NATURA ED OBIETTIVI DELLA POLITICA DELLA FONDAZIONE PER LA SICUREZZA DELLE INFORMAZIONI

La presente Politica per la Sicurezza delle Informazioni riguarda i dati personali (attuali o futuri) relativi alle attività di assistenza ai rifugiati svolte dalla **FONDAZIONE CITTÀ DELLA PACE**.

Per "dati personali" si intendono tutte quelle informazioni relative ad un soggetto identificato o identificabile che siano state in qualsiasi modo registrate.

RACCOLTA DELLE INFORMAZIONI

Tipologia e fonti delle informazioni raccolte

Le informazioni non personali sono dati relativi a operazioni d'uso e servizio che non sono direttamente associate a una specifica identità personale. La **FONDAZIONE CITTÀ DELLA PACE** può raccogliere e analizzare informazioni non personali per analizzare le modalità d'uso del suo sito Web da parte dei visitatori. Nel corso normale della propria attività di assistenza la **FONDAZIONE CITTÀ DELLA PACE** può raccogliere i dati personali relativi ai propri FORNITORI, LAVORATORI, VOLONTARI ed in parte dei RIFUGIATI. Tali dati comprendono:

- Le informazioni quali: nome, cognome del rifugiato, data e luogo di nascita del rifugiato, Paese di provenienza, informazione sui programmi di aiuto a cui è sottoposto, Associazioni/Enti che lo assistono;
- Le informazioni quali: nome, indirizzo del fornitore, datore di lavoro, numero di telefono del fornitore, numero di fax del fornitore, indirizzo e-mail, data e luogo di nascita del datore di lavoro;
- Le informazioni quali: nome, indirizzo del lavoratore, numero di identificazione del dipendente, numero di telefono del lavoratore, indirizzo e-mail del lavoratore, data e luogo di nascita del dipendente;
- Le informazioni quali: nome, indirizzo del volontario, numero di identificazione del volontario, numero di telefono, numero di fax, indirizzo e-mail del volontario, data e luogo di nascita del volontario.

CONSERVAZIONE DELLE INFORMAZIONI

Le informazioni personali relative ai fornitori, lavoratori, volontari e rifugiati della **FONDAZIONE CITTÀ DELLA PACE** vengono conservate finché si ritiene che possano essere utili, ma non per un periodo superiore a quello consentito dalla Normativa Vigente.

SICUREZZA DELLE INFORMAZIONI

La **FONDAZIONE CITTÀ DELLA PACE** adotta adeguate misure di salvaguardia fisica, elettronica e procedurale per proteggere le informazioni personali da:

- PERDITA;
- USO ILLEGITTIMO;
- ACCESSO NON AUTORIZZATO;
- DIVULGAZIONE;
- ALTERAZIONE E DISTRUZIONE.

Nell'ambito di tali precauzioni, la fondazione cerca di tutelare i dati personali tramite sistemi tecnologici progettati per salvaguardare le informazioni durante la trasmissione. L'accesso ai dati personali è limitato a quei dipendenti che a proprio parere hanno necessità di conoscere tali informazioni, per consentire alla fondazione e ai collaboratori di fornire i servizi di assistenza richiesti.

La **FONDAZIONE CITTÀ DELLA PACE** ha adottato una politica di condotta secondo la quale l'uso illegittimo delle informazioni personali da parte dei dipendenti e dei collaboratori è considerato una grave trasgressione, contro cui può essere avviata una procedura disciplinare. Va tuttavia sottolineato che non esistono metodi di trasmissione o archiviazione dei dati totalmente sicuri. Seppur dotati di caratteristiche diverse, i vari tipi di comunicazione delle informazioni, tra cui il servizio postale, le chiamate telefoniche, i fax e le trasmissioni via Internet, presentano tutti possibilità di perdita, errato smistamento, intercettazione ed uso illegittimo dei dati trasmessi.

Quando la **FONDAZIONE CITTÀ DELLA PACE** decide quali dati richiedere o inviare o come reperirli o comunicarli, si cerca di farlo conservando un giusto equilibrio tra la sicurezza dei dati e una modalità che sia conveniente per tutti. Questo perché si ritiene che i lavoratori, i collaboratori, i volontari, i fornitori di beni e servizi ed assistiti diano importanza ad entrambi gli aspetti. Di conseguenza, talvolta si utilizza un metodo di comunicazione meno sicuro rispetto ad altri metodi che comunque risulterebbero meno convenienti. Un esempio rilevante al riguardo è rappresentato dalla posta elettronica. Quando si invia un messaggio e-mail, lo si invia in formato non crittografato, perché si ritiene che i fornitori, i collaboratori, i volontari non siano attualmente in grado di ricevere messaggi e-mail crittografati. Pertanto, se il messaggio e-mail non crittografato che viene inviato andasse smarrito o fosse intercettato, potrebbe essere letto più facilmente di uno crittografato. Per tutelare efficacemente i dati personali dei rifugiati, dei fornitori, dei volontari, dei dipendenti o collaboratori si ha bisogno della collaborazione di tutti.

GESTIONE DEGLI INCIDENTI INFORMATICI

Quando viene rilevata un'anomalia, un bug o un incidente viene contattato l'AMM della **FONDAZIONE CITTÀ DELLA PACE** e notificato l'evento a tutti gli addetti accreditati per il progetto/archivio oggetto di segnalazione.

L'RSSI della **FONDAZIONE CITTÀ DELLA PACE** provvede a valutare la classificazione di gravità della segnalazione secondo le seguenti modalità:

- Se la segnalazione riguarda incidenti relativi alla Sicurezza delle informazioni o alla continuità operativa, l'RSSI provvede all'immediato trattamento registrandolo nel registro degli incidenti e valuta in base alla gravità l'attivazione di uno dei Piani presenti nel documento “Piani per la continuità operativa e gestione degli incidenti”.
- Se le segnalazioni riguardano possibili violazioni della sicurezza l'RSSI provvede all'immediato trattamento ed alla registrazione dell'evento nel registro degli incidenti

L'incidente viene descritto nel “Registro delle NC” dal RSSI specificando il trattamento e le eventuali AC a seguire, in conformità a quanto stabilito dalla PG “Gestione delle NC, AC, AP “.

UTILIZZO DELLE INFORMAZIONI

Le informazioni personali possono essere utilizzate dalla **FONDAZIONE CITTÀ DELLA PACE** per varie finalità.

Ad esempio, per fornire l'assistenza ai rifugiati, per preparare gli estratti-conto dei dipendenti, per pagare le fatture dei fornitori di beni e servizi per contattare i volontari ecc. È possibile che per questi servizi vengano utilizzati consulenti esterni.

La comunicazione delle informazioni potrebbe inoltre avvenire in risposta a richieste di Organi Giudiziari o Amministrativi.

Quando vengono comunicate le informazioni personali dei fornitori, degli assistiti, dei dipendenti o collaboratori, dei volontari a terzi, la conservazione e l'utilizzo (compresa la comunicazione) dei dati sono soggetti alla politica di tutela della privacy dei summenzionati terzi, e non a quella della **FONDAZIONE CITTÀ DELLA PACE**.

La fondazione può utilizzare e comunicare le informazioni personali, quando ritiene a ragione che sia necessario tutelare la propria attività; per ottemperare alla vigente legislazione; per tutelare i diritti, la privacy, la sicurezza; per attuare i rimedi disponibili o limitare i danni che potrebbe subire.

Ad esempio, qualora un assistito infrangesse le regole previste è possibile usare, comunicare a terzi o divulgare pubblicamente i dati personali relativi a tale assistito entro i limiti consentiti dalla legge. È possibile comunicare i dati personali agli organi giudiziari per assisterli nell'identificazione di soggetti che siano stati o possano essere coinvolti in attività illecite.

Comunicazione ai volontari ed ai collaboratori nei servizi di assistenza ai rifugiati.
La **FONDAZIONE CITTÀ DELLA PACE** può comunicare informazioni personali di cui è in possesso a qualunque individuo o Ente/Associazione che la aiuta nella conduzione delle attività assistenziali, compresi individui o Enti/Associazioni che forniscono servizi di assistenza per suo conto, ma soltanto se quell'individuo o quell'Ente/Associazione acconsente ad usare i dati personali unicamente per svolgere i compiti che gli sono stati assegnati in base alle istruzioni che la Fondazione gli ha fornito e ad osservare le disposizioni della propria Politica Aziendale per la Sicurezza delle Informazioni.

Uso di informazioni ricevute da altri. La **FONDAZIONE CITTÀ DELLA PACE** può ottenere dei dati personali dai propri collaboratori nei servizi di assistenza ai rifugiati, dai volontari e da altri Enti/Associazioni con i quali intrattiene relazioni. Tali informazioni possono essere abbinate ai dati personali da essa raccolti in precedenza o utilizzate per renderli più significativi, in conformità con la legislazione vigente e la Politica Aziendale per la Sicurezza delle Informazioni.

INFORMAZIONI SENSIBILI

Talvolta la **FONDAZIONE CITTÀ DELLA PACE** nell'ambito dello svolgimento della propria attività di assistenza potrebbe venire in possesso di dati sullo stato di salute, opinioni su convinzioni religiose su eventuali precedenti penali del rifugiato. In questo caso tali informazioni non vengono condivise con i volontari e/o con i collaboratori se non Autorizzati dagli Organi preposti e seguendo quanto stabilito dalla vigente legislazione.
La fondazione potrebbe anche ottenere informazioni sull'appartenenza di un lavoratore ad un sindacato o ad altra organizzazione analoga.
La **FONDAZIONE CITTÀ DELLA PACE** non comunica informazioni sull'appartenenza sindacale dei propri dipendenti, collaboratori o volontari a terzi, se non nei casi previsti dalla vigente legislazione.

FORMAZIONE DEGLI ADDETTI DELLA FONDAZIONE

Gli addetti della **FONDAZIONE CITTÀ DELLA PACE**, nel corso dell'anno, effettuano almeno 2 ore di formazione al fine di mantenere aggiornate le proprie conoscenze:

- Sulle Politiche relative alla sicurezza delle informazioni applicate;
- Sui compiti assegnati agli Incaricati al trattamento dei dati.

Le tematiche trattate si possono riassumere in:

- Compiti spettanti in funzione del proprio incarico e ruolo;
- Modalità di Gestione e Sicurezza delle informazioni degli archivi gestiti.

La definizione delle necessità di addestramento, la pianificazione dei corsi e delle modalità di svolgimento, la registrazione della frequenza ai corsi e dell'efficacia è gestita e controllata dal RSSI.

UTILIZZO DEI PC AZIENDALI DA PARTE DEGLI ADDETTI

Il PC aziendale è uno strumento di lavoro messo a disposizione del lavoratore della **FONDAZIONE CITTÀ DELLA PACE** per permettergli di adempiere ai suoi compiti lavorativi. Ogni lavoratore responsabile di una postazione di lavoro informatica deve usare la diligenza del "buon padre di famiglia" nella custodia e gestione della stessa. In particolare:

- Al termine della giornata lavorativa è tenuto a spegnere la postazione per mezzo della funzione prevista dal sistema operativo per lo spegnimento e non lasciare sulla scrivania materiale cartaceo o supporti removibili;
- In caso di allontanamento dalla postazione per più di 5 minuti è tenuto ad impostare il blocca sessione;
- Gli utenti non devono avere cartelle condivise in rete sulla propria postazione di lavoro;
- Gli utenti devono evitare di avere materiale aziendale (i.e.: documenti, ecc) sulle proprie postazioni di lavoro. In via eccezionale, nel caso di custodia di dati aziendali sulla propria postazione devono informare di ciò l'AMS e devono salvare tutto all'interno della propria cartella documenti. È preferibile, comunque, l'utilizzo delle apposite aree di memorizzazione sullo storage centralizzato aziendale;
- Gli utenti devono evitare di lasciare documenti cartacei di progetto incustoditi sulla propria scrivania,
- È vietato tassativamente l'uso delle porte USB in lettura e scrittura e la lettura di floppy disk;

UTILIZZO DELL'EMAIL DA PARTE DEGLI ADDETTI

La **FONDAZIONE CITTÀ DELLA PACE** gestisce il servizio di posta elettronica all'interno del perimetro applicativo del SGSI "Sistema di Gestione per la Sicurezza delle Informazioni". Le email aziendali sono sottoposte a custodia in un archivio centralizzato nella sala server aziendale. Gli utenti possono accedere alla propria casella di posta elettronica solo dall'interno della **FONDAZIONE CITTÀ DELLA PACE** L'email aziendale deve essere usata esclusivamente per obbiettivi lavorativi.

- Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, e dunque, non deve essere usata per inviare informazioni, dati o documenti di lavoro "strettamente Riservati";
- Non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum o mail-list; solo in questo ultimo caso è possibile, previa autorizzazione per la verifica della validità dell'emittente, iscriversi a servizi di informazione strettamente inerenti all'attività aziendale;
- Non è consentito utilizzare web mail esterni, ovvero caselle di posta elettronica non appartenenti al dominio o ai domini aziendali salvo diversa ed esplicita autorizzazione.

UTILIZZO DELLA CONNESSIONE AD INTERNET DA PARTE DEGLI ADDETTI

Tutti i dipendenti, collaboratori o estranei alla **FONDAZIONE CITTÀ DELLA PACE** che usufruiscono dell'accesso ad Internet mediante la rete aziendale sono tenuti a seguire le seguenti regole:

- Non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate; a maggior ragione non è consentito navigare in siti che accolgono contenuti contrari alla morale e alle prescrizioni di Legge;
- È vietato accedere a siti pornografici, pedofili e qualsiasi altro sito a contenuto poco decoroso per la morale;
- È vietato accedere ad Internet senza i meccanismi di protezione predisposti dall'azienda, cioè saltando il firewall aziendale.
- È vietato occupare tutta o la maggior parte della banda disponibile mediante operazioni di scaricamento da Internet o di inoltro verso Internet. Nel caso fosse necessario, e sempre in ambito lavorativo, le attività connesse a tale occupazione di banda vanno concordate con l'AMS;
- Non è consentito navigare in siti che possano rivelare una profilazione dell'individuo definita “sensibile” ai sensi del D. Lgs. 196/03: quindi siti la cui navigazione palesi elementi attinenti alla fede religiosa, alle opinioni politiche e sindacali del dipendente o le sue abitudini sessuali;
- Non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili;
- Non è consentito lo scarico di software gratuiti trial, freeware e shareware prelevati da siti Internet senza l'autorizzazione dell'AMS;
- Non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) né attraverso Internet né attraverso servizi di peer to peer;
- È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- Non è permessa la partecipazione, per motivi non professionali a Forum e giochi in rete pubblica, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);
- Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

UTILIZZO DELL'ANTI-VIRUS DA PARTE DEGLI ADDETTI

L'antivirus è uno strumento messo a disposizione dalla **FONDAZIONE CITTÀ DELLA PACE** per proteggere le postazioni di lavoro da attacchi fraudolenti ad opera di programmi maligni. L'antivirus è obbligatoriamente installato, aggiornato ed in esecuzione sulle postazioni con sistema operativo MS-Windows. Sulle postazioni GNU/Linux la presenza di un tale strumento di protezione è da ritenersi opzionale.

Come prevenire i virus

1. Usare soltanto programmi provenienti da fonti fidate

Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzi programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

2. Assicurarsi che il software antivirus sia aggiornato

La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Eventuali problemi di funzionamento o segnalazioni dell'Antivirus vanno riportate tempestivamente all'AMS.

3. Non diffondere messaggi di provenienza dubbia

Se riceve messaggi che avvisano di un nuovo virus pericolosissimo, Io ignori: le mail di questo tipo sono dette con terminologia anglosassone hoax (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal suo migliore amico, dal suo capo o da un tecnico informatico. È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure dall'IBM (sono gli hoax più diffusi).

4. Non partecipare a "catene di S. Antonio" o simili

Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono hoax. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti hoax aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso.

GESTIONE DEL NOME UTENTE E DELLE PASSWORD DA PARTE DEGLI ADDETTI

Ad ogni dipendente della **FONDAZIONE CITTÀ DELLA PACE** è assegnata una USER – ID così strutturata: iniziale del nome di battesimo_cognome sino a 8 caratteri totali; così per esempio, l'ipotetico dipendente Mario Rossi avrà la seguente USER – ID: mrossi.

L'addetto della **FONDAZIONE CITTÀ DELLA PACE** quindi per accedere alla rete aziendale dovrà loggarsi ed inserire la propria password;

Al primo accesso la pwd è fornita dagli amministratori di sistema che avranno cura di farla sostituire al primo log-in in maniera tale che solo l'utente possegga le credenziali per accedere con quel determinato profilo; inoltre, trascorsi 6 mesi, l'Amministrazione ricorderà a tutti la modifica della pwd, secondo una metodologia specifica:

1. Il dipendente provvederà al cambio della pwd avendo cura di trascriverla su apposito modello precompilato;
2. Quindi inserirà il modello in busta, quindi sigillerà la busta apponendovi firme e data;
3. Quindi consegnerà la busta chiusa all'AMS;
4. DIR conserverà le buste in luogo sicuro (cassaforte) fino al prossimo rinnovo del cambio.

I PC devono essere bloccati dall'addetto della **FONDAZIONE CITTÀ DELLA PACE** quando ci si allontana dalla postazione lavorativa.

Di seguito le regole per il corretto utilizzo delle pwd:

Cosa non fare

- NON dire a nessuno la propria password: lo scopo principale per cui si usa una password è assicurare che nessun altro possa utilizzare le risorse altrui o possa farlo a suo nome;
- NON scrivere la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
- Quando viene immessa la password NON farsi sbirciare da nessuno;
- NON scegliere password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta;
- NON credere che usare parole straniere renda più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue;
- NON usare il nome utente. È la password più semplice da indovinare;
- NON usare password che possano in qualche modo essere legate all'utente come, ad esempio: il nome della propria/o moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

Cosa fare obbligatoriamente

- La password deve essere composta da almeno otto caratteri o, se il sistema non l'accetta, da un numero di caratteri pari a quello consentito dal sistema; è buona norma che, di questi caratteri, da un quarto alla metà siano di natura numerica;
- L'incaricato deve provvedere a modificare la password immediatamente, non appena la riceve per la prima volta, da chi amministra il sistema;
- Qualora si dovesse accedere al gestionale dalla postazione di un collega è obbligatoria l'autenticazione con le proprie credenziali (USER-ID/PWD).

Cosa fare praticamente

Utilizzare più di una parola e creare password lunghe

A volte è più semplice ricordare una frase completa di senso compiuto piuttosto che una parola complicata, e questa tecnica oltre a facilitare la memorizzazione migliora la sicurezza stessa della parola chiave: la lunghezza influisce sulle difficoltà di individuazione e ci consente di utilizzare lo "spazio" tra una parola e l'altra come ulteriore elemento da intercettare.

Inoltre è bene sapere che diversi strumenti di intercettazione presumono che le password non siano formate da più di 14 caratteri, e quindi, anche senza complessità, le password molto lunghe (da 14 a 128 caratteri) possono rappresentare un' ottima protezione contro possibili violazioni. Non tutti i software sono tuttavia in grado di accettare password superiori a 14 caratteri: ad esempio i sistemi operativi Windows 95 98 e Mc non oltrepassano questo limite.

Utilizzare numeri e simboli al posto di caratteri

Non limitarsi alle sole lettere ma, dove possibile, utilizzare l'ampia gamma di minuscole/maiuscole, numeri e simboli a disposizione sulla propria tastiera:

- Caratteri minuscoli: a, b, c,...
- Caratteri maiuscoli: A, B, C,...
- Caratteri numerici: 0,1,2,3,4,5,6,7,8,9
- Caratteri non alfanumerici: (< > , .) ` ~ ! $ % ^ ; * - + = | \ { @ # } [/] : ; " '?

Non inserirli alla fine di una parola nota come ad es.:"computer987". In questo caso la password può essere identificata abbastanza facilmente: la parola "computer" è inclusa in molti dizionari contenenti nomi comuni e quindi dopo aver scoperto il nome restano solo 3 caratteri da identificare. Al contrario, è sufficiente sostituire una o più lettere all'interno della parola con simboli che possono essere ricordati facilmente. Ad esempio si può provare a utilizzare "@"al posto di "A", "$"al posto di "S", zero (0) o la doppia parentesi () al posto di "O", e "3"al posto di "E": si tratta di trovare delle analogie che ci rendano familiare la sostituzione di lettere con simboli e numeri. Con alcune sostituzioni si possono creare password riconoscibili per l'utente, ad esempio (es.: "Ve$tit0 di Mari0"), già sufficientemente lunghe e estremamente difficili da identificare o decifrare.

Cercare di realizzare password utilizzando caratteri appartenenti a tutti i quattro gruppi rappresentati nella lista. Allo stesso modo, ma con una pwd differente l'utente dovrà ripetere la stessa operazione per accedere al sistema gestionale aziendale e per accedere alla propria casella di posta elettronica se la stessa gli spetta per profilo aziendale.

In fase di riesame annuale andrà effettuata una verifica della situazione complessiva dei diritti di accesso di tutti gli utenti attuando, se necessario, le idonee azioni.

ACCESSO ALLE RISORSE AZIENDALI

Ogni dipendente o collaboratore della **FONDAZIONE CITTÀ DELLA PACE** è abilitato dall'AMM all'uso dei servizi minimi che seguono comunicati in forma orale:

1. Cartelle condivise centralizzate. Le autorizzazioni sono determinate in base all'appartenenza a gruppi di lavoro
2. Posta elettronica mediante webmail
3. Accesso ad Internet.
4. Accesso al portale interno aziendale e relativi altri collegamenti (portale aziendale).

A seguito delle necessità contingenti, legati a nuovi progetti/servizi, AMS provvederà ad estendere la autorizzazioni di base alle risorse aziendali per gli utenti interessati.

UTILIZZO DI NOTEBOOK NELLA RETE AZIENDALE

I portatili aziendali, utilizzati all'interno del perimetro applicativo, sono assimilati alle postazioni fisse e restano in custodia dell'utente al quale è stato affidato. Agli addetti della **FONDAZIONE CITTÀ DELLA PACE** non è permesso l'utilizzo di notebook personali all'interno del perimetro aziendale.

Questa politica deve essere rigorosamente applicata al fine di garantire una custodia sicura, soprattutto sotto il profilo dei backup.

COME CORREGGERE LE INFORMAZIONI

La **FONDAZIONE CITTÀ DELLA PACE** fa il possibile per assicurare che i dati personali di cui è in possesso siano precisi, aggiornati e completi per gli scopi per i quali li utilizza. È diritto dei fornitori, dei volontari, dei collaboratori correggere le informazioni personali raccolte dalla fondazione.
È possibile correggere gli errori rilevati inviando una richiesta che indichi chiaramente l'errore. Per informazioni su come esercitare tale diritto bisogna contattare la sede della fondazione.

FUTURE MODIFICHE DELLA POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La Politica per la Sicurezza delle Informazioni della **FONDAZIONE CITTÀ DELLA PACE** è disponibile sul sito della Fondazione.
Ci si riserva il diritto di modificare in futuro la Politica per la Sicurezza delle Informazioni.
Conformemente alla Vigente Legislazione, qualunque modifica alla Politica per la Sicurezza delle Informazioni sarà effettiva non appena la Politica modificata sarà accessibile tramite Internet, per mezzo di un collegamento attivo sulla pagina iniziale del sito. Nel caso siano state effettuate modifiche, si correggerà la data e la revisione sulla parte superiore o sulla prima pagina del documento. Nel caso in cui la modifica della Politica per la Sicurezza delle Informazioni comporti una minore Tutela della Sicurezza delle Informazioni, la modifica non si applicherà all'uso, da parte della Fondazione, dei dati personali raccolti prima della modifica, eccetto nei casi in cui si provveda alla comunicazione offrendo la possibilità di richiede di non utilizzare in modi diversi i dati personali.

COORDINAMENTO CON LA VIGENTE LEGISLAZIONE

La raccolta e l'uso, da parte della **FONDAZIONE CITTÀ DELLA PACE**, di informazioni personali saranno regolati dalle leggi italiane e sarà limitato, conformemente ad essi, qualunque comunicazione dei dati.

INFORMAZIONI RELATIVE AD EX-ASSISTITI

I dati personali relativi ad ex assistiti della **FONDAZIONE CITTÀ DELLA PACE** verranno comunicati soltanto in conformità alla Politica Aziendale per la Sicurezza delle Informazioni.

DOMANDE DEI FORNITORI, DIPENDENTI, VOLONTARI E ASSISTITI

Se la Politica per la Sicurezza delle Informazioni della **FONDAZIONE CITTÀ DELLA PACE** non risponde alle domande sulla raccolta e l'uso, dei dati personali di fornitori, dipendenti, volontari e assistiti e ci sono delle domande Vi preghiamo di comunicarcelo. Se si riterranno insoddisfacente le risposte alle vostre domande o preoccupazioni, vi metteremo in contatto con un'organizzazione/professionista esterno neutrale e indipendente, per la risoluzione dell'eventuale controversia.

Potenza lì, 05/02/2018

Firma dell'Amministratore Delegato

della FONDAZIONE CITTÀ DELLA PACE

.....