Fondazione
"Villa della Fraternità – ONLUS"
Centro Residenziale per Anziani
Centro di Riabilitazione, Diagnosi e Terapia
"Nuova Calabria"
Sant'Andrea Hospice

Politica di utilizzo corretto delle strutture e delle risorse tecnologiche IS02

Documento rif:	Politica di utilizzo corretto delle strutture e delle risorse tecnologiche IS02
Versione:	1
Data della versione:	25/05/2018
Autore:	Fondazione Villa della Fraternita' Onlus
Approvato da:	Fondazione Villa della fraternità Onlus – Voci Maria Caterina
Livello di riservatezza:	Controllato

Lista di distribuzione

Questo documento viene controllato e mantenuto sul server in sola lettura. Il rappresentante per la gestione della sicurezza delle informazioni deve garantire che tutte le modifiche siano diffuse e che le copie obsolete siano rimosse e archiviate. Le copie cartacee utilizzate per l'addestramento e l'auditing interno sono controllate e distribuite come segue.

Copia n. 1 **Titolare**

Copia n. 2 **Rappresentante della gestione della sicurezza delle informazioni**

Cronologia modifiche

Il presente documento viene riesaminato periodicamente, almeno una volta all'anno, e viene conservato per un periodo di cinque anni. Le modifiche e le revisioni sono distribuite ai titolari citati. La cronistoria delle modifiche e delle revisioni sono riportate di seguito.

Data	Modificare. No.	Pagina n.	Nuovo numero	Motivo del cambiamento	Autorizzato da
25/05/2018	-	Tutti	1	Rilascio iniziale.	AS
	1		2		
	2		3		
	3		4		
	4		5		
	5		6		
	6		7		
	7		8		
	8		9		
	9		10		
	10		11		
	11		12		
	12		13		
	13		14		
	14		15		
	15		16		
	16		17		

Sommario

0. Controlli applicati

Rif. controllo	Titolo
A.7.2.2	Consapevolezza, Sensibilizzazione, istruzione e formazione in materia di sicurezza dell'informazione
A.7.2.3	Procedimento disciplinare
A.8.1.3	Utilizzo accettabile degli asset
A.9.3.1	Utilizzo di informazioni di autenticazione segrete
A.11.2.8	Apparecchiature incostudite degli utenti
A.11.2.9	Politica di schermo e scrivania puliti
A.12.1.1	Procedure operative documentate
A.12.5.1	Installazione di software su sistemi operativi
A.16.1.2	Segnalazione di eventi relativi alla sicurezza delle informazioni
A.16.1.3	Segnalazione dei punti di debolezza relativi alla sicurezza delle informazioni

1. Introduzione

La società fornisce molti servizi essenziali e funzioni aziendali che si basano su risorse tecnologiche ITC. L'utilizzo delle risorse ITC deve essere in linea con le buone pratiche e procedure di lavoro professionali e deve garantire la sicurezza e l'integrità di tutte le informazioni e i dati aziendali.

2. Scopo

Lo scopo di questa procedura è quello di stabilire come devono essere utilizzate le strutture e le risorse ITC.

3. Ambito di applicazione

L'ambito di applicazione di questa procedura si estende a tutti i reparti, dipendenti, consulenti, appaltatori, fornitori che utilizzano/accedono alle strutture ITC .

4. Principi fondamentali

4.1 Uso del computer

Gli utenti dei computer devono assicurarsi in ogni momento che:

- Sia stato autorizzato l'utilizzo delle strutture ITC con username e password di dominio forniti dalla Direzione IT.
- Le password di accesso all'account dell'utente e del sistema sono private e non vengono condivise, visualizzate o comunicate a chiunque non abbia un diritto legittimo su tali informazioni.
- Le informazioni e i dati non vengano salvati in modo permanente sui dischi rigidi del PC; in caso di indisponibilità della rete, rivolgersi al reparto IT.
- I dati sensibili e personali non vengono salvati consapevolmente sul disco rigido del PC in nessuna circostanza.

- I dati e le informazioni salvati su dispositivi portatili tramite PC vengono copiati solo su un dispositivo portatile approvato e crittografato in conformità ai criteri di crittografia IS07.

  N.B. - I dispositivi informatici mobili come fotocamere digitali e dispositivi di dettatura digitali, ecc., non devono essere trattati come dispositivi di memorizzazione dei dati, le foto/file audio possano essere classificati come dati e tutte le foto/file audio scattati devono pertanto essere rimossi dai dispositivi e memorizzati sulla rete il più presto possibile.

- I monitor dei pc vengono bloccati dagli utenti quando sono lontani dal computer.
- Le apparecchiature informatiche, come i desktop, (ad eccezione dei laptop e dei dispositivi mobili autorizzati all'uso) non vengono rimosse dalla loro sede senza la gestione della linea e/o l'approvazione del dipartimento IT.
- Le apparecchiature non autorizzate e non standard non sono collegate o inserite nel computer.
- Il software non viene installato da personale non autorizzato (l'accesso autorizzato può includere compiti specifici che richiedono l'accesso amministrativo del personale per svolgere determinate funzioni lavorative) - qualsiasi software installato deve essere (o essere) inserito nell'elenco dei software approvati.
- L'attrezzatura ITC non deve essere utilizzata per memorizzare dati personali come foto di matrimoni, CV, file musicali, ecc.
- I computer non vengono maneggiati in modo scorretto, danneggiati intenzionalmente o manomessi in alcun modo, ad esempio togliendo il coperchio della custodia del PC/laptop o rimuovendo viti o fissaggi.
- Qualsiasi dispositivo sospetto o sconosciuto vicino o vicino a PC/laptop è segnalato al reparto IT.
- I computer vengono disconnessi e spenti quando non vengono utilizzati per periodi prolungati (ad esempio durante la notte) e i monitor vengono spenti.

4.2 Utilizzo di Internet e della posta elettronica

Internet

- L'uso personale di Internet è consentito, ma non durante l'orario di lavoro. È possibile utilizzare Internet prima di iniziare a lavorare, durante il pranzo o dopo il lavoro.
- Non è consentito utilizzare Internet o i sistemi di posta elettronica della società per scopi commerciali o personali.
- Se si utilizza Internet per scopi non lavorativi, la Fondazione non si assume alcuna responsabilità per il mancato pagamento o per la sicurezza delle informazioni personali fornite.
- Le merci acquistate per scopi non lavorativi, non devono essere consegnate presso gli uffici della società.
- Il download di video, file musicali, giochi, file software e altri programmi per computer - per scopi non lavorativi - è severamente proibito. Questi tipi di file consumano grandi quantità di spazio di archiviazione sul sistema (e possono rallentarlo notevolmente) e possono violare le leggi sul copyright.

Molti siti Internet che contengono contenuti inaccettabili vengono bloccati automaticamente dai sistemi della Fondazione, tuttavia, non è possibile bloccare elettronicamente tutti i siti "inaccettabili". Pertanto, non è consentito visualizzare, copiare o diffondere deliberatamente alcun materiale che:

- E' sessualmente esplicito o osceno.

- E' razzista, sessista, omofobo, molesto o in qualsiasi altro modo discriminatorio o offensivo.
- Contiene materiale il cui possesso costituirebbe un reato penale.
- Promuove qualsiasi forma di attività criminale.
- Contiene immagini, cartoni animati o barzellette che causano offesa.

La direzione della Fondazione registra i dettagli di tutto il traffico Internet. Questo per proteggere l'azienda e i suoi dipendenti da violazioni della sicurezza, incluso l'hacking, e per garantire che non vengano visitati siti "inaccettabili".

Email

Ove possibile, l'uso personale della posta elettronica dovrebbe avvenire nel proprio tempo libero; è consentito un uso personale limitato della posta elettronica durante la giornata lavorativa, ma dovrebbe essere limitato a un totale di non più di pochi minuti per rispondere a e-mail personali urgenti in entrata.

L'uso personale non deve in alcun modo distrarre il personale dall'efficace svolgimento delle sue mansioni.
L'uso eccessivo non è consentito e può comportare azioni disciplinari, tra cui la perdita dell'accesso a Internet e alla posta elettronica.

Non è consentito utilizzare il sistema di posta elettronica in modo offensivo. È vietato visualizzare, copiare o diffondere deliberatamente qualsiasi materiale che:

- E' sessualmente esplicito o osceno
- È razzista, sessista, omofobo, molesto o in qualsiasi altro modo discriminatorio o offensivo
- Contiene materiale il cui possesso costituirebbe un reato penale
- Promuove qualsiasi forma di attività criminale
- Contiene proposte indesiderate
- Contiene immagini, cartoni animati o barzellette che causano offesa
- Sembra essere una lettera a catena

Maggiori informazioni sono disponibili in IS12 Politica di Utilizzo di Internet e della Posta Elettronica.

La Fondazione produce regolarmente informazioni di monitoraggio che riassumono l'utilizzo della posta elettronica e possono condurre a ulteriori indagini.

4.3 Sicurezza

I sistemi informatici sono continuamente minacciati da hacker, infezioni da virus/malware, furto di dati e apparecchiature. La direzione della Fondazione deve, pertanto, rimanere vigile in ogni momento al fine di salvaguardare le informazioni e i dati e per proteggere la sicurezza e l'integrità di tutti i sistemi ITC.
Gli utenti di tutti i computer e dispositivi devono assicurarsi che ciò avvenga e per tale ragione:

- I computer e i dispositivi non devono essere consegnati a persone non autorizzate per ragioni di sicurezza.
- I computer e i dispositivi non devoni essere abbandonati o lasciati incustoditi in luoghi pubblici.

- Tutti i dispositivi informatici mobili portatili e le altre apparecchiature IT non devono mai essere lasciati incustoditi a bordo di un veicolo.
- I computer e i dispositivi devono essere adeguatamente protetti da danni fisici.
- I computer e i dispositivi non devono essere noleggiati, prestati o ceduti senza l'autorizzazione del dipartimento IT.
- Tutti i computer/dispositivi che non sono più necessari o che hanno raggiunto la fine della vita utile devono essere restituiti alla Direzione per essere smaltiti in conformità alla norma IS27 Smaltimento delle apparecchiature TIC.

4.4 Antivirus

Qualsiasi avviso visibile sullo schermo dal software antivirus/antimalware in merito a minacce identificate/rilevate da virus/malware deve essere immediatamente segnalato allla Direzione Amministrativa.

4.5 Dispositivi personali

I dispositivi personali che non sono di proprietà della Fondazione, compresi telefoni cellulari, palmari, penne digitali, ecc., non devono essere utilizzati per registrare o acquisire informazioni relative all'attività della Fondazione e ai suoi servizi.

5. Violazioni della policy

Le violazioni della presente procedura e/o gli incidenti di sicurezza possono essere definiti come eventi che potrebbero avere, o hanno avuto come conseguenza, perdite o danni alle attività della Fondazione, o come eventi che violano le procedure e le politiche di sicurezza della società.

Tutti i dipendenti, i collaboratori, i partner, i contraenti e i fornitori hanno la responsabilità di segnalare incidenti di sicurezza e violazioni di questa procedura il più presto possibile attraverso la Procedura di segnalazione e gestione degli incidenti IS31. Tale obbligo si estende anche a qualsiasi organizzazione esterna incaricata di supportare o accedere ai sistemi informativi della Fondazione.

La Fondazione adotterà misure appropriate per porre rimedio a qualsiasi violazione della politica e delle relative procedure e linee guida attraverso i relativi quadri normativi in vigore. Nel caso di una persona, la questione può essere trattata nell'ambito del procedimento disciplinare.

Per ulteriori informazioni, vedere la procedura denominata: "Politica di gestione degli incidenti di sicurezza IS20".

Tutti gli utenti delle strutture ITC devono conformarsi a questa procedura e rispettare la procedura denominata: "Politica di sicurezza ITC IS08".

6. Documentazione e registri associati

Nome documento/registrazione	Posizione di stoccaggio	Proprietario	Controllo della protezione	Programma di ritenzione
Criteri di crittografia IS07		Nome 2	Controllato: Accesso protetto da password	Tempo
Politica di sicurezza TIC IS08		Fondazione Villa della Fraternità Onlus	Controllato: Accesso protetto da password	Tempo
Politica di utilizzo accettabile di Internet e della posta elettronica IS12		Fondazione Villa della Fraternità Onlus	Controllato: Accesso protetto da password	Tempo
Politica di gestione degli incidenti di sicurezza IS20		Fondazione Villa della Fraternità Onlus	Controllato: Accesso protetto da password	Tempo
IS27 Smaltimento di apparecchiature ITC		Fondazione Villa della Fraternità Onlus	Controllato: Accesso protetto da password	Tempo

7. Gestione Documentale

Il presente documento è valido a partire dal 25/05/2018.

Il presente documento viene periodicamente e comunque con cadenza almeno annuale al fine di garantire il rispetto dei seguenti criteri previsti.

- Conformità ai requisiti Reg.UE 2016/679 e D.lgs 101/2018
- Requisiti legislativi definiti dalla legge, se del caso

IL Presidente e LR

_____

Firma