POLITICA della SICUREZZA delle INFORMAZIONI

SCOPO

Le informazioni devono essere sempre protette, qualsiasi sia la loro forma e comunque condivise, comunicate o memorizzate.
La Sicurezza delle Informazioni è la protezione di informazioni da una vasta gamma di minacce, al fine di garantire la business continuità, ridurre al minimo i rischi e massimizzare il guadagno di investimenti e opportunità.

CAMPO DI APPLICAZIONE

- Questa politica sostiene l'organizzazione generale delle politiche per la sicurezza delle informazioni
- Questa politica si applica a tutta l'organizzazione.

OBIETTIVI

⇒ Rischi strategici e operativi per la sicurezza delle informazioni sono compresi e trattati per raggiungere un livello accettabile per l'organizzazione.

⇒ La riservatezza delle informazioni dei clienti, dello sviluppo del prodotto e dei piani di marketing è protetta.

⇒ L'integrità dei documenti contabili è conservata.

⇒ Pubblici servizi web e reti interne soddisfano determinati livelli di disponibilità.

PRINCIPI

- ✓ Questa organizzazione incoraggia l'analisi dei rischi e quindi può tollerare i rischi che potrebbero non essere tollerati in organizzazioni gestite in modo conservativo, a condizione che rischi concernenti le informazioni siano capiti, monitorati e trattati, se necessario, come previsto dal Sistema di Gestione conforme alla norma 27001.
- ✓ Tutto il personale è reso consapevole e responsabile per quanto riguarda la sicurezza delle informazioni rilevanti connesse al proprio ruolo.
- ✓ Sono state assegnate risorse per il finanziamento dei controlli di sicurezza delle informazioni .
- ✓ Nella gestione complessiva del sistema di informazione viene analizzata la possibilità di frode associata all'abuso dei sistemi di informazione.
- ✓ Sono disponibili evidenze oggettive sullo stato della Sicurezza delle Informazioni.
- ✓ I rischi per la Sicurezza delle Informazioni sono monitorati e sono intraprese idonee azioni qualora eventuali cambiamenti generino rischi che non sono accettabili dall'organizzazione.
- ✓ Nel Sistema di Gestione conforme alla norma 27001 sono descritti i criteri per la classificazione del rischio e il livello di accettabilità.
- ✓ Non saranno tollerate situazioni che pongono l'organizzazione in violazione di leggi e norme di legge.

RESPONSABILITÀ

- Il Responsabile della Sicurezza delle informazioni
  i) fornisce supporto per l'organizzazione del personale
  ii) garantisce che i verbali sullo stato della Sicurezza delle Informazioni siano disponibili
  iii) agisce in caso di incidente delle informazioni

- Ogni membro del personale ha responsabilità in materia di Sicurezza delle Informazioni come parte del proprio lavoro.

RISULTATI CHIAVE

1) Gli Incidenti di Sicurezza delle Informazioni non comporteranno costi gravi e imprevisti o un'interruzione di servizi e delle attività commerciali.
2) Le perdite dovute a frodi saranno conosciute e confinate entro limiti accettabili.
3) L'accettazione del Cliente di prodotti o servizi non sarà influenzata negativamente dalle preoccupazioni legate alla Sicurezza delle Informazioni.

RELATIVE POLITICHE

Per la corretta implementazione del sistema sono state definite, dall'organizzazione, delle politiche specifiche, raccolte in allegato.

SANT'ILARIO D'ENZA, 12/12/2018

IL DIRIGENTE SCOLASTICO

DOTT.SSA MARGHERITA ATTANASIO

POLITICA UTILIZZO ACCETTABILE

Un sistema di sicurezza efficace è fondato su un lavoro di squadra, con la partecipazione ed il sostegno di ogni dipendente e ogni affiliato che si occupa di informazioni e/o dei sistemi di informazione. È responsabilità di ogni utente del computer conoscere queste linee guida e svolgere la propria attività di conseguenza.

SCOPO

Lo scopo di questa politica è quello di delineare l'uso accettabile di apparecchiature informatiche dell'organizzazione. Queste regole sono in vigore per proteggere il personale dai rischi di un uso improprio degli assets dell'organizzazione:

- ⇒ Non conformità legislativa
- ⇒ Attacchi di virus
- ⇒ Compromissione dei sistemi e servizi di rete

CAMPO DI APPLICAZIONE

Questa politica si applica ai dipendenti, collaboratori, consulenti, lavoratori temporanei, incluso tutto il personale affiliato a terze parti e a tutte le attrezzature di proprietà o in leasing dell'organizzazione.

MODALITÀ OPERATIVE

Uso Generale e Proprietà

- ⇒ Si ha la responsabilità di segnalare tempestivamente il furto, la perdita o la divulgazione non autorizzata di informazioni riservate.
- ⇒ Si può accedere, utilizzare o condividere informazioni di proprietà dell'organizzazione solo nella misura in cui è autorizzato e necessario per eseguire le proprie funzioni.
- ⇒ I dipendenti sono responsabili nell'uso personale dei dispositivi e, in caso di incertezza della politica da adottare, devono consultare il proprio supervisore o manager.
- ⇒ Per garantire la sicurezza e la costante manutenzione della rete, soggetti autorizzati all'interno dell'impresa possono monitorare le attrezzature, i sistemi e il traffico di rete in qualsiasi momento.
- ⇒ Le informazioni cartacee devono essere conservate in luogo/struttura adeguatamente protetta.
- ⇒ L'organizzazione si riserva il diritto di eseguire audit di sistemi e reti su base periodica per garantirne la conformità con questa politica.

Sicurezza e Proprietà delle Informazioni

- ⇒ Tutti i cellulari e i computer che si connettono alla rete interna devono rispettare la politica dell'Access Control.
- ⇒ Sia a livello di Sistema, che a livello di utente, le password devono essere conformi alla Politica delle Password. Fornire l'accesso a un altro individuo, deliberatamente o per propria mancanza, è vietato.
- ⇒ Tutti i dispositivi di elaborazione devono essere protetti in base alla politica "Clear Desk, Clear Screen".
- ⇒ i Dipendenti devono prestare estrema attenzione durante l'apertura di allegati di posta elettronica ricevuti da mittenti sconosciuti: potrebbero contenere malware.

Uso Inaccettabile
Le seguenti attività sono, in generale, vietate, tranne specifiche esenzioni, concesse per svolgere legittime responsabilità lavorative.
In nessun caso un dipendente è autorizzato a svolgere qualsiasi attività illecita ai sensi della legge locale, statale o internazionale, utilizzando risorse di proprietà dell'organizzazione.

Di seguito è riportato un elenco – da non considerarsi in alcun modo esaustivo - di attività che rientrano nella categoria di utilizzo inaccettabile nel tentativo di fornire un quadro di riferimento:

1. La violazioni dei diritti di qualsiasi persona o azienda protetti da copyright, segreto commerciale, brevetti o altri diritti di proprietà intellettuale, o simili leggi o regolamenti, tra cui, ma non limitato a, l'installazione e/o la distribuzione "pirata" o senza adeguata licenza d'uso del software
2. La copia non autorizzata di materiale protetto da copyright, tra cui, ma non limitato a, la digitalizzazione e la distribuzione di fotografie da riviste, libri o altro materiale protetto da copyright, musica protetta da copyright, e l'installazione di qualsiasi software protetto da copyright, per cui l'organizzazione o l'utente finale non dispone di una licenza attiva, è severamente proibito.
3. L'accesso ai dati di un server o di un account per qualsiasi scopo diverso da quello lavorativo, anche se si dispone di accesso autorizzato, è vietato.
4. L'esportazione di software, informazioni tecniche, software o tecnologia di cifratura, in violazione di norme internazionali o regionali, è illegale.
5. L'introduzione di programmi malevoli in rete o nel server (ad esempio, virus, cavalli di Troia, e-mail, etc.).
6. Rivelare la password del tuo account ad altri o consentire l'uso del proprio account da parte di altri. Questo include la famiglia, quando si lavora a casa.
7. Utilizzare un asset dell'impresa per attivamente ottenere o trasmettere materiale che viola le leggi concernenti le molestie sessuali o l'ambiente di lavoro ostile.
8. Fare offerte fraudolente di prodotti, oggetti o servizi provenienti da un qualsiasi account dell'organizzazione.
9. La realizzazione di violazioni della sicurezza o di interruzioni dell'attività di rete.
   Le violazioni della sicurezza comprendono, ma non sono limitate a:
   - l'accesso ai dati di cui il dipendente non è un destinatario.
   - l'accesso a un server o a un account a cui il dipendente non è espressamente autorizzato.

   Ai fini della presente politica, l'"interruzione delle attività" include, ma non è limitata a:
   - Denail of service: malfunzionamento dovuto ad un attacco informatico che impedisce al sistema di svolgere la propria attività ordinaria
10. La scansione delle porte o scansione di sicurezza, è espressamente vietata senza la preventiva segnalazione.
11. L'esecuzione di qualsiasi forma di monitoraggio della rete che è in grado di intercettare i dati non destinati al dipendente, a meno che faccia parte dell'attività lavorativa.
12. Fornire informazioni in merito o gli elenchi dei dipendenti a soggetti esterni.

SANT'ILARIO D'ENZA, 12/12/2018

IL DIRIGENTE SCOLASTICO

DOTT.SSA MARGHERITA ATTANASIO

POLITICA ACCESS CONTROL

SCOPO

Questa politica definisce gli utenti che hanno l'accesso e il controllo su dati sensibili o specialmente regolamentati ed è stata progettata per ridurre al minimo il rischio di danni nei confronti delle risorse e dei dati dell'organizzazione. Viene stabilito il privilegio di accesso degli utenti in relazione a dati e dispositivi per permettere agli utenti di eseguire le loro funzioni lavorative senza particolare disagio.

CAMPO DI APPLICAZIONE

Questa politica si applica a tutto il personale dell'organizzazione.

MODALITÀ OPERATIVE

Privilegi del Computer Locale
Ci sono tre categorie principali di utenti su un computer o una rete. Queste categorie includono:

1. Utente Limitato → Può utilizzare il computer e salvare i documenti, ma non può modificare le impostazioni di sistema.
2. Utente Standard → Può modificare le impostazioni di sistema e installare programmi che non coinvolgono i file del sistema operativo.
3. Amministratori → Hanno accesso completo nel leggere e scrivere i dati sul sistema, aggiungere/rimuovere programmi o modificare le impostazioni di sistema.

   La maggior parte degli utenti sulle reti comuni devono essere classificati come "Utente Limitato".
   Solo agli utenti con formazione speciale o necessità di un accesso ulteriore deve essere consentito di cambiare le impostazioni di sistema e installare i programmi che non sono programmi del sistema operativo. Questo perché molti virus, adware (Software sovvenzionato da pubblicità) o spyware (Software spia) possono essere installati in modo da ingannare l'utente. Se l'utente non ha la possibilità di installare programmi o modificare le impostazioni rendendole più vulnerabili, la maggior parte di questi potenziali problemi di sicurezza possono essere evitati.

Il livello di accesso è strettamente legato al ruolo dell'utente, può essere modificato solo dopo la dimostrazione dell'assoluta necessità per lo svolgimento delle funzioni lavorative, inoltre deve essere approvato dal responsabile della sicurezza delle informazioni prima di poter diventare effettivo.

Gruppi che possono essere ammessi ad un tipo di accesso ulteriore includono:
- ⇒ gli Amministratori di Dominio
- ⇒ gli Sviluppatori di applicazioni a scopo di test che hanno una conosciuta educazione o abilità informatica.

Privilegi di Rete
La Maggior parte degli utenti della rete potranno accedere ai seguenti tipi di risorse di rete:

a) E-Mail → la Maggior parte degli utenti avrà pieno accesso alla propria e-mail. Essi non saranno in grado di trasferire la proprietà a qualcun altro.
b) Un personale spazio di archiviazione (drive) su un file server di rete → Si tratta di una cartella in uno spazio di archiviazione che solo l'utente principale di questa unità è in grado di leggere e modificare, con l'eccezione degli amministratori del dominio. L'utente non potrà trasferire la proprietà a qualcun altro.

c) Un gruppo condiviso della drive → Questa è una cartella a cui i membri di determinati gruppi o divisioni dell'organizzazione possono accedere. L'accesso può essere limitato alla lettura e/o alla scrittura e può variare per esigenze organizzative.
d) Accesso alle banche dati (database) → Ci possono essere ulteriori banche dati che possono essere memorizzate su una drive condivisa, o su qualche altra risorsa. La maggior parte dei database dispone di un livello d'uso standard che consente agli utenti, con un'autorizzazione appropriata, di inserire dati e leggere le informazioni dei report. Tuttavia solo gli amministratori della banca dati avranno pieno accesso a tutte le risorse del database che amministrano.

Gruppi a cui può essere concesso un livello di accesso ulteriore includono:

- Operatore Backup → Ha il permesso di leggere i dati sul dominio con lo scopo di salvare i file sul supporto di backup. Questo gruppo non può modificare i dati di un dominio.
- Operatore Account → E' in grado di gestire e visualizzare le informazioni sull'account utente del dominio.
- Operatore Server → Ha dei privilegi concernenti i server, tra cui la lettura e la scrittura dei dati, l'installazione di programmi, e la modifica delle impostazioni.
- Amministratore Dominio → Ha privilegi su tutti i computer del dominio, compresi i server e workstation. Privilegi includono la lettura e la scrittura dei dati, l'installazione di programmi, e la modifica delle impostazioni.

REGOLAMENTO
Poiché la sicurezza e l'integrità dei dati, insieme alla protezione delle risorse, sono fondamentali per il funzionamento dell'organizzazione, i dipendenti che non rispettano questo regolamento possono essere soggetti a provvedimenti disciplinari, incluso il licenziamento.

SANT'ILARIO D'ENZA, 12/12/2018

IL DIRIGENTE SCOLASTICO

DOTT.SSA MARGHERITA ATTANASIO

POLITICA PASSWORD

SCOPO

Tutti i dipendenti ed il personale che ha accesso ai computer dell'organizzazione devono rispettare i criteri di password definiti nella seguente politica, al fine di proteggere:

- ✓ la sicurezza della rete
- ✓ l'integrità dei dati
- ✓ i sistemi informatici.

CAMPO DI APPLICAZIONE

Questa politica si applica a tutte le persone che hanno un account che richiede una password su un computer collegato alla rete aziendale (Es. account di dominio, account di posta elettronica, etc.).

MODALITÀ OPERATIVE

Questa politica è stata definita per proteggere le risorse organizzative della rete mediante la richiesta di password complesse unitamente alla protezione di queste password e nello stabilire un tempo minimo tra le modifiche delle password.

Protezione della Password

a) Non annotare mai la password.
b) Non inviare mai una password tramite e-mail.
c) Non includere una password documento archiviato non-crittografato.
d) Non dire mai a nessuno la tua password.
e) Non rivelare la propria password al telefono.
f) Non accennare mai al formato della password.
g) Non rivelare o suggerire la propria password in un modulo in internet.
h) Non utilizzare mai l'opzione "ricorda password", di programmi come internet explorer, di posta elettronica, o qualsiasi altro programma.
i) Non utilizzare mai la password aziendale o di rete per un account internet, che non dispone di un accesso protetto (dove l'indirizzo browser web inizia con https:// invece di http:/).
j) Segnalare eventuali sospetti concernenti la sicurezza della password al reparto/incaricato della sicurezza it.
k) Se qualcuno ti chiede la password, indirizzali al reparto/incaricato di sicurezza it.
l) Non usare acronimi comuni come parte della password.
m) Non usare parole comuni o invertire l'ortografia delle parole come parte della password.
n) Non utilizzare nomi di persone o luoghi, come parte della password.

o) Non utilizzare una parte del tuo nome utente per la tua password.

p) Non utilizzare parti di numeri facili da ricordare, come numeri di telefono, numeri di indirizzo o altro di similare .

q) Stare attenti a lasciare che qualcuno veda la digitazione della password.

Requisiti di Password (soggetto a variazioni)

Coloro che fissano i requisiti di password devono ricordare che rendere queste regole troppo difficili può effettivamente diminuire la sicurezza: gli utenti possono decidere che sono impossibili da soddisfare o, se le password sono cambiate troppo spesso, gli utenti tendono ad annotarle o rendere la loro nuova password una variante di una vecchia, cosa che la renderebbe più vulnerabile ad un attacco. I seguenti requisiti di password verranno impostati dal reparto/incaricato di sicurezza IT:

- ✓ Lunghezza Minima → 8 caratteri raccomandato
- ✓ Lunghezza Massima → 14 caratteri
- ✓ Minimo livello di complessità → Nessuna parola del dizionario. Ciascuna password deve includere tre o quattro dei seguenti tipi di caratteri:
  - o Minuscole
  - o Maiuscole
  - o Numeri
  - o caratteri Speciali, ad esempio !@#$%^&*(){}[]
- ✓ le Password differenziano tra maiuscole e minuscole, mentre il nome utente o l'ID di accesso no.
- ✓ Ripetizione Password → numero min. di password prima che una vecchia password possa essere riutilizzata: questo numero non deve essere inferiore a 24.
- ✓ Validità Massima password → 180 giorni.
- ✓ Validità Minima password → 2 giorni.
- ✓ Memorizzare le password tramite crittografia reversibile → Questo non dovrebbe essere fatto senza una speciale autorizzazione da parte del reparto/incaricato IT, dato che ne ridurrebbe il livello di protezione.
- ✓ Soglia di blocco degli Account → 4 tentativi di login falliti.
- ✓ Reset blocco account → Il tempo che intercorre tra tentativi di accesso non valido e la possibilità di ritentare: il valore raccomandato è di 20 minuti. Questo significa che se ci sono tre tentativi non validi in 20 minuti, l'account verrà bloccato.
- ✓ Account durata di blocco → Alcuni esperti raccomandano che il blocco dell'account sia compreso tra 30 minuti e 2 ore.
- ✓ Uno Screen saver protetto da Password dovrebbe essere attivato e dovrebbe proteggere il computer entro 5 minuti di inattività dell'utente. Il computer non dovrebbe essere lasciato incustodito mentre è connesso (logged-on) e senza aver attivato uno screen saver protetto da password. Gli utenti dovrebbero avere l'abitudine di non lasciare i loro computer sbloccati; per facilitarne il compito si può impostare una combinazione rapida di tasti (es. CTRL-ALT-CANC e selezionare "Blocca Computer").
- ✓ Le regole che si applicano per le password, sono applicate anche alle frasi che vengono utilizzate per l'autenticazione della chiave pubblica/privata

Scelta della Password

In primo luogo bisogna essere sicuri che la password soddisfi i requisiti minimi delle linee guida sopra citate, di seguito sono elencati alcuni suggerimenti per la creazione di una nuova password:

- ✓ Incorporare una parola o parte di una parola all'interno di un altra. ***Es.*** Mare + sabbia. Password: "Marebbia".
- ✓ Sbagliare volontariamente l'ortografia di una parola, soprattutto se si usa una sola parola come parte della vostra password. ***Es.*** Cioccolato. Password: "Ciocolatto".
- ✓ Utilizzare una frase che è personale e usare il primo, il secondo o il terzo carattere di ogni parola nella frase. Ci possono essere diverse varianti di questo approccio:
  - o Utilizzare una frase che ha un numero alla fine.

    Es. Il mio numero preferito è 333. Password: "IMNPE333"
  - o Dopo la creazione della password, combinare i numeri e caratteri in modo che da poterli ricordare.

    Es. Quanto darò oggi? Il 100%. Password: "qdo?I100%"
  - o Usare lettere maiuscole e lettere minuscole in modo insolito.

    Es. Non rimandare a domani ciò che puoi fare oggi! Password: "NraDccpfO!"
  - o Utilizzare una rappresentazione numerica delle lettere dell'alfabeto per parte della frase o parte di una parola. Per esempio A è 1, B 2, C 3, etc.

    Es. Il nome di mia nonna è Gina. Password: "IndMnè79121".
  - o Utilizzare i segni di punteggiatura o caratteri speciali.

    Es. Preferisci mare o montagna? Mare. Password: "Pm/m?111165"

    ⇒ In molti degli esempi sopra citati, è facile inserire punteggiatura come "?" quando parte della frase è una domanda. Se la frase coinvolge numeri aggiungere $, %, # può facilitarne l'uso. Se nella frase si usa la lettera "e" o "o", è possibile sostituire "&" o "|". Inoltre, è possibile dividere le password con "/" o "\".

Applicazione

Dal momento che la password di protezione è fondamentale per la sicurezza dell'organizzazione, tutti i dipendenti che non rispettano questa politica possono essere soggetti a provvedimenti disciplinari.

Altre Considerazioni

Le password dell'account di Amministratore devono essere protette con particolare attenzione: dovrebbe essere consentito esclusivamente il livello minimo di accesso necessario per lo svolgimento della loro funzione e non devono essere condivise.

SANT'ILARIO D'ENZA, 12/12/2018

IL DIRIGENTE SCOLASTICO

DOTT.SSA MARGHERITA ATTANASIO

POLITICA CLEAR DESK CLEAR SCREEN

SCOPO

Per migliorare la sicurezza e la riservatezza delle informazioni, l'organizzazione ha adottato una politica "clear desk" (scrivania pulita) per documenti e supporti di archiviazione rimovibili, ed una politica "clear screen" (schermo pulito) per gli strumenti di elaborazione delle informazioni.
Questo al fine di ridurre il rischio di accessi non autorizzati, perdita e danneggiamento di informazioni durante e al di fuori del normale orario di lavoro o quando le aree non sono presidiate.

CAMPO DI APPLICAZIONE

Questa politica si applica a tutto il personale dell'organizzazione.

MODALITÀ OPERATIVE

Clear Desk

- Ove possibile, carta e supporti informatici devono essere conservati in apposite casseforti, armadi o altre forme di protezione quando non sono in uso, soprattutto al di fuori dell'orario di lavoro.
- Le porte delle aree di ufficio devono essere chiuse a chiave quando non sono in uso o non sono vigilate.
- Informazioni riservate, sensibili o classificate, una volta stampate, devono essere rimosse immediatamente dalle stampanti. Ove possibile, devono essere utilizzate le stampanti con l'opzione di inserimento password per la protezione dei documenti.
- Utilizzare appositi cestini di sicurezza per eliminare fogli con informazioni sensibili o personali di cui non si ha più bisogno.
- Considerare la scansione di documenti e la conservazione sul PC.
- Notare che le informazioni lasciate sulla scrivania hanno più probabilità di essere danneggiate o distrutte in una situazione di emergenza come incendio, inondazione o esplosione.
- Non stampare le email per leggerle: aumenta soltanto la quantità di disordine.
- La scrivania della reception può essere particolarmente vulnerabile ai visitatori. Questa zona deve essere mantenuta il più "pulita" possibile in ogni momento; in particolare, la documentazione medica o altre informazioni personali non dovrebbero essere tenute sulla scrivania a portata/vista dei visitatori.
- Liberare sempre la scrivania prima di andare a casa.

Clear Screen

- Gli utenti devono SEMPRE "log-off"(disconnettersi), quando lasciano il computer incustodito.
- Impostare il Blocco schermo di Windows affinché si attivi automaticamente quando non vi è alcuna attività per un breve predeterminato periodo di tempo.
- Il Blocco schermo di Windows deve essere protetto da password per la riattivazione.
- Le password non devono essere annotate su/sotto al computer o in qualsiasi altra posizione accessibile.

Modalità di Monitoraggio e Revisione

Tutto il personale è responsabile nel monitorare il proprio rispetto dei principi/procedure descritti in questa politica. Questa politica sarà soggetta a revisione periodica durante il Riesame della Direzione.

Una revisione eccezionale può essere giustificata se si verifica una delle seguenti situazioni:

- Sono avvenute cambiamenti societari (es. Statutari);
- In base ai risultati/effetti di incidenti critici;
- Per ogni altra pertinente ragione.

Non Conformità

C'è un obbligo per tutto il personale di conformarsi alla presente politica e, ove richiesto, di dimostrare tale conformità. L'inosservanza di tale obbligo sarà considerata al pari di un incidente disciplinare e sarà trattata di conseguenza.

SANT'ILARIO D'ENZA, 12/12/2018

IL DIRIGENTE SCOLASTICO

DOTT.SSA MARGHERITA ATTANASIO

POLITICA BACKUP

SCOPO

Questa politica definisce i criteri di backup per i computer all'interno dell'organizzazione che necessitano del backup dei dati. Questi sistemi sono in genere i server (file server, server di posta e il server web) ma non sono necessariamente limitati a questi.
Questa politica ha il fine di proteggere i dati dell'organizzazione garantendo che non vadano persi e possano essere recuperati in caso di un guasto delle apparecchiature, una distruzione di dati intenzionale, o un'emergenza.

CAMPO DI APPLICAZIONE

Questa politica si applica a tutte le attrezzature e ai dati di proprietà e/o gestiti dall'organizzazione.

MODALITÀ OPERATIVE

Definizioni
Backup → Il salvataggio di file su supporto di memorizzazione off-line (disconnesso dalla rete) con lo scopo di prevenire la perdita dei dati in caso di guasto o distruzione delle apparecchiature.
Archivio → Il salvataggio di vecchi o inutilizzati file off-line al fine di catalogarli e alleggerire il sistema.
Ripristina → Il processo di riportare dati conservati off-line, in un sistema di archiviazione online come un file server.

Tempi
Backup completi vengono eseguiti con cadenza settimanale. Se, per ragioni di manutenzione, non vengono eseguiti backup il venerdì, devono essere fatti il sabato o la domenica.

L'archiviazione dei supporti Backup (se presenti)
Devono essere conservati in modo adeguato al fine di prevenirne il danneggiamento.

Responsabilità
La Direzione deve incaricare un membro che ha il compito di eseguire backup regolari. La persona delegata deve sviluppare una procedura per testare i backup e provare mensilmente la capacità di ripristino dei dati.

Test
La capacità di ripristinare i dati dal backup deve essere eseguita almeno una volta al mese.

Dati di Backup
I dati che necessitano il backup includono le seguenti informazioni:

- ✓ I dati dell'Utente.
- ✓ I dati dello stato del Sistema
- ✓ Il Registro di Sistema

Sistemi di backup includono ma non sono limitati a:

- File server
- Server di Posta
- Server di Produzione web
- Server di Produzione database
- Controller di dominio
- Server di Database Test
- Server di Web Test

Archivi
Archivi sono effettuati alla fine di ogni anno, nel mese di dicembre. I dati di account utente, i file e il server di posta elettronica sono archiviati un mese dopo aver lasciato l'organizzazione.

Ripristino
Gli Utenti che hanno bisogno di file ripristinati, devono presentare una richiesta alla funzione individuata, includendo informazioni circa la data di creazione del file, il nome del file, l'ultima volta che è stato cambiato, e la data e l'ora in cui è stato cancellato o distrutto.

SANT'ILARIO D'ENZA, 12/12/2018

IL DIRIGENTE SCOLASTICO

DOTT.SSA MARGHERITA ATTANASIO

POLITICA PER LA GESTIONE DEGLI INCIDENTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI

SCOPO

L'obiettivo di questa politica è quello di garantire che l'impresa reagisca in modo appropriato a qualsiasi tipologia, effettiva o presunta, di incidenti di sicurezza relativamente ai sistemi informativi e ai dati.
L'organizzazione ha la responsabilità di monitorare tutti gli incidenti che si verificano al suo interno che possono violare la sicurezza e/o la riservatezza delle informazioni. Tutti gli incidenti devono essere identificati, segnalati, studiati e monitorati: lo scopo principale di questa politica non è quello di attribuire colpe, ma di contenere i problemi e apprendere dagli errori in ottica di miglioramento continuo.

CAMPO DI APPLICAZIONE

Questa politica si applica a tutti i dipendenti, collaboratori, consulenti, lavoratori temporanei all'interno dell'organizzazione.

MODALITÀ OPERATIVE

Partiamo dalla definizione: con "incidenti di sicurezza delle informazioni" s'intende un evento avverso che ha causato o ha il potenziale di causare danni agli assets, alla reputazione e/o al personale dell'organizzazione, attraverso l'intrusione, la compromissione e l'abuso di informazioni e risorse. Quindi è la realizzazione di una delle minacce analizzate nel Risk Assessment dell'organizzazione.

Tipi di Incidenti

Le principali categorie di incidente sono:

- Incidenti **CRITICI** devono essere segnalati immediatamente
  Es.
  - furto di documenti
  - computer infettato da virus
- Incidenti **SIGNIFICATIVI** devono essere segnalati entro 4 ore
  Es.
  - uso di un software privo di licenza
  - accesso e/o uso non autorizzato dei dati di accesso di un altro utente
- Incidenti **MINORI** devono essere segnalati entro 1 giorno
  Es.
  - Tentata penetrazione delle difese
  - Spedizioni email non appropriate

Rischi

L'organizzazione riconosce che ci sono dei rischi associati all'accesso degli utenti e alla gestione delle informazioni nello svolgimento delle proprie attività, infatti questa politica mira a:

- ✓ Ridurre l'impatto delle violazioni di sicurezza, assicurando che gli incidenti siano seguiti correttamente.
- ✓ Aiutare a identificare le aree di miglioramento per ridurre il rischio e l'impatto di futuri incidenti.
- ✓ Ridurre il numero degli incidenti

Non conformità con questa politica potrebbe avere un impatto significativo sull'efficienza del funzionamento dell'organizzazione e può causare perdite finanziarie, multe e l'impossibilità di fornire i servizi necessari ai nostri clienti.

Procedura da seguire

Fase 1 **RILEVAZIONE INCIDENTE**

Un incidente può e deve essere rilevato:

- ✓ Dal personale operativo nello svolgimento delle proprie attività.
- ✓ Dall'avviso automatico dei dispositivi che monitorano le proprie attività di sistema.
- ✓ Dall' utente finale.

Fase 2 **VALUTAZIONE INCIDENTE**

Lo scopo di questa fase è quello di determinare rapidamente e con precisione se l'incidente è un incidente grave.

- ✓ Raccolta dati del problema iniziale - I dati sono raccolti e viene fatta un'appropriata classificazione dell'Impatto.
- ✓ Valutazione dell'Incidente - l'incidente è valutato e la relativa categoria è confermata dal Responsabile della Sicurezza delle informazioni.
- ✓ Incidente Grave - Se l'incidente è classificato come 'Critico', la valutazione deve essere confermata entro 60 minuti dalla rilevazione.

Fase 3 **COMUNICAZIONE INCIDENTE**

I processi di comunicazione hanno lo scopo di garantire che tutte le parti siano informate dello stato dell'incidente.

- ✓ I Responsabili di progetto e/o le parti coinvolte devono essere informati dell'incidente e tenuti aggiornati sui relativi progressi per consentire loro di gestire i propri clienti.
- ✓ In casi di incidente grave la Direzione deve essere informata e tenuta aggiornata.
- ✓ Qualora la violazione possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare di trattamento notifica al Garante entro 72h dal momento in cui ne è venuto a conoscenza. (Vedi *Modulo Segnalazione Data Breach*).

Fase 4 **RISOLUZIONE INCIDENTE**

Questa fase comprende tutte le varie indagini tecniche che saranno necessarie per portare l'incidente a risoluzione; può richiedere l'intervento di diverse figure tecniche e non – si prevede che le risorse siano rese disponibili su richiesta.

Fase 5 **POST-RISOLUZIONE INCIDENTE**

Il processo di post-risoluzione è avviato una volta che l'incidente è stato risolto.

⇒ *Riesame Incidente Critico*: Il Responsabile della Sicurezza delle Informazioni, in occasione di incidente grave, indice una riunione di riesame entro 3 giorni lavorativi dalla data di risoluzione dell'incidente, alla quale partecipa il personale coinvolto.

⇒ *Verbale Incidente Critico*: E' costituito dal verbale della riunione di riesame: riassume gli eventi dell'incidente, l'impatto, le azioni intraprese per risolvere l'incidente e le ulteriori misure adottate per ridurre il rischio di accadimento futuro/impatto.

⇒ *Incidente Non Critico*: E' segnalato tramite la compilazione di un verbale (**M 10.1.1 Rilevazione NC**) firmato dal Responsabile della Sicurezza; non è necessaria riunione apposita.

SANT'ILARIO D'ENZA, 12/12/2018

IL DIRIGENTE SCOLASTICO

DOTT.SSA MARGHERITA ATTANASIO