Mediaddress Srl è una società che fornisce servizi per la comunicazione rivolti agli Uffici Stampa di Aziende, Agenzie e Istituzioni concernenti la fornitura di dati mirati e aggiornati su Media e Giornalisti.

Grazie all'esperienza maturata fin dalla sua nascita nel 1992, **Mediaddress Srl** (prima Mediadata), con la sua banca dati Mediaddress, è ormai un punto di riferimento sul mercato italiano nella fornitura di dati relativi a Media e Giornalisti e gode di un'ottima reputazione anche sul mercato europeo.

La nostra Mission è quella di migliorare continuativamente la soddisfazione dei clienti e delle altre parti interessate (personale, fornitori, giornalisti, proprietà).

Nello specifico scopo del SGI è delle Policy Aziendali quello di garantire il soddisfacimento dinamico, in termini di miglioramento e di adattamento ai cambiamenti, dei requisiti delle parti interessate tenendo conto del contesto in cui opera l'organizzazione, in termini di Riservatezza - Integrità - Disponibilità di informazioni (personali e non) presenti nelle nostre banche dati di giornalisti utilizzati per diffondere informazioni e comunicazioni rivolte agli Uffici Stampa di Aziende, Agenzie e Istituzioni.

Il documento Politica della Sicurezza delle Informazioni è un documento composto da una politica generale disposta dalla Presidenza e da altre politiche aziendali assegnate al Responsabile del Sistema di Gestione della sicurezza delle informazioni.

Politica per la sicurezza delle informazioni

1. Policy di sicurezza logica
2. Policy portatili
3. Policy supporti removibili
4. Policy dismissioni
5. Policy Telelavoro

6. Policy Scrivania e schermo pulito
7. Policy Password
8. Policy per videoconferenza
9. Policy per fotocopiatrici e fax
10. Policy per posta elettronica
11. Policy per i rapporti con i fornitori
12. Policy diritto d'autore

Le politiche per la sicurezza delle informazioni sono riesaminate almeno annualmente o nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia. Ogni politica è assegnata ad un responsabile che ha il compito di riesaminare il documento

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

L'attività di miglioramento passa anche dalla gestione in modo sicuro delle informazioni. Gli indirizzi strategici della Presidenza di Mediaddress Srl nell'ambito della sicurezza delle informazioni (SI) sono il raggiungimento dei seguenti obiettivi:

a) garantire un servizio continuo (senza interruzioni) ai nostri utenti/clienti,
b) garantire la sicurezza in termini di riservatezza, integrità e disponibilità dei dati e delle informazioni all'interno del perimetro di nostra competenza,

c) fare affidamento su fornitori qualificati e sicuri nell'ottica della sicurezza delle informazioni,
d) definire un percorso di miglioramento delle performance dei requisiti per la sicurezza delle informazioni,
e) creare e mantenere delle sinergie coi fornitori di servizi italiani ed esteri;
f) avere a disposizione una chiara strategia di business;
g) essere in conformità con regolamenti, leggi e contratti;
h) avere ben chiaro il contesto di rischio per la sicurezza delle informazioni attuale e previsto;
i) la definizione dei principi di sicurezza delle informazioni, e relativi obiettivi devono essere principi guida per tutte le attività relative alla gestione del relativo sistema conforme alla ISO/IEC 27001;
j) aver definito attribuzione delle responsabilità, generali e specifiche, per la gestione della sicurezza delle informazioni a ruoli definiti;
k) aver definito i processi per il trattamento degli scostamenti e delle eccezioni, in ambito della gestione delle informazioni e dei dati;
l) operare un'attenta selezione e screening dei candidati in ingresso in Mediaddress;
m) operare con fornitori qualificati, selezionati e con i requisiti utili a garantire qualità del servizio e la sicurezza delle informazioni.

1. POLICY DI SICUREZZA LOGICA

Gli indirizzi per la sicurezza logica di Mediaddress Srl nell'ambito della sicurezza delle informazioni (SI) sono:

a) controllo degli accessi alle reti e ai servizi di rete;

b) controllo degli accessi al codice sorgente;
c) regolamentazione dei controlli crittografici;
d) divieto di uso di software e file non autorizzati;
e) disposizione di controlli che prevengano o individuano il software non autorizzato;
f) disposizione per installazione, l'aggiornamento e la rimozione del sw di produzione, delle librerie e dei vari componenti (effettuato solo da personale formato);
g) stabilità e monitorata periodicamente la capacità del fornitore dei servizi di rete di gestire in modo sicuro i servizi concordati;
h) test relativi alle funzionalità di sicurezza sono effettuati durante lo sviluppo.

2. POLICY DISPOSITIVI PORTATILI E PERSONALI SUPPORTI REMOVIBILI

La politica per i dispositivi portatili di Mediaddress Srl nell'ambito della sicurezza delle informazioni (SI) prevede che occorre procedere alla:

a) la registrazione dei dispositivi portatili;
b) la definizione dei requisiti per la loro protezione fisica;
c) determinare le limitazioni all'installazione di software;
d) determinare i requisiti per il software dei dispositivi portatili e per l'applicazione di patch;
e) definire la limitazione della connessione a servizi informatici;
f) aggiornamento dei controlli di accesso;
g) gestire le tecniche crittografiche;

h) provvedere alla protezione da malware;
i) provvedere alla disabilitazione, cancellazione o il blocco remoti;
j) provvedere ai backup;
k) l'uso di servizi e applicazioni web.

Per ciò che concerne le buone pratiche sui dispositivi portatili ricordare all'utilizzatore:

– di non lasciarli mai incustoditi (per evitare i furti es: automobile e nelle aree di sosta delle autostrade),
– evitare di usarli in luoghi pubblici che qualcuno possa visualizzare i dati visualizzati a video
- non farli usare a persone non autorizzate per evitare il danneggiamento o che venga pregiudicata la sicurezza delle informazioni;
- per quanto riguarda i cellulari, ricordare di non intrattenere conversazioni riservate in luoghi pubblici.

3. POLICY SUPPORTI REMOVIBILI

La politica per la gestione dei dispositivi e supporti removibili di Mediaddress Srl nell'ambito della sicurezza delle informazioni (SI) prevede che occorre procedere a seguire le seguenti regole:

a) se non sono più necessari, i supporti mobili dovrebbero essere resi irrecuperabili i contenuti di ogni supporto riutilizzabile che deve essere dismesso dall'organizzazione;

b) quando utile e fattibile, deve essere richiesta all'organizzazione un'autorizzazione per spostare i supporti e dovrebbe essere mantenuta una registrazione di ogni spostamento al fine di mantenere un audit trail;
c) tutti i supporti devono essere conservati in un ambiente sicuro, in conformità con le specifiche del produttore;
d) se la riservatezza o l'integrità dei dati sono importanti, devono essere utilizzate tecniche di crittografia per proteggere i dati memorizzati sui supporti rimovibili;
e) per mitigare il rischio del deperimento dei supporti durante il periodo in cui i dati archiviati sono ancora necessari, i dati devono essere trasferiti su supporti nuovi prima di diventare illeggibili;
f) più copie di dati importanti devono essere archiviate su supporti separati per ridurre ulteriormente il rischio di danneggiamento o perdita coincidenti;
g) devono essere considerata la registrazione dei supporti rimovibili per limitare le possibilità di perdita di dati;
h) i dischi rimovibili devono essere abilitati solo se esiste una ragione di business;
i) dove vi è la necessità di utilizzare supporti di memorizzazione rimovibili, il trasferimento di informazioni verso tali supporti deve essere monitorato.

4. POLICY DISMISSIONI

La politica per la gestione delle dismissione degli strumenti ITC di Mediaddress Srl nell'ambito della sicurezza delle informazioni (SI) prevede che occorre procedere a seguire le seguenti regole:

a) i supporti contenenti informazioni riservate devono essere archiviati e dismessi secondo criteri di sicurezza, ad esempio l'incenerimento, la triturazione, o la

cancellazione dei dati al fine di poter essere utilizzati per un altro scopo all'interno dell'organizzazione;

b) sono attive procedure per identificare i supporti che potrebbero richiedere una dimissione sicura;
c) potrebbe essere più semplice raccogliere e dismettere in modo sicuro tutti i supporti, piuttosto che fare attenzione a separare i supporti critici;
d) è stata selezionata una terza parte appropriata con controlli ed esperienza adeguati per la dismissione dei supporti ITC;
e) la dismissione di oggetti critici sono tracciate al fine di mantenere un audit trail;
f) quando vengono accumulati dei supporti per essere dismessi, dovrebbe essere considerato l'effetto di aggregazione, che potrebbe far sì che una grande quantità di informazioni non critiche diventino importanti;
g) Il deterioramento di dispositivi che contengono dati critici potrebbe richiedere una valutazione del rischio per determinare se i supporti dovrebbero essere fisicamente distrutti piuttosto che inviati in riparazione o scartati;
h) Tutti gli apparati e i supporti informatici devono essere controllati per assicurare che ogni dato critico sia rimosso o sovrascritto in modo sicuro prima della dismissione o del riutilizzo

5. POLICY PER IL TELELAVORO

La politica per la gestione del telelavoro svolto dai collaboratori di Mediaddress Srl nell'ambito della sicurezza delle informazioni (SI) prevede che occorre procedere a seguire le seguenti regole:

a) provvedere la forniture di apparecchiature e attrezzature idonee per le attività di Mediaddress Srl,
b) l'uso di apparecchiature private non sotto il controllo dell'organizzazione non è permesso;
c) definito il c.d. lavoro consentito, delle ore di lavoro, della classificazione delle informazioni che possono essere trattenute e dei sistemi e servizi interni a cui il telelavoratore è autorizzato ad accedere; la fornitura di idonee apparecchiature di comunicazione, ivi inclusi i metodi per rendere sicuro l'accesso remoto;
d) si è provveduto alla sicurezza fisica, alla definizione di regole e le linee guida sull'accesso alle apparecchiature e alle informazioni da parte dei famigliari e dei visitatori;
e) è garantita la fornitura di supporto e manutenzione hardware e software;
f) sono definite le procedure per il backup e per la continuità operativa;
g) è stata disposta la revoca dei privilegi e dei diritti di accesso e la restituzione delle apparecchiature al termine delle attività di telelavoro.

6. POLICY PER SCRIVANIA PULITA E SCHERMO PULITO

A) è importante che Informazioni sensibili o confidenziali e altre informazioni di valore, conservate sia elettronicamente, sia in modalità cartacea, siano conservate in modo sicuro quando ci si assenta dalla propria postazione di lavoro (In particolare questa regola trova applicazione su aree di lavoro (es: tavoli) in comune)
B) I fascicoli che contengono informazioni riservate devono sempre essere riposti sotto chiave in cassetti della scrivania, armadietti;

C) le scrivanie devono essere pulite alla fine di ogni giornata lavorativa da qualsiasi informazione di identificazione personale o riservata;
D) è necessario che se eventuali PC/notebook siano posizionati aree pubbliche, non sia possibile leggere dagli schermi da persone in prossimità non interessate all'informazione;
E) se occorre lasciare un messaggio sulla scrivania ad altra persona (es: collega) occorre assicurarsi che non contenga informazioni riservate.

7. POLICY PER PASSWORD

A) Definire password senza riferimenti diretti a persone, cose, date, ecc.. dell'utente in modo da rendere difficoltosa la determinazione con maiuscole, minuscole e segni speciali;
B) non rivelare a nessuno Password o proprio user ID (salvo non richiesto da persone autorizzate);
C) è obbligatorio cambiare la password ogni volta che c'è il sospetto che questa possa essere compromessa;
D) cambiare la password iniziale al primo collegamento;
E) non digitare mai la password se qualcuno di non autorizzato sta osservando la tastiera

8. POLICY PER VIDEOCONFERENZA

A) le videocamere e i microfoni devono essere spenti quando non vengono usati;

B) prima del collegamento assicurarsi che la videocamera non sia posizionata dove possano riprendere documenti sensibili o schermi di computer sulle scrivanie;
C) assicurarsi che i microfoni non raccolgano conversazioni private;
D) per videoconferenze dove si devono discutere informazioni sensibili il traffico video andrebbe criptato.

9. POLICY PER FOTOCOPIATRICI E FAX (uso accettabile)

A) le stampanti e le fotocopiatrici devono essere liberi da carte (quando non utilizzate);
B) è responsabilità della persona che stampa raccogliere I propri documenti;
C) prima di stampare gli utenti si devono assicurare che la stampante predefinita sia quella corretta.

10. POLICY PER POSTA ELETTRONICA

A) la cartella Posta in arrivo da mantenere più pulita possibile;
B) cercare di organizzare i messaggi in più cartelle per gruppi di appartenenza;
C) ricordarsi di cancellare I messaggi non più necessari;
D) comprimere sempre gli allegati più “pesanti”;
E) per e-mail con alto numero di destinatari, valutare l’impiego del campo CCN per migliorare la gestione della privacy;
F) Non aprire MAI allegati e-mail o selezionare collegamenti web nel corpo del messaggio se non si considera attendibile il mittente.

11. POLICY PER RAPPORTI (CONTRATTUALI) CON I FORNITORI

Gli accordi e i contratti con i propri fornitori devono basarsi su aspetti e requisiti preventivamente stabiliti. In termini generali possiamo distinguere 3 tipologie di forniture

- fornitori di prodotti o assistenza (esclusi accesso diretto ai sistemi ICT di Mediaddress);
- fornitori di servizi informatici
- fornitori di servizi non informatici.

Per definizione per una corretta gestione del rapporto con il fornitore, nell'ambito della sicurezza delle informazioni ogni contratto o accordo dovrebbe avere

A) accordo di riservatezza e di non divulgazione, dove le parti impegnano a non divulgare o comunicare ad altri informazioni riservate dell'uno e dell'altro (anche dopo la conclusione del rapporto. Inoltre a prevedere che il il medesimo impegno, mediante accordi o contratti scritti, anche col proprio personale, gli altri fornitori o subfornitori;
B) le misure di sicurezza da rispettare;
C) i criteri di continuità operativa (il tempo massimo di indisponibilità dei servizi
D) le modalità controllo/analisi di performance.

I contratti per definizione hanno una durata variabile. E` compito della Presidenza prestare attenzione alle relative scadenze e soprattutto riesaminare con cadenza regolare se requisiti, nel tempo hanno perso validità, perché e basati su normative decadute o perché siamo in presenza di nuove esigenze non sono formalizzate.

12. POLICY PER DIRITTO D'AUTORE

Mediaddress riconosce e rispetta la normativa a favore della protezione del diritto d'autore, prevenzione dei crimini Informatici e legge antipirateria ed intende applicare tutti i controlli possibili affinché si operi nel pieno rispetto, mediante attività di:

- acquisto di copie con licenza di software, registrazioni e libri o altri documenti protetti da copyright da una varietà di editori e fornitori legali;
- acquisto di copie di programmi software, registrazioni e libri o altri documenti protetti da copyright registrate e licenziate per l'installazione sui computer e i sistemi centralizzati;
- la gestione esclusiva da parte dell'Amministratore di sistema delle relative licenze sw, compresa la dismissione a fine ciclo di vita (provvedendo alla disinstallazione corretta dei programmi e ritiro di eventuali copie di backup e licenze).

Inoltre si fa presente che è vietato dalla legge e dalle norme di comportamento di Mediaddress:

- l'uso del software, registrazioni e libri o altri documenti protetti da copyright ottenuto da qualsiasi altra fonte (rispetto a quelle sopra elencate);
- la duplicazione non autorizzata di software, registrazioni e libri o altri documenti protetti da copyright;
- l'acquisto da parte dei collaboratori di ulteriori software rispetto a quelli gestiti dall'amministratore di sistema.

13. POLICY INCIDENT

Mediaddress riconosce tra gli obiettivi principali La gestione degli incidenti di sicurezza al fine di

- ridurre l'impatto degli eventi malevoli;
- adoperarsi affinchè si attuino in maniera tempestiva idonee misure di contenimento degli effetti;
- adoperarsi affinchè tutte le attività di ripristino a seguito di un incidente siano operative;
- imparare dall'esperienza per alimentare il processo di azioni preventive per migliorare le performance in materia di salute e sicurezza dei dati;

Si richiede la massima collaborazione da parte di tutti gli addetti e nello specifico è demandato all'Amministratore di Sistema la gestione dell'incidente e il coordinamento delle azioni e dei protocolli di Mediaddress per la rilevazione dell'incident e di tutte le misure prese per limitarne i danni e coordinare le attività di ripristino.

14. POLICY TICKETING (HELP DESK)

Mediaddress help desk per offrire ai propri utenti un aiuto immediato su tutti gli aspetti del lavoro a computer organizzando il servizio su 2 livelli:

1° livello di servizio fornito da uno specialista help desk chiamato a risolvere i problemi più comuni ed un

2° livello di servizio, a cui vengono inoltrate le richieste più complesse, formato da specialisti di ogni settore (software, rete, server, ecc…) che analizzano e risolvono il problema

- risolvere nel minor tempo possibile problematiche legate al'utilizzo, alla sicurezza e funzionalità del software e relativa banca dati;
- ridurre l'impatto degli eventi malevoli, nel momento in questi si verificano, in modo da non danneggiare in ultima istanza il nostro cliente;
- adoperarsi affinchè si forniscano suggerimenti e indicazioni preziose per migliorare il servizio IT e semplificare le procedure;
- imparare dall'esperienza per alimentare il processo di azioni preventive per migliorare le nostre performance.

Milano, 21.01.2022

Il Presidente