POLICY DI SICUREZZA DELLE INFORMAZIONI

<Aldeghi S.r.l.>

Verificato e Approvato da Direzione	Cesare Aldeghi	**Responsabile Sicurezza**	Vincenzo D'Angelo
Data	04 Aprile 2019		
Distribuito a:	**Tutti gli incaricati dell'organizzazione al trattamento dei dati, ove competenza**		

1 Scopo e campo di applicazione

Queste politiche, norme e procedure si applicano a tutti i dati, i sistemi informativi, le attività e le risorse di proprietà di Aldeghi S.r.l. (da qui in poi "ALDEGHI"), noleggiati, controllati o utilizzati da ALDEGHI, dai suoi agenti, appaltatori o altri partner commerciali per conto di ALDEGHI. Queste politiche, norme e procedure si applicano a tutti i dipendenti, appaltatori, subappaltatori e le rispettive strutture che supportano le operazioni aziendali di ALDEGHI, ovunque siano archiviati o elaborati i dati ALDEGHI, comprese le terze parti designate da ALDEGHI per gestire, elaborare, trasmettere, archiviare o eliminare i dati ALDEGHI.

Alcune politiche fanno esplicito riferimento a persone con una specifica funzione lavorativa (ad es. un amministratore di sistema); in caso contrario, tutto il personale deve rispettare le politiche.

ALDEGHI si riserva il diritto di revocare, modificare o integrare politiche, procedure, standard e linee guida in qualsiasi momento senza preavviso. Tali modifiche saranno efficaci immediatamente dopo l'approvazione da parte della direzione, salvo diversa indicazione.

2 Ruoli e Responsabilità

La Direzione di ALDEGHI identifica i ruoli e le responsabilità necessari per la gestione dei Sistemi implementati. In generale, vista la natura del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), tutti i dipendenti e collaboratori sono coinvolti nei processi di sicurezza delle informazioni all'interno del perimetro identificato. In particolare, di seguito si elencano le principali aree organizzative coinvolte attivamente nell'implementazione, gestione e controllo del SGSI.

La Direzione Aziendale è responsabile dell'implementazione del SGSI e delle politiche, delle linee guida e del supporto attivo ai processi.

- approva l'implementazione del processo del SGSI;
- nomina, per iscritto, un responsabile del sistema di gestione della sicurezza delle informazioni incaricato di implementare e gestire il SGSI
- fornisce chiare linee guida alle unità organizzative interessate per assicurare un adeguato livello di protezione per tutte le risorse informative di proprietà o mantenute dall'azienda;
- approva manuali, politiche e linee guida relative al SGSI stesso;
- prepara, sviluppa e controlla i budget complessivi relativi al SGSI;
- assicura la disponibilità e la formazione di risorse con adeguate competenze e capacità per l'implementazione e l'attuazione del processo di SGSI;
- assicura la disponibilità di risorse per l'adozione delle necessarie misure tecnologiche e organizzative a supporto dell'implementazione dell'SGSI
- assicura che il processo di SGSI sia soggetto ad efficaci verifiche esterne e/o interne;
- coordina il Comitato della Sicurezza delle Informazioni.

Responsabile del Sistema di Gestione della Sicurezza delle Informazioni: è responsabile dell'implementazione e della gestione delle politiche, delle procedure e dei controlli relativi all'SGSI.

- garantisce l'implementazione e la gestione dei processi del SGSI;
- garantisce un'adeguata reportistica alla Direzione;
- collabora alla definizione delle politiche dell'SGSI;
- stabilisce strategie e obiettivi del SGSI, nonché standard e linee guida che l'organizzazione deve adottare;
- definisce sistemi di misurazione delle performance dei processi del SGSI;
- garantisce un regolare coordinamento con le unità organizzative che sono maggiormente coinvolte nei processi del SGSI;
- Predispone regolarmente attività di Security Assessment e Information Risk Management;
- prepara, sviluppa e controlla i budget relativi al SGSI per quanto di competenza;
- stimola le auto-valutazioni ed i feedback da parte degli utenti;
- sviluppa strategie atte a garantire la preparazione e la conoscenza degli utenti in tema di SGSI;
- coordina la gestione degli Incidenti di Sicurezza

Il Responsabile del Sistema di Gestione non ha compiti operativi ma funzioni di coordinamento, indirizzo ed orientamento.
Esso esplica le proprie funzioni tramite riunioni periodiche (almeno una volta l'anno) e quando si renda necessario per specifiche esigenze. Suo principale compito è la scelta e l'emanazione delle politiche di sicurezza, che rappresentano le linee guida dell'amministrazione per quanto riguarda gli aspetti di sicurezza.
Queste linee guida possono essere definite a tre livelli:

- politica di sicurezza dell'amministrazione, riferita agli aspetti di sicurezza che riguardano l'amministrazione nel suo complesso;
- politica di sicurezza del sistema informativo, riferita agli aspetti di sicurezza propri del sistema informatico;
- politica di sicurezza tecnica, riferita agli aspetti più propriamente tecnici della sicurezza del sistema informatico.

Il Responsabile SGSI, definisce le linee guida di carattere generale relative al primo aspetto e delega l'approfondimento e l'implementazione degli altri aspetti tecnologici ed organizzativi.
Gli obiettivi maggiormente significativi che devono essere perseguiti nella definizione della politica di sicurezza dell'amministrazione riguardano i seguenti punti:

- determinazione degli obiettivi di sicurezza, concordemente con le indicazioni della Politica aziendale per la sicurezza informatica;
- definizione ed approvazione della struttura organizzativa alla quale è affidata la sicurezza;
- attribuzione di responsabilità ed autorità in materia di sicurezza;

Il Responsabile SGSI ha dunque una importante funzione di indirizzo e di avallo dell'operato dell'intera organizzazione di sicurezza attraverso la elaborazione e l'emanazione delle norme e dei regolamenti. Le norme in materia di sicurezza sono approvate formalmente dalla Direzione Aziendale.

Responsabili delle risorse aziendali (Asset Owners)
Responsabile aziendale o di reparto con autorità di bilancio sulle risorse aziendali (informazioni in forma cartacea o elettronica, hardware, software, persone, edifici, etc.) di sua competenza per quanto concerne manutenzione, gestione, sicurezza.

Amministratori di sistema

- implementano e gestiscono i controlli tecnologici e le attività di sicurezza previsti dal SGSI;
- analizzano periodicamente i diritti di accesso e di utilizzo delle informazioni delle risorse appartenenti alla propria unità;
- garantiscono la sorveglianza dei sistemi;
- sono responsabili della manutenzione ordinaria e straordinaria dei sistemi informativi
- gestiscono gli incidenti di sicurezza sotto il coordinamento del Responsabile della Sicurezza delle Informazioni

Responsabile Risorse Umane: ha il ruolo di referente per l'implementazione e la gestione delle politiche, delle procedure, dei controlli e dei piani formativi che riguardano le risorse umane.

Utenti finali
Tutti i dipendenti e in generale gli incaricati del trattamento dei dati che accedono ai sistemi informativi di ALDEGHI sono tenuti a rispettare tutte le politiche, le procedure, gli standard e le linee guida applicabili in materia di sicurezza delle informazioni.

DPO
La figura del DPO viene istituita da ALDEGHI con incarico ad un consulente esterno.

Responsabili dei dipendenti
ALDEGHI predispone e distribuisce apposita informativa relativa alla politica aziendale sulle responsabilità sul trattamento dei dati ("Politica Aziendale M.S. Ambrogio") distribuita a tutti i dipendenti.

3 Gestione degli asset

3.1 Inventario degli asset

Gli Asset del Sistema Informativo ALDEGHI sono costantemente controllati tramite un apposito file Excel ("Riepilogo materiale informatico") nel quale vengono codificati e assegnati alle

Funzioni/Utenti di riferimento. Nel documento vengono inoltre registrate le principali informazioni (codice ALDEGHI, serial number, cespite, ubicazione). In tale file vengono registrate anche le dismissioni degli Asset Aziendali.

3.2 Assegnazione e responsabilità dei beni aziendali

Ogni Asset gestito dall'IT è assegnato ad un singolo utente oppure al responsabile di ufficio/ funzione. L'assegnazione è registrata nel file "Gestione PC".

3.3 Regolamento di uso accettabile dei dispositivi

Le modalità di utilizzo corretto dei dispositivi sono documentate nel documento "MSA Informativa ai dipendenti" che ogni neoassunto riceve dall'Ufficio Personale all'atto dell'assunzione. Si rimanda a tale documento, reperibile presso l'Ufficio Personale, per i dettagli.

3.4 Uso dei dispositivi personali (BYOD) in azienda

Come regola generale non è permesso l'utilizzo di dispositivi privati a scopi aziendali. Solo in casi eccezionali il Responsabile di Funzione può chiedere via mail al Responsabile IT per se stesso o per un suo collaboratore la possibilità di utilizzare un dispositivo privato. Se non vi sono particolari controindicazioni in merito questo viene concesso per un periodo temporaneo o illimitato.

4 Controllo degli accessi

4.1 Registrazione e gestione degli utenti

Ogni nuovo utente che ha le autorizzazioni per entrare nel dominio "ALDEGHISRL" viene definito sul Server Domain Controller dall'Amministratore di dominio. Ad esso vengono associate le autorizzazioni di base del gruppo (ufficio) di appartenenza oppure autorizzazioni diverse qualora il Responsabile di Funzione ne faccia richiesta specifica via mail all'IT.
Ogni qualvolta un utente cessa la sua collaborazione con ALDEGHI, la Direzione Aziendale Aldeghi ne richiede al gestore IT la sospensione (e la successiva eliminazione) dell'utente impedendone quindi l'utilizzo per poter accedere alle cartelle di rete. Tale operazione può essere posticipata su richiesta via mail da parte del Responsabile di Funzione che può aver bisogno di mantenere attivo temporaneamente l'utente per consentire di chiudere lavori già iniziati.

4.2 Profilazione degli utenti e segregazione dei ruoli

Ogni utente può avere specifiche autorizzazioni di accesso alle diverse cartelle di rete e quindi ai dati aziendali. I diritti di accesso ai primi livelli delle cartelle di rete sono documentate in un apposito file Excel ("Accessi_alla_rete_ufficiali_ALDEGHI"). In questo file vengono specificati per ciascuna cartella i diritti in lettura e scrittura o sola lettura.
Il Responsabile della singola cartella di rete deve sempre essere a conoscenza e/o autorizzare direttamente via mail la richiesta di accesso da parte di un utente del dominio.
In base alla criticità e sensibilità delle informazioni presenti nelle singole cartelle il Responsabile della cartella decide a chi concedere l'accesso ed in quale modo (se sola lettura o anche modifica).

Così, per esempio, le informazioni riservate contenute nelle cartelle dell'Ufficio Amministrazione sono accessibili solo alle persone autorizzate dal Responsabile della Contabilità.

4.3 Sistemi di autenticazione e autorizzazione informatica

Solitamente i sistemi ALDEGHI richiedono un sistema di autenticazione tramite password ad un solo livello.

4.4 Password Policy

La politica della gestione delle password prevede alcune regole restrittive in linea con la Legge della Privacy. Si riporta in Appendice 1 il testo della mail che ogni 6-12 mesi viene inviata agli utenti per sensibilizzarli al corretto utilizzo delle password.
Anche le password predefinite per sistemi operativi, router, firewall, punti di accesso wireless aziendali, applicazioni e altri sistemi devono seguire le medesime regole riportate in tale comunicazione aziendale.
Possono fare eccezione i punti di accesso wireless Guest che non consentono di accedere ad alcuna informazione aziendale ma che servono solamente per concedere navigazione su Internet gratuita a Clienti e Fornitori senza fornire loro la connessione alla nostra rete aziendale.

4.5 Amministratori di sistema

Gli Amministratori di Sistema sono definiti in base ai diversi sistemi gestibili in MSA (Server-PC- Rete o AS/400).
Per l'elenco aggiornato si rimanda al documento "Amministratori_di_Sistema_2018_ALDEGHI.xls" disponibile sotto la cartella "Privacy-DPS Ufficiali" del Server32.
Gli utenti amministratori hanno profili dedicati nominali.

4.6 Accesso alla rete aziendale

4.6.1 Accesso remoto

L'accesso remoto alla rete Aziendale è consentito solamente tramite prodotto TeamViewer.

La postazione di lavoro utilizzata deve avere antivirus operativo ed aggiornato per potersi collegare alla rete. Ai dipendenti vengono fornite postazioni aziendali (notebook) per connettersi in remoto alla rete e queste devono essere costantemente tenute aggiornate anche con le patch di sicurezza del sistema operativo.
L'accesso remoto per l'amministrazione di sistemi IT da parte dei dipendenti autorizzati ad agire come amministratori dei nostri sistemi può essere effettuato attraverso l'apposita VPN predisposta sul Firewall perimetrale e viene effettuato solo mediante utente personale e non condiviso con altri colleghi.
Quando invece è necessario effettuare un collegamento remoto estemporaneo per esempio con un fornitore è possibile utilizzare il prodotto Teamviewer. Vincolo però per questo tipo di sessione è che sia costantemente monitorata; cioè l'addetto IT ALDEGHI che sta seguendo la connessione da

fuori deve essere dedicato a seguire in tempo reale quello che viene fatto dall'inizio alla fine della sessione.
Qualora fosse indispensabile concedere ad un amministratore incaricato dal fornitore un accesso in VPN sul nostro firewall perimetrale questo deve avvenire come sempre con apposita comunicazione che avvisa delle regole da rispettare e con un utente dedicato al fornitore. Pertanto anche l'accesso remoto per l'amministrazione di sistemi IT da parte di soggetti esterni autorizzati in tal modo avverrebbe attraverso un collegamento VPN dedicato e verificabile.

4.7 Segregazione delle reti – VLAN

Non sono presenti VLAN all'interno della rete ALDEGHI.

4.8 Limitazioni di accesso (firewalling, etc.)

Utilizziamo 2 firewall Zyxel Zywall USG60 in stato attivo/passivo a commutazione manuale.
Si rimanda per i dettagli alla relativa documentazione presente nella cartella OP_ALDEGHI del Server32.
Il firewall perimetrale è impostato in modo da bloccare il traffico non permesso in ingresso e in uscita dalla rete aziendale; a tale scopo vengono definite al suo interno regole specifiche su protocolli e porte. Il sistema registra nel proprio LOG gli accessi concessi e bloccati.
Per i dettagli di tutti i controlli, blocchi e permessi fatti dal firewall (in continuo aggiornamento) si rimanda alla configurazione presente nel sistema.

4.9 Monitoraggio del traffico (IDS/IPS, etc.)

In ALDEGHI non utilizziamo specifici prodotti per l'analisi delle intrusioni. Alcune informazioni sulle principali attività di accesso dall'esterno vengono registrate dal firewall.
Il traffico di rete in uscita verso Internet passa attraverso un Proxy che utilizza regole specifiche per bloccare porte o servizi non autorizzati.
Inoltre per una maggiore sicurezza sulla navigazione Web, viene utilizzato il prodotto Triton Cloud per il Web Filtering per bloccare URL/domini pericolosi o non attinenti con l'ambito lavorativo.
Tutti i gli indirizzi Web oggetto di navigazione vengono pertanto registrati per poter identificare attività potenzialmente dannose e identificare sistemi potenzialmente compromessi

4.10 Time-out di sessione

Su tutti i server aziendali è obbligatorio impostare lo screen-saver con password (durata minima per l'attivazione: 20 minuti).
Anche per i PC utente viene indicata sul documento Aziendale "MSA Informativa ai dipendenti" l'obbligatorietà di screen saver e relativa password.

4.11 Sicurezza dei dispositivi mobili

I dispositivi mobili aziendali sono assegnati in base alle Direttive Aziendali alla persona o al Responsabile dell'Ente che li deve prendere in carico.

La connessione del dispositivo mobile alla rete aziendale (solo posta elettronica per gli smartphone) viene impostata dal personale dei Sistemi Informativi utilizzando la rete WIFI aziendale.
Uno smartphone personale può accedere alla rete aziendale solo a seguito di inderogabile esigenza e su richiesta ed autorizzazione del responsabile di Funzione. In tal caso il dispositivo può accedere solo alla posta elettronica.
I dispositivi mobili devono essere protetti da un codice di accesso (password).

4.12 Standard di accesso alle reti Wireless

In ALDEGHI è disponibili una rete Wireless utilizzata solo per utenti interni ALDEGHI con password complessa. La password non va comunicata a personale non ALDEGHI.
Per l'accesso alla Wireless aziendale vengono utilizzati protocolli di autenticazione adeguati agli standard di riferimento (WPA2, WPA-PSK, etc.).

4.13 Dipendenti non più in forza

Al personale che cessa il rapporto di collaborazione con ALDEGHI, l'ultimo giorno di lavoro viene ritirato da parte dell'Ufficio Personale il badge che permette l'accesso all'Azienda.

5 Business Continuity e Disaster Recovery

Il backup viene effettuato quotidianamente su più unità disco dislocate in punti diversi dell'azienda.
Come Disaster Recovery la Direzione Aziendale Aldeghi porta a casa due unità disco di backup.
Per preservare i dati del backup in caso di evento disastroso è necessario disporre di due copie del backup totale dei Server in una locazione distante dal luogo dove risiede la sede dell'Azienda.
Ogni giorno la Direzione ALDEGHI raccoglie 2 unità disco esterne dei propri backup criptate e le porta a casa.

6 Backup

Quotidianamente vengono salvati su varie unità di backup tutti i dati presenti sul server aziendale.

7 Gestione delle vulnerabilità tecnologiche

7.1 Valutazione delle vulnerabilità

L'Azienda riceve informazioni periodiche sulle vulnerabilità (solitamente mail dai vendor e una volta all'anno analisi ufficiale da parte del fornitore designato) e sugli aggiornamenti di sicurezza disponibili (update mensile manuale da parte dell'amministratore di sistema).
Tali comunicazioni sono in parte utili ed a volte indispensabili per definire le modalità di gestione delle vulnerabilità stesse e le tempistiche di aggiornamento dei sistemi e del software.
Le vulnerabilità esterne del sistema di Sicurezza ALDEGHI vengono annualmente verificate dalla Società esterna che ci segue per la Sicurezza Informatica. Il Fornitore attraverso appositi tool effettua questa analisi e ci invia un report in cui evidenzia le vulnerabilità esistenti indicandone per ciascuna il livello di criticità.

A seguito di tale analisi ALDEGHI verifica poi con il Fornitore quali vulnerabilità è necessario correggere e quali invece possono essere lasciate tali in base ad un'analisi del rischio connesso alle singole vulnerabilità.

7.2 Priorità e pianificazione degli aggiornamenti

Gli aggiornamenti periodici dei firewall/router sono applicati secondo date valutate e pianificate in accordo con la Società esterna che ci segue per la Sicurezza Informatica.
Gli aggiornamenti di Sicurezza vengono costantemente applicati anche su Server e PC Aziendali.
Per l'installazione di server e client devono essere utilizzati sempre CD o supporti ufficiali (del produttore), oppure immagini e/o sorgenti di installazione devono essere scaricati dai siti ufficiali dei produttori/fornitori e prima di essere utilizzati devono essere salvati su dispositivi dotati di antivirus in modo tale che questi ne possa effettuare la scansione.
Non effettuiamo invece aggiornamenti generici "suggeriti" da produttori di software o firmware dei sistemi ma effettuiamo l'aggiornamento solo "al bisogno", cioè quando questo viene richiesto da un motivo legato alla Sicurezza o da una funzionalità del prodotto/dispositivo.

8 Change Management

Per questo argomento si rimanda alla specifica procedura Aziendale "Change management".

9 Sicurezza delle postazioni di lavoro

9.1 Protezione dal malware

9.1.1 Strumenti

Per la protezione da virus e malware a livello di server e postazioni di lavoro utilizziamo l'antivirus Kaspersky.
Oltre alla protezione in real-time viene aggiunta una scansione programmata periodica che per i server avviene quotidianamente alle ore 23:30 mentre per le postazioni di lavoro il Venerdì alla ore 12:30.
Tutte le eventuali rilevazioni di virus o malware su server e PC vengono registrate nell'apposito LOG dell'antivirus.

9.1.2 Modalità di detection

La detection di virus e malware è soprattutto in tempo reale perchè su ogni sistema è costantemente in linea il sistema antivirus aziendale.

9.1.3 Modalità di aggiornamento

I sistemi antivirus verificano periodicamente sul sito del produttore la presenza di nuovi aggiornamenti; nel caso in cui questi siano presenti vengono scaricati ed immediatamente inviati alle utenze (server e PC vengono aggiornati in questo caso senza intervento manuale)

9.1.4 Sandboxing

Il sistema antispam è dotato di un sistema sandboxing che consente di verificare la bontà di un link prima dell'accesso da parte dell'utente. Nel caso di link pericoloso il sistema antispam avverte l'utente. Ogni URL presente nelle mail viene protetto da questo sistema.

9.2 Sistemi Antispam

Il nostro sistema antispam è Libra Esva, uno dei prodotti considerati più efficaci al mondo.
Il sistema filtra tutte le mail, le categorizza in base al contenuto e lascia passare solo quelle ritenute non pericolose e non SPAM.

9.3 Limitazione dei privilegi utente

L'accesso degli utenti alle informazioni presenti sui server dati aziendali è gestito attraverso delle autorizzazioni in lettura e/o scrittura sulle cartelle di rete.
Gli utenti non hanno le autorizzazioni con i loro account per disattivare l'antivirus.
Gli utenti non sono autorizzati ad installare software estraneo all'uso aziendale e rispondono personalmente nel caso in cui non rispettino questa regola riportata sul documento "MSA Informativa ai dipendenti".
Ogni utente di dominio, per esigenze tecniche, è "amministratore" della propria postazione di lavoro; l'utilizzo corretto di tale utente è a carico dell'utente stesso.

9.4 Trasferimento dei dati su supporti rimovibili o esterni

Non è consentito utilizzare supporti di proprietà del dipendente.
Non è consentito l'utilizzo ad uso personale dei supporti rimovibili o esterni di proprietà aziendale.
L'utilizzo di tali supporti è consentito per scopi aziendali.

9.5 Sicurezza del browser

Per rendere sicura la navigazione utilizziamo un prodotto di Web Filtering (Triton) che ha il duplice scopo di evitare che l'utente acceda a siti notoriamente pericolosi e sia di evitare che l'utente navighi su siti non attinenti all'attività lavorativa. Il sistema è dotato di una serie di regole, in evoluzione con l'evolvere delle diverse esigenze o utenze aziendali, che consentono di personalizzare le autorizzazioni di navigazione in base alle singole esigenze degli utenti/funzioni.
Il sistema registra in un LOG le navigazioni (concesse o negate) effettuate.

9.6 Sicurezza del client di posta elettronica

Per accedere al Client di posta elettronica viene utilizzata l'autenticazione di dominio.
Internamente la sicurezza è garantita con i protocolli proprietari Microsoft. Esternamente La connessione alla web mail è garantita attraverso un certificato SSL (oltre all'autenticazione Active Directory).
Manteniamo tutti i software aggiornati (Exchange Server e Clienti di posta Outlook).

9.7 Whitelisting delle applicazioni

All'interno del sistema antivirus Kaspersky gestiamo alcuni processi in whitelist come per esempio SQL Server ed Exchange.

9.8 Cifratura dei laptop

I dischi dei computer portatili (notebook) vengo crittografati con un prodotto McAfee specializzato (McAfee Complete EndPoint Protection). L'utilizzo di un prodotto all'avanguardia ci garantisce anche che gli algoritmi di cifratura utilizzati siano in linea con le raccomandazioni delle buone pratiche di sicurezza e dagli standard riconosciuti. Per gli algoritmi utilizzati si rimanda alla documentazione del prodotto.
Con la crittografia dei laptop risulta praticamente impossibile accedere ai dati utente per chi non conosce la password dell'utente stesso (per esempio a seguito di smarrimento o furto del dispositivo).

10 Monitoraggio

10.1 Finalità e modalità di raccolta dei log

I log vengono raccolti dai singoli prodotti (Sistema operativo Windows, Web Filtering) in database proprietari che vengono salvati giornalmente con il salvataggio del relativo server sul quale vengono eseguiti.
A fronte di segnalazione di anomalie i sistemisti incaricati intervengono per analizzare e correggere il problema.

10.2 Salvataggio e conservazione sicura dei log

Come indicato nel paragrafo precedente, non effettuiamo un salvataggio dedicato dei LOG ma questi vengono backuppati con i relativi server. I dati dei server (e quindi anche i LOG) possono eventualmente essere recuperati dai backup che vengono effettuati.
I file di log risiedono su server la cui data e ora è sincronizzata con il server DNS primario a sua volta connesso con i server pubblici dedicati a fornire data e ora aggiornate. Pertanto anche i LOG stessi riportano data e ora corretta.

10.3 Controllo degli accessi e protezione dei log

Non gestiamo password dedicate per l'accesso ai log. Tali log sono comunque gestiti all'interno di Database dedicati per i quali è sempre richiesta una password per accedere.
I file di log sono sempre residenti sui dischi interni o database di server; pertanto l'accesso è riservato a coloro che conoscono le password di accesso a tali server (solitamente il personale del Sistemi Informativi)

11 Gestione degli incidenti

Per questo argomento si rimanda alla specifica procedura Aziendale "Gestione degli incidenti di sicurezza delle informazioni".

12 Sicurezza fisica e ambientale

12.1 Planimetria e classificazione aree sicure

La planimetria del sito ALDEGHI è disponibile in formato cartaceo presso il Centralino ed in formato digitale (.dwg) presso l'Ufficio HSE di MSA.
Le aree considerate sicure per la presenza dei dati e delle informazioni sono classificate come di seguito:

ALTA: Infermeria
BASSA: gli altri Uffici

12.2 Sicurezza del perimetro aziendale

Il perimetro aziendale è protetto da allarme interno ad infrarossi e da telecamere.
Il servizio telecamere è presidiato durante l'orario non lavorativo dalla portineria di MSA.

12.3 Gestione accessi dipendenti

L'accesso ai dipendenti avviene dall'ingresso principale col proprio badge che attiva una registrazione dell'accesso avvenuto.

12.4 Gestione accessi visitatori

La Direzione Aziendale Aldeghi, per gestire al meglio l'ingresso dei visitatori, si impegna ad acquistare un programma dedicato a tale scopo entro il 30/06/2019.

12.5 Videosorveglianza

L'Azienda è dotata di un Sistema di videosorveglianza che copre tutto il perimetro aziendale.

12.6 Sicurezza degli apparati e dei dispositivi

Apparati e dispositivi che contengono dati sensibili sono custoditi all'interno di armadi chiusi a chiave.

12.7 Riutilizzo e smaltimento sicuro dei dispositivi

Tutti i dispositivi vengono smaltiti tramite appositi smaltitori autorizzati al trasporto ed allo smaltimento.

A questi "rifiuti" viene attribuito il codice CER relativo.
Il corretto avvenuto smaltimento è garantito dalla restituzione da parte dello smaltitore della quarta copia del formulario.
La procedura di smaltimento dei rifiuti è gestita da una persona dedicata.
Per quanto riguarda i dispositivi che contengono supporti informatici, questi sono cancellati e/o distrutti prima dello smaltimento.
Per quanto riguarda i dispositivi riutilizzati, questi vengono "resettati" (compresa la totale cancellazione dei dati) prima del loro reimpiego.

12.8 Conservazione dati relativi al personale

Tutti i dati relativi al personale e ritenuti sensibili vengono conservati in appositi armadi chiusi a chiave.

13 Consapevolezza e formazione sulla sicurezza delle informazioni

13.1 Informativa ai nuovi assunti

All'atto dell'assunzione il personale riceve documentazione ("Informativa Privacy") relativa al trattamento dei dati ed alle responsabilità ad esso collegate.
Per quanto sopra facciamo riferimento alla "Procedura Inserimento Personale", disponibile presso l'Ufficio del Personale.

13.2 Piani di formazione

Tra i numerosi Piani di Formazione che l'Azienda è solita organizzare sono previste anche sessioni relative al trattamento e consapevolezza della sicurezza sulle informazioni. I Piani formativi sono reperibili presso l'Ufficio del Personale.

13.3 Educazione continua

L'Azienda è impegnata nel mantenere costantemente formati ed informati i propri dipendenti.

14 Appendice

14.1 Comunicazione sulle password

Da:
Inviato: *martedì 6 febbraio 2018 13.23*
A:
Oggetto: *Decreto Legge sulla Privacy: gestione delle password - 06/02/18*
Priorità: *Alta*

Per rinfrescare (e notificare ai nuovi arrivati) quanto previsto per la gestione delle password personali nel rispetto del Decreto Legge sulla Privacy, inoltriamo periodicamente quanto segue.

Si chiede ai Responsabili di passare la comunicazione ai propri collaboratori che non hanno la posta elettronica.

Le regole sono valide anche per ALDEGHI.

Per le password in ambiente Windows è necessario utilizzare una combinazione di caratteri speciali (es. +, %, ecc.), lettere maiuscole e minuscole per renderne più complessa l'individuazione. Ciò non è possibile in AS/400.

Evitare l'utilizzo di password molto comuni come per es. quelle che contengono solo il proprio nome o cognome e l'anno di nascita o l'anno attuale (Es. "paolo2016").

----- Inoltrato il 11/06/2004 17.08 -----

17/05/2004 11.02

Per: TuttiUtenti
Cc:
Oggetto: Gestione delle password in base al nuovo Decreto Legge sulla Privacy

A partire dall'1 gennaio 2004 è entrato in vigore Il Testo Unico sulla Privacy (D.Lgs 196/2003) che impone anche alcune regole per le password di accesso ai sistemi informatici dove risiedono dati personali:

(*) la password deve avere lunghezza minima di 8 caratteri

(*) la password deve essere cambiata con una frequenza almeno semestrale (tre mesi per i dati "sensibili")

(*) la password è riservata e personale

Le password devono inoltre contenere sia lettere che numeri per renderne più difficile l'identificazione.

Ogni utente è responsabile delle eventuali conseguenze causate da una non corretta applicazione di queste minime regole.

Per allineare il nostro sistema a quanto richiesto dalla Legge dobbiamo operare come segue:

(*) AS/400:
sull'AS/400 è già impostata la richiesta periodica automatica di modifica delle password. L'unica operazione che dovrete fare sarà quella di inserire, alla prossima scadenza, una password composta da un minimo di 8 tra caratteri e numeri.

(*) Rete:
sul sistema sarà impostato nei prossimi giorni un meccanismo che Vi chiederà di cambiare forzatamente la password per accedere alla rete. Sarà questo l'istante in cui regolarizzarsi e inserire una nuova password (seguendo le istruzioni a video) composta da un minimo di 8 tra caratteri e numeri.
Da questo momento ciascuno di Voi sarà responsabile di modificarsi la password di rete periodicamente, attenendosi alle tempistiche e modalità richieste dalla Legge.

(*) Personal Computers:
anche eventuali password definite a livello del proprio PC devono seguire le stesse regole. Per queste password è necessario che le modifichiate personalmente (non ci sono sistemi automatici che possiamo applicare). Se necessario chiamateci per fare insieme la modifica.

Tutte le password devono essere regolarizzate entro il 30/06/04.

Si pregano i Responsabili di informare i propri collaboratori che non hanno la posta elettronica.

Il CED è a disposizione per qualsiasi aiuto fosse necessario per la corretta applicazione di quanto sopra.

Grazie per l'attenzione

14.2 Cancellazione dell'informazione e del dato

Ogni volta che un supporto di memoria deve essere eliminato è necessario procedere alla sua distruzione fisica affinchè qualche malintenzionato non possa accedere ai dati che vi erano in precedenza memorizzati.
In Azienda sono inoltre disponibili postazioni "distruggi documenti" a disposizione di tutti gli utenti e da utilizzare per i supporti cartacei contenenti informazioni da non divulgare.