
- una valutazione dei possibili impatti sull'Utente in caso di accesso;
- le azioni che sono state svolte per cercare di reperire altrimenti i dati e per cercare di contattare l'Utente;
- Le modalità in cui si è effettuato il tentativo di prendere contatto con l'Utente e – ove sia andato a buon fine - eventuali obiezioni o considerazioni fatte dall'Utente in merito alla possibilità di un accesso.

Laddove possibile, il Direttore della Direzione ICT identifica preventivamente le modalità di accesso ai diversi Strumenti Informatici (posta elettronica, PC, ecc.) efficaci per garantire la disponibilità dei dati in essi contenuti, che minimizzino l'impatto sulla riservatezza dell'Utente. Laddove le informazioni debbano essere cercate in più Strumenti Informatici dell'Utente, e salvo vi siano ragioni specifiche per un ordine diverso (ad esempio, la probabilità che le informazioni si trovino nell'uno o nell'altro Strumento Informatico), l'ordine preferenziale di ricerca è:

- Storage on premises;
- PC;
- Servizi cloud;
- Posta elettronica.

Il Direttore ICT incarica un Amministratore di Sistema competente per supportare il Responsabile dell'accesso nell'esecuzione della Procedura di accesso ai dati in emergenza, operando sempre alla presenza del Responsabile dell'accesso.
In nessun caso il Responsabile dell'accesso accederà autonomamente ai dati dell'Utente. Le attività dovranno essere svolte in un ambiente adeguatamente riservato, in assenza di estranei all'attività, a tutela della riservatezza dell'Utente.
Nell'effettuare la ricerca, l'Amministratore di Sistema limiterà l'accesso ai dati allo stretto necessario per raggiungere lo scopo dell'attività. Le modalità di ricerca saranno diverse per ciascuno Strumento Informatico. Nel seguito sono descritti i principali.

a. Cartelle su storage on premises

L'Amministratore di Sistema, in presenza del Responsabile dell'accesso, accede alle cartelle su storage on premises utilizzando le proprie credenziali amministrative. Il Responsabile dell'accesso fornisce all'Amministratore di Sistema tutte le informazioni utili ad identificare i dati a cui è necessario accedere (ad esempio, nomi di progetti, nomi di file, date) minimizzando la necessità di accedere ad altri dati. L'Amministratore di Sistema provvederà quindi a cercare i dati, prediligendo modalità di ricerca che riducano l'accesso a dati non pertinenti (ad es. strumenti di ricerca di file, cartelle e contenuti di file basati su parole chiave, anziché sfogliare i contenuti delle cartelle e dei file).

b. Personal Computer

L'Amministratore di Sistema, in presenza del Responsabile dell'accesso, accede al PC dell'Utente utilizzando le proprie credenziali amministrative. Il Responsabile dell'accesso fornisce all'Amministratore di Sistema tutte le informazioni utili ad identificare i dati a cui è necessario accedere (ad esempio, nomi di progetti, nomi di file, date) minimizzando la necessità di accedere ad altri dati. L'Amministratore di Sistema provvederà quindi a cercare i dati, prediligendo modalità di ricerca che riducano l'accesso a dati non pertinenti (ad es. strumenti di ricerca di file, cartelle e contenuti di file basati su parole chiave, anziché sfogliare i contenuti delle cartelle e dei file). Nell'effettuare la ricerca, l'Amministratore di Sistema individuerà le cartelle che, in linea con la Policy ICT, l'Utente avrà reso chiaramente riconoscibili come "ad uso personale", escludendo tali cartelle dalla ricerca.
Qualora l'Amministratore di Sistema non abbia possibilità di accedere attraverso le proprie credenziali amministrative al PC dell'Utente potrà, secondo il caso:
- accedere alla macchina attraverso un disco di boot esterno;
- estrarre il disco per accedervi da un altro PC.

Qualora l'accesso al disco non sia possibile semplicemente con queste modalità, ad esempio perché i dati o il disco sono cifrati, eventuali tentativi di recupero dovranno essere fatti su di una copia dei dati, per non rischiare di danneggiare irrimediabilmente o perdere i dati originali.

c. Servizi in cloud forniti dalla Fondazione

L'Amministratore di Sistema, in presenza del Responsabile dell'accesso, individua la modalità di accesso ai servizi in cloud assegnati all'Utente. Le modalità di accesso potranno variare in funzione del tipo di servizio, e potranno comprendere, se necessario, il reset della password dell'Utente e l'accesso alla relativa casella di posta elettronica, nelle modalità sotto descritte, per prendere visione delle informazioni inviate dal servizio cloud stesso nell'ambito della procedura di reset della password. Eventuali nuove password definite saranno scelte e conservate a cura dell'Amministratore di Sistema, senza darne visione al Responsabile dell'accesso.

Il Responsabile dell'accesso fornisce all'Amministratore di Sistema tutte le informazioni utili ad identificare i dati a cui è necessario accedere (ad esempio, nomi di progetti, nomi di file, date) minimizzando la necessità di accedere ad altri dati. L'Amministratore di Sistema provvederà quindi a cercare i dati, prediligendo modalità di ricerca che riducano l'accesso a dati non pertinenti (ad es. strumenti di ricerca di file, cartelle e contenuti di file basati su parole chiave, anziché sfogliare i contenuti delle cartelle e dei file).

d. Posta elettronica

L'Amministratore di Sistema, in presenza del Responsabile dell'accesso, individua la modalità di accesso alle cartelle di posta elettronica più opportune che consenta una ricerca dei messaggi in base a mittente, destinatario, data, oggetto o testo. Il Responsabile dell'accesso fornirà quindi all'Amministratore di Sistema i parametri in base ai quali effettuare la ricerca, nel modo più preciso e puntuale possibile.
L'Amministratore di Sistema individuerà quindi un insieme di messaggi di posta elettronica corrispondenti ai requisiti indicati, consentendo al Responsabile dell'accesso la visione a video dei parametri (mittente, destinatario, oggetto e data) affinché quest'ultimo gli possa indicare di quali prendere visione al fine di individuare quello o quelli cercati, proseguendo nelle ricerche fino ad individuare i messaggi necessari.

Una volta identificati i dati ricercati, l'Amministratore di Sistema provvederà ad estrarli, ad esempio scaricandoli su una memoria esterna e consegnandola al Responsabile dell'accesso.
Al termine dell'attività, il Responsabile dell'accesso provvederà quindi a scrivere nel Verbale le operazioni svolte e l'elenco dei file estratti con una descrizione dei relativi contenuti. L'Amministratore di Sistema sottoscriverà il Verbale per validazione di quanto dichiarato. Il Verbale, opportunamente sottoscritto dai soggetti coinvolti (cfr. Processo 1 sottoindicato), sarà quindi trasmesso a cura del responsabile dell'accesso alla Direzione Risorse Umane e Organizzazione, dove l'Utente ne potrà in seguito prendere visione.
La Direzione Risorse Umane e Organizzazione provvederà quindi a darne tempestiva comunicazione via email all'Utente, dove saranno indicate le modalità per prendere visione del Verbale.

Processo 1

#	Attività	Funzione	Input/Output
1	Valutazione dell'effettiva necessità d'accesso ai dati in tempi tali da non poter attendere il rientro dell'Utente	Direttore Scientifico	I: Segnalazione di necessità
2	Valutazione della possibilità d'accesso ai dati (tramite collaboratori o attendendo l'Utente)	Responsabile dell'accesso	I: Segnalazione di necessità
3	Redazione del Verbale	Responsabile dell'accesso	O: Verbale bozza
4	Integrazione del Verbale e valutazione dell'opportunità e delle modalità di prosecuzione	Responsabile dell'accesso	I: Verbale bozza O: Verbale integrato
5	Identificazione modalità d'accesso ai sistemi	Direzione ICT (Direttore)	

6	Designazione di un Amministrazione di Sistema	Direzione ICT (Direttore)	
7	Estrazione e consegna i dati ricercati	Direzione ICT (Amministratore di Sistema)	O: estrazione dati ricercati
8	Verbalizzazione e validazione operazioni svolte e dati estratti	Responsabile dell'accesso / Direzione ICT (Amministratore di Sistema)	I: Verbale integrato O: Verbale validato
9	Notifica all'utente e definisce le modalità di visione del Verbale	Direzione Risorse Umane e Organizzazione	

5. Procedura: flow chart