INDICE

1 DEFINIZIONI 2
2 SCOPO 3
3 TERMINI DI VALIDITÀ 3
4 AMBITO DI APPLICAZIONE 3
5 RESPONSABILITÀ 3
6 MODALITÀ OPERATIVE 3
6.1 SICUREZZA FISICA E AMBIENTALE 3
6.2 PROTEZIONE CONTRO SOFTWARE DANNOSI E CODICI AUTOESEGUIBILI 3
6.3 SALVATAGGIO, CONSERVAZIONE E RIPRISTINO DEI DATI 4
6.4 GESTIONE DELLA SICUREZZA DELLA RETE 4
6.5 MONITORAGGIO 4
6.6 GESTIONE PROFILI UTENTI E PASSWORD 4
6.7 CASELLE DI POSTA ELETTRONICA 5
6.8 ACCESSI REMOTI 5
6.9 GESTIONE ACCOUNT E CREDENZIALI DI ACCESSO A SITI DI TERZE PARTI 5
6.10 SICUREZZA DEL SOFTWARE E GESTIONE DEI CAMBIAMENTI 5
6.11 DOCUMENTI CON FIRMA ELETTRONICA O DIGITALE CON FINALITÀ GIURIDICA AVENTI EFFICACIA PROBATORIA 6
7 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA 6

REL.	DATA		REDATTO	APPROVATO	NOTE
1.0	28/10/2013	==		Consiglio di Amministrazione	
2.0	24/02/2022	==		Consiglio di Amministrazione	

1 DEFINIZIONI

Sistema informatico (o «*sistema*»): qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, che consentono l'elaborazione automatica di dati.

Account di rete: credenziale *personale* di accesso alla rete composta da nome utente e dalla relativa password.

Amministratore di sistema: come indicato nel Provvedimento del Garante per la protezione dei dati personali "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Vengono però 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.

Credenziali di accesso: l'insieme degli elementi identificativi di un utente o di un Account di rete (generalmente userID e password).

Dato informatico (o «*dato*»): qualunque rappresentazione di fatti, informazioni o concetti, in forma idonea per l'elaborazione o la conservazione con un sistema informatico, incluso un programma atto a consentire ad un sistema informatico lo svolgimento di funzioni.

Gestione dei permessi o profilazione: definizione, da parte del Responsabile di funzione, delle modalità di accesso (scrittura, lettura, modifica e stampa) ai dati di competenza dell'Unità Organizzativa e indicazione del supporto sul quale le stesse debbano essere gestite e salvate.

Personale Tecnico: Amministratori di sistema, Operatori di sistema, Sistemisti, Sviluppatori di software, tecnici che effettuano manutenzione Hardware e, in generale, tutti coloro che per esigenze di manutenzione, gestione, monitoraggio e implementazione, operano sul sistema informatico.

Postazione di Lavoro: postazione informatica aziendale fissa oppure mobile in grado di trattare informazioni aziendali.

Server: elaboratore dedicato alla fornitura di risorse e servizi per altri computer, detti "*client*", connessi fisicamente tra loro in *rete*. Detto server può essere fisico (in Azienda), virtualizzato (tecnica informatica) in Azienda o in remoto (su cloud o nuvola, in hosting, in housing, …).

Servizi di rete: servizi forniti dai server: la posta elettronica interna ed esterna, la navigazione Internet e Intranet, le cartelle condivise, le stampanti condivise, gli applicativi aziendali.

Sistema informatico: (o «*sistema*»): qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, che consentono l'elaborazione automatica di dati.

Spamming: l'invio di messaggi indesiderati (generalmente commerciali).

Virus: software, appartenente alla categoria dei malware, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di se stesso, generalmente senza farsi rilevare dall'utente.

2 SCOPO

Il Protocollo definisce, nell'ambito dell'attività svolta da Fondazione Maddalena Grassi (di seguito «*FMG*» o «*Fondazione*»), le responsabilità, le modalità operative ed i flussi informativi verso l'Organismo di Vigilanza a cui devono attenersi i Destinatari, così come individuati nella Parte Generale del Modello Organizzativo, nella gestione e nell'utilizzo dei Sistemi Informativi (di seguito più brevemente anche solo «*Destinatari*»).

3 TERMINI DI VALIDITÀ

Il Protocollo assume validità dalla data della sua emissione indicata in copertina.

Ogni eventuale successivo aggiornamento annulla e sostituisce, dalla data della sua emissione, tutte le versioni emesse precedentemente.

4 AMBITO DI APPLICAZIONE

Il Protocollo si applica, per i rispettivi ambiti di competenza, a tutti coloro che utilizzano (anche «*utenti*» o «*utilizzatori*»), gestiscono (anche «*Personale Tecnico*») o comunque abbiano accesso ai sistemi e/o ai dati informatici aziendali, ivi inclusi persone ed enti esterni o fornitori terzi.

In particolare, nei rapporti contrattuali con questi ultimi, sono formulate specifiche clausole di garanzia volte ad assicurare nello sviluppo, esercizio e manutenzione di sistemi informatici, l'aderenza ai principi ed agli aspetti procedurali descritti nel § 6. *Modalità Operative*.

Per gli aspetti non previsti nel Protocollo si fa riferimento al *Regolamento per l'utilizzo dei sistemi informatici* a cui si rimanda.

5 RESPONSABILITÀ

La Responsabilità funzionale è assegnata al Direttore Amministrativo che si avvale del supporto operativo del Responsabile sviluppo informatico dell'assistenza domiciliare integrata e dei Consulenti esterni / Personale Tecnico per gli aspetti legati all'hardware e ad altro software.

Il Direttore Amministrativo, con il supporto del Responsabile sviluppo informatico dell'assistenza domiciliare integrata e delle altre Funzioni eventualmente interessate, è responsabile di effettuare un adeguato monitoraggio, anche sull'attività dei fornitori, per verificare il rispetto di tali obbligazioni.

6 MODALITÀ OPERATIVE

6.1 SICUREZZA FISICA E AMBIENTALE

I server sono collocati sia presso le sedi aziendali (uffici di Milano e strutture) sia presso fornitori esterni. I centri di elaborazione dati e i server ivi contenuti sono sottoposti a apposite misure di protezione fisica e logica. I server della sede di Milano sono protetti da gruppi di continuità.

6.2 PROTEZIONE CONTRO SOFTWARE DANNOSI E CODICI AUTOESEGUIBILI

Tutti i computer e i server devono essere dotati di idonei programmi antivirus, costantemente aggiornati.

Il Direttore Amministrativo, con il supporto del Personale Tecnico, deve, inoltre, assicurarsi che i computer delle Società esterne, qualora interagiscano con il sistema informativo aziendale, siano dotati di adeguate misure di protezione antivirus.

Per tutti i computer e i server è prevista l'attuazione di tutti gli aggiornamenti (patch) dei sistemi operativi e degli applicativi suggeriti dai produttori al fine di limitare i possibili rischi legati a vulnerabilità riscontrate negli stessi. L'installazione degli aggiornamenti segue un piano di diffusione progressiva, volto a prevenire e mitigare la possibilità di impatti negativi sulla stabilità dei sistemi di destinazione.

6.3 SALVATAGGIO, CONSERVAZIONE E RIPRISTINO DEI DATI

I backup, per tutti i dati memorizzati sui server, devono essere effettuati quotidianamente secondo le modalità atte ad assicurare che i dati possano essere recuperati a fronte di:

- errori degli utenti o del Personale Tecnico;
- incidenti e guasti ai sistemi di memorizzazione;
- errori nelle procedure informatiche;
- errori conseguenti a messa in produzione di modifiche;
- altre possibili cause di alterazione dei dati (intrusioni, sabotaggio, ecc.).

Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, …), contenenti dati o informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il Direttore Amministrativo e seguire le istruzioni da questo impartite.

I Destinatari sono responsabili della custodia dei supporti e dei dati aziendali in essi contenuti.

6.4 GESTIONE DELLA SICUREZZA DELLA RETE

L'architettura di sicurezza prevede un firewall, in modo da assicurare la creazione di diversi strati di sicurezza perimetrale. Il controllo del firewall è effettuato bloccando ogni accesso dalla rete Internet verso la rete aziendale, salvo eccezioni puntuali dovute a specifiche esigenze. Il sistema prevede un filtro non consentendo l'accesso a messenger e ai social network e bloccando l'accesso ad alcuni siti in relazione al contenuto ("Content Filter").

L'efficacia dei sistemi firewall deve essere verificata prima del rilascio in esercizio degli stessi e costantemente aggiornata.

6.5 MONITORAGGIO

Il monitoraggio della rete è attuato tramite controlli manuali sui sistemi firewall per verificare eventuali violazioni o anomalie che possano comportare problematiche ai sistemi e alla loro sicurezza.

6.6 GESTIONE PROFILI UTENTI E PASSWORD

Gli accessi alla rete, alle applicazioni e ai dati aziendali devono avvenire in modo controllato con identificazione certa e univoca dell'utente mediante credenziali, nonché profilazione dello stesso atta a definire i diritti di accesso e le operazioni alle quali è abilitato. L'assegnazione delle utenze a dipendenti / collaboratori e la relativa profilazione deve essere basata su principi di necessità in modo da attribuire solo le autorizzazioni atte ad eseguire i compiti aziendali di

competenza dell'utente in questione e solo per il tempo richiesto per svolgere l'attività concordata.

Per il gestionale è previsto un accesso web https con credenziali di autenticazione diverse rispetto a quelle utilizzate per l'accesso alla rete della Fondazione. Anche l'accesso al sistema della ASL (Adweb) è previsto tramite web.

Ciascun Destinatario è responsabile della generazione e conservazione delle password.

L'autorizzazione di un collaboratore all'utilizzo della rete internet (così come la cessazione) deve essere notificata dal Direttore Amministrativo e al Personale Tecnico attraverso una comunicazione interna (e-mail), che abbia in copia il Responsabile della Funzione interessata.

6.7 CASELLE DI POSTA ELETTRONICA

Gli utenti della Fondazione sono dotati di un account di dominio che permette l'accesso alla rete aziendale ed a specifiche applicazioni (per le quali è necessaria un'ulteriore profilazione dedicata). Le mail di gruppo non nominative sono riconducibili agli utenti a cui è consentito l'accesso ed all'utilizzatore di ogni singola attività.

Per un corretto uso della posta elettronica:

- i Destinatari non possono scaricare su disco, allegati di posta elettronica di cui non si conosca con certezza il mittente o sulla sicurezza dei quali si nutrono, dubbi, anche minimi;
- i Destinatari non possono rispondere a messaggi apparentemente provenienti da mittenti considerati "sicuri" (es. bollettini tecnici della Microsoft, …) e soprattutto non fornire alcun dato personale richiesto all'interno di queste e-mail né, tantomeno, collegarsi ad eventuali siti Internet proposti nel messaggio.
- in tutte le situazioni sopra descritte, nel caso sussista qualche dubbio su come gestire il messaggio, si ricorda di non aprire né il messaggio né l'eventuale allegato, e contattare il Personale Tecnico;
- è fatto esplicito divieto di attivare o diffondere messaggi di tipo "catene di S. Antonio", così come di trasmettere materiale diffamatorio, osceno o che violi il diritto d'autore.

6.8 ACCESSI REMOTI

Il Responsabile di Funzione, a fronte di specifiche esigenze e dietro motivata richiesta, può autorizzare l'accesso da remoto ai sistemi e ai dati informatici aziendali.

Le richieste dovranno essere formulate per iscritto, autorizzate ed archiviate dal Direttore Amministrativo, restando in carico al Responsabile di Funzione, l'obbligo di comunicare con tempestività la cessazione dello stato di necessità o del rapporto di collaborazione.

6.9 GESTIONE ACCOUNT E CREDENZIALI DI ACCESSO A SITI DI TERZE PARTI

La gestione di account e credenziali per l'accesso a siti di terze parti necessita dell'autorizzazione del Direttore Amministrativo che valida l'abilitazione dell'account necessario e verifica che sia utilizzato in conformità con le direttive aziendali e le norme e regolamenti della terza parte che eroga il servizio.

6.10 SICUREZZA DEL SOFTWARE E GESTIONE DEI CAMBIAMENTI

I sistemi applicativi e le infrastrutture hardware in uso alla Fondazione non possono essere manomessi o modificati autonomamente dall'utente finale. La gestione dei cambiamenti

software si riferisce a nuove implementazioni o a modifiche di applicazioni informatiche che gestiscono le basi dati aziendali. La gestione dei cambiamenti hardware riguarda gli interventi sui server e sulle reti informatiche aziendali.

Il Direttore Amministrativo, con il supporto del Responsabile sviluppo informatico dell'assistenza domiciliare integrata e del Personale Tecnico per i rispettivi ambiti di competenza, garantisce un costante aggiornamento dei software ed hardware in uso alla Fondazione al fine di preservare un livello di efficienza e sicurezza adeguato alle necessità operative.

Eventuali ulteriori e specifiche esigenze di modifica o aggiornamento, dovranno essere formulate dal Responsabile della Funzione interessata al Direttore Amministrativo per il benestare che provvederà ad attivare per l'operatività il Personale Tecnico.

È vietato il trasferimento di software aziendale su hardware non autorizzato, salvo i casi consentiti dalle licenze utilizzate.

6.11 DOCUMENTI CON FIRMA ELETTRONICA O DIGITALE CON FINALITÀ GIURIDICA AVENTI EFFICACIA PROBATORIA

La gestione di documenti con firma qualificata o digitale (a titolo esemplificativo, ma non esaustivo, Smart card, generatori di numeri pseudocasuali, posta elettronica certificata, ecc.) con finalità giuridica aventi efficacia probatoria è in carico ai Responsabili di Funzione, fermo restando l'obbligo di autorizzazione da parte del Direttore Amministrativo, al possesso della firma stessa.

7 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

I Flussi Informativi sono definiti nell'Allegato "*Elenco Flussi Informativi verso l'Organismo di Vigilanza*" e devono essere trasmessi all'Organismo di Vigilanza della Fondazione agli indirizzi in seguito indicati.

Organismo di Vigilanza di Fondazione Maddalena Grassi	
Posta elettronica (E-mail)	Indirizzo e-mail: odv@fondazionemaddalenagrassi.it
Posta fisica	Posta fisica: Via Giovanni Prati n. 4, Milano – 20145 (MI) (all'attenzione dell'Organismo di Vigilanza).