



ENTAKSI SOLUTIONS

AZIENDA CON SISTEMA INTEGRATO DI GESTIONE
QUALITÀ, SICUREZZA DELLE INFORMAZIONI, SERVIZI
ISO 9001 | ISO 27001 | ISO 20000-1
CONSERVATORE ACCREDITATO AGID

Istruzioni operative

IO ISO 20170621 Disposizione sulla sicurezza delle informazioni

Entaksi Solutions Srl

Indice

Informazioni sul documento	1
Revisioni e relative distribuzioni	1
Approvazione del documento	2
1. Introduzione	3
1.1. Obiettivi del documento	3
1.2. Campo di applicazione	3
1.3. Definizioni e documentazione di riferimento	3
2. Disposizione sulla sicurezza delle informazioni	4
2.1. Sistema di Conservazione	4
2.2. Ruoli e responsabilità	4
2.3. Mantenimento del documento	5
3. Regole sulla sicurezza delle informazioni	6
4. Classificazione delle informazioni	7
4.1. Sistema di conservazione	7
5. Procedure e politiche relative alla sicurezza delle informazioni	8
5.1. Protezione dei dati	8
5.2. Accessi	8
5.3. Password	9
5.4. Gestione della documentazione	10
5.5. Crittografia	11
5.6. Contromisure per attacchi informatici basati su malware/virus	11
5.7. Sviluppo sicuro	13
5.8. Gestione degli incidenti	13

Informazioni sul documento

Progetto	Sistema Integrato di Gestione
Tipo	Istruzione Operativa
Nome documento	IO ISO 20170621 Disposizione sulla sicurezza delle informazioni
Versione	1.3.0
Data creazione	21/06/2017
Ultima revisione	24/01/2020
Autore	Alessia Soccio
Stato	Rilasciato
Classificazione	Pubblico



Riproduzioni cartacee di questo documento sono da considerarsi copie di lavoro non censite dal SIG.

Revisioni e relative distribuzioni

Data	Versione	Nome	Mansione	Azione	Distribuzione
21/06/2017	0.0.1	Alessia Soccio	RFAC	Creazione bozza	Interno
21/06/2017	1.0.0	Alessia Soccio	RFAC	Revisione e rilascio	Pubblico
21/06/2017	1.0.0	Alessia Soccio	RFAC	Conversione del documento nel nuovo formato. Nuovo template. Aggiornamento al nuovo sistema di versionamento. Aggiunto § "Sistema di conservazione" nel capitolo "Classificazione delle informazioni".	Pubblico
07/09/2017	1.1.1	Alessia Soccio	RFAC	Modifica template.	Pubblico
01/12/2017	1.1.2	Alessia Soccio	RFAC	Aggiunta descrizione log out automatico nelle procedure e modalità di gestione delle chiavi crittografiche.	Pubblico
23/10/2019	1.2.0	Alessia Soccio	RFAC	Aggiornato capitolo "Procedure e politiche relative alla sicurezza delle informazioni".	Pubblico
24/01/2020	1.3.0	Alessia Soccio	RFAC	Aggiunto capitolo sulla gestione degli incidenti.	Pubblico

Approvazione del documento

Data	Addetto	Mansione	Firma
24/01/2020	Alessandro Geri	Responsabile del SIG	<i>Firmato digitalmente</i>

© 2020 Entaksi Solutions

Le informazioni contenute nel presente documento sono di proprietà di Entaksi Solutions, sono fornite ai destinatari in via riservata e confidenziale e non possono essere usate per fini produttivi, né comunicate a terzi o riprodotte, per intero o in parte, senza il consenso scritto di Entaksi Solutions.

1. Introduzione

1.1. Obiettivi del documento

Il presente documento contiene la dichiarazione delle politiche adottate da Entaksi Solutions Srl riguardo la sicurezza delle informazioni, e corrisponde a quello che viene anche chiamato *Information Security Policy Document (ISPD)*.

L'obiettivo principale di questa disposizione è documentare tutte le strategie e gli accorgimenti procedurali attraverso i quali Entaksi si propone di tutelare le informazioni documentate presenti a qualunque titolo nel proprio sistema informativo.

La finalità generale è quella di garantire un adeguato livello di protezione dei dati, che comprendono sia quelli dell'azienda che quelli conservati e gestiti per clienti e terze parti. Il presente documento espone il progetto di sicurezza dell'azienda, ed i suoi obiettivi corrispondono a quelli del Sistema di Gestione della Sicurezza delle Informazioni (SiGSI):

- assicurare l'adozione di procedure finalizzate alla progettazione, all'utilizzo e al mantenimento dei livelli di sicurezza delle informazioni;
- assolvere ai requisiti legislativi, siano essi norme o standard di riferimento, stabiliti per il SiGSI;
- garantire che le procedure attuate siano diffuse fra le parti interessate.

Questi propositi vengono perseguiti attenendosi agli standard internazionali di riferimento in materia e alle disposizioni legislative vigenti in materia di sicurezza, privacy, trattamento dei dati.

Questo documento riassume in forma di disposizione i requisiti e le relative procedure riguardanti la sicurezza delle informazioni così come espressi nei vari documenti nel Sistema Integrato di Gestione di Entaksi.

1.2. Campo di applicazione

La presente disposizione si applica ad ogni Utente assegnatario di beni e risorse informatiche aziendali ovvero utilizzatore di servizi e risorse informative di pertinenza della Società.

La presente disposizione è pubblica, in quanto i principi in essa contenuti riguardano anche aspetti relativi ai servizi erogati da Entaksi, e pertanto si ritiene opportuno che gli utenti che utilizzano tali servizi siano messi a conoscenza di tutte le azioni e le procedure interne intraprese da Entaksi a salvaguardia delle informazioni raccolte o conservate dalla Società.

1.3. Definizioni e documentazione di riferimento

Per *Utente* si intende a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore (interno o esterno), consulente, fornitore e/o terzo che in modo continuativo e non occasionale operi all'interno della struttura aziendale utilizzandone beni e servizi informatici.

Per *Società* si intende, invece, la società Entaksi Solutions Srl, la quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

Per le altre definizioni e le abbreviazioni si rimanda allo specifico documento "MAN ISO 20130804 Definizioni".

Per i riferimenti alla documentazione, interna o esterna, si rimanda allo specifico documento "MAN ISO 20130804 Documentazione di riferimento".

2. Disposizione sulla sicurezza delle informazioni

Questo documento comprende tutti gli aspetti relativi a come Entaksi Solutions Srl tratta la sicurezza delle informazioni.

Entaksi gestisce quotidianamente informazioni appartenenti ai propri clienti, e mette in atto tutte le strategie necessarie per proteggerle e salvarle.

Entaksi è dotata di un **Sistema Integrato di Gestione (SIG)** che copre interamente le attività della società.

Il SIG è conforme alle seguenti norme:

- ISO/IEC 9001:2015 – Sistema di Gestione della Qualità (SGQ)
- ISO/IEC 20000-1:2011 – Sistema di Gestione per l'Erogazione di Servizi Informatici (SGS)
- ISO/IEC 27001:2013 – Sistema di Gestione della Sicurezza delle Informazioni (SiGSI)
- ISO/IEC 27017:2015 - Estensione del Sistema di Gestione della Sicurezza delle Informazioni (SiGSI)
- ISO/IEC 27018:2014 - Estensione del Sistema di Gestione della Sicurezza delle Informazioni (SiGSI)

La gestione della sicurezza delle informazioni è parte centrale e fondamentale delle attività di Entaksi.

Al fine di poterle salvaguardare al meglio, le informazioni vengono classificate in base ad un livello adeguato che ne definisca il grado di riservatezza, integrità e disponibilità. Tale classificazione viene descritta nel capitolo [Classificazione delle informazioni](#).

Il personale con particolare responsabilità rispetto alle informazioni deve assicurarne il livello di classificazione, e trattarle rispetto al livello individuato. Deve inoltre mettere in atto tutte le procedure definite dall'azienda per assicurarne la sicurezza, e attenersi alle indicazioni definite nel capitolo [Procedure relative alla sicurezza delle informazioni](#).

Le informazioni vengono protette da accessi non autorizzati e mantenute nel tempo anche grazie alla sicurezza fisica delle strutture di Entaksi.

Entaksi Solutions ha deciso di impostare la sicurezza del proprio sistema informativo assumendo convenzionalmente, nell'analisi dei rischi, il valore più alto per la probabilità che si possa verificare una minaccia di tipo 'fisico', e concentrando gli sforzi sulla minimizzazione dell'impatto che tali minacce possono determinare, ove si verifichino.

In altre parole, a seguito del verificarsi di una minaccia di tipo "fisico", Entaksi considera accettabile il rischio del danno economico determinato sulle apparecchiature, purché questo non impatti sulla sicurezza delle informazioni ospitate o gestite dalle stesse. Tutte le procedure sono pertanto finalizzate a questo obiettivo.

2.1. Sistema di Conservazione

Fra i vari servizi gestiti da Entaksi è di particolare rilevanza il servizio rivolto all'esercizio del Sistema di Conservazione, nel quale vengono ospitati e gestiti a norma di legge documenti digitali fiscalmente rilevanti. Il servizio è rivolto sia all'interno di Entaksi, per la conservazione dei documenti contabili e fiscali inerenti l'attività propria, sia ai Clienti.

Per tale servizio Entaksi ha definito, oltre alle politiche di sicurezza per le informazioni, anche le disposizioni necessarie per preservare nel tempo i dati archiviati nei propri sistemi.

Tutte le informazioni relative ai formati definiti per la conservazione, la verifica sull'integrità dei file, le soluzioni adottate in caso di anomalie, il monitoraggio e il controllo del sistema, sono contenute nel Manuale del Servizio di Conservazione "MAN eCON 20151222 Manuale della conservazione".

2.2. Ruoli e responsabilità

Vengono di seguito riportati i ruoli assunti all'interno di Entaksi Solutions per quanto riguarda la sicurezza delle informazioni.

Ruolo	Responsabilità
Amministratore Unico	Pianifica, controlla e supervisiona le attività della Società. Formulare la Politica della Società e i relativi indirizzi strategici, inclusi quelli riguardanti la sicurezza delle informazioni.
Direzione / Rappresentante della Direzione	Definisce e verifica le informazioni documentate da produrre, e garantisce la loro rintracciabilità e conservazione. Pianifica, coordina e supervisiona le attività aziendali di concerto con l'Amministratore.

Ruolo	Responsabilità
Responsabile del Sistema Integrato di Gestione	Mantiene aggiornato il SIG, e ne gestisce la documentazione, verifica la conformità, l'efficacia e l'efficienza del SIG.
Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (SiGSI)	Ha la responsabilità di tutte le attività inerenti la sicurezza delle informazioni del sistema informativo di produzione.
Responsabile Tecnico (Direzione Tecnica)	Ha la responsabilità di assicurare la pianificazione dell'architettura, lo sviluppo e la gestione dei sistemi di Information Technology della Società, garantendo l'integrazione delle piattaforme hardware/software, la coerenza dei sistemi/processi e l'uniformità della diffusione sul territorio.
Responsabile del Servizio di Conservazione	È il soggetto responsabile della creazione e del mantenimento del sistema e del processo di conservazione documentaria. Definisce e attua le politiche complessive del Sistema di Conservazione, e ne governa la gestione.

2.3. Mantenimento del documento

La responsabilità per la produzione, il mantenimento, e la diffusione del seguente documento appartiene al Responsabile del Sistema Integrato di Gestione di Entaksi Solutions.

Questo documento è stato approvato dalla Direzione di Entaksi, e la sua diffusione è pubblica, in quanto rivolta sia al personale interno che agli utenti che utilizzano servizi o prodotti Entaksi. Il documento è pubblicato sul sito di Entaksi a [questo link](#).

Il documento viene rivisto annualmente, o in base alle necessità, per esempio nel caso cambiamenti straordinari nella normativa lo richiedano.

Il documento segue le regole descritte in "MAN ISO 20130920 Gestione documenti SIG", e riporta nella parte iniziale i dati relativi a autore, data di rilascio, cambiamenti, approvazione da parte della Direzione.

3. Regole sulla sicurezza delle informazioni

Tutte le informazioni devono essere classificate secondo un livello adeguato che ne definisca il grado di riservatezza, integrità e disponibilità.

Riservatezza	L'accesso ai dati deve essere limitato in base ai privilegi indicati per gli utenti definiti, in accordo con il loro livello di classificazione. Le informazioni devono essere protette da eventuali accessi non autorizzati.
Integrità	Le informazioni devono essere complete e precise. Tutti i sistemi, gli asset e le reti devono funzionare correttamente, secondo specifiche che ne garantiscano la piena operatività.
Disponibilità	Le informazioni devono essere disponibili all'accesso e poter essere distribuite a chi ne detiene i diritti in base al livello di classificazione.

Tutto il personale di Entaksi interessato nella creazione o nella gestione delle informazioni deve assicurare che le stesse siano classificate, e che vengano trattate in accordo al livello di classificazione scelto.

Tutti gli utenti interessati da questa disposizione devono trattare le informazioni in accordo con il livello di classificazione scelto.

I principi indicati da Entaksi per garantire riservatezza, integrità e disponibilità delle informazioni sono i seguenti:

- Ogni utente che venga in possesso di informazioni riservate di Entaksi è considerato responsabile della protezione delle stesse, soprattutto dall'accesso di terzi e dall'uso non autorizzato.
- Tutti gli utenti hanno la responsabilità di proteggere le loro password aziendali e altre credenziali di accesso collegate ad attività aziendali da un uso non autorizzato.
- Tutti gli accessi e l'utilizzo di informazioni riservate di proprietà di Entaksi devono essere autorizzate da Entaksi, per gli scopi connessi all'attività aziendale.
- I dipendenti Entaksi e chiunque si trovi ad accedere a informazioni riservate di proprietà di Entaksi dovranno ricevere una adeguata formazione volta all'addestramento alla protezione delle stesse.
- Tutti gli utenti che utilizzano informazioni riservate appartenenti ad Entaksi devono essere univocamente identificati.
- Le informazioni riservate devono essere protette su qualsiasi dispositivo aziendale.
- Le informazioni riservate devono essere protette anche nel caso l'utente le trasferisca su un dispositivo non aziendale. In tal caso il dispositivo dovrà seguire le regole per i dispositivi aziendali (es.: cellulare personale connesso alla email aziendale).
- Tutti i server che memorizzano informazioni riservate appartenenti a Entaksi devono essere protetti da accessi non autorizzati.
- Tutti i dispositivi aziendali devono essere adeguatamente censiti e devono esserne note le loro ubicazioni fisiche abituali. Nel caso si verificano spostamenti devono essere seguite le regole per il trasporto.
- I software vanno mantenuti aggiornati su tutti i dispositivi, in modo tale da garantire che le versioni correnti siano le più sicure. Le eventuali patch sono approvate dalla Direzione Tecnica, che provvede ad informare i dipendenti tramite i canali di comunicazione concordati che è possibile aggiornare i dispositivi in sicurezza.

Ogni violazione rispetto alle direttive contenute in questa disposizione deve essere riportata e trasmessa a tutti gli utenti interessati.

4. Classificazione delle informazioni

Le informazioni possono essere classificate come:

- Riservate;
- Confidenziali;
- Pubbliche.

Questa classificazione deriva dalla tipologia delle informazioni (fondamentali o di supporto) e dal pubblico che può avere accesso alle suddette informazioni (ristretto, interno, circoscritto o allargato), secondo il seguente schema:

	Ristretto	Interno	Circoscritto	Allargato
Fondamentale	Riservato	Riservato	Confidenziale	Pubblico
Di supporto	Riservato	Confidenziale	Confidenziale	Pubblico

I documenti che veicolano le informazioni sono di conseguenza così classificati:

- **Informazioni fondamentali riservate (uso ristretto o interno):** dati sensibili che non sono oggetto di divulgazione al di fuori di un ristretto insieme di addetti.
I documenti che contengono questo tipo di informazioni sono classificati come "Riservati".
- **Informazioni fondamentali confidenziali (uso circoscritto):** dati che non sono oggetto di divulgazione al pubblico. I documenti che contengono questo tipo di informazioni sono classificati come "Confidenziali".
- **Informazioni fondamentali non confidenziali (uso pubblico):** dati oggetto di divulgazione al pubblico, senza alcun requisito di riservatezza.
I documenti che contengono questo tipo di informazioni sono classificati come "Pubblici".
- **Informazioni di supporto riservate (uso interno):** dati che non sono oggetto di divulgazione al di fuori di un ristretto insieme di addetti.
I documenti che contengono questo tipo di informazioni sono classificati come "Riservati".
- **Informazioni di supporto confidenziali (uso interno o circoscritto):** documenti / informazioni specificatamente legate al Sistema ed al suo funzionamento la cui divulgazione a soggetti non autorizzati potrebbe compromettere l'efficacia delle contromisure poste in essere nel Sistema Integrato di Gestione a protezione della disponibilità, integrità e riservatezza delle informazioni. I documenti che contengono questo tipo di informazioni sono classificati come "Confidenziali".
- **Informazioni di supporto non confidenziali (uso pubblico):** documenti / informazioni specificatamente legate al Sistema ed al suo funzionamento la cui divulgazione non compromette in alcun modo l'efficacia delle procedure poste in essere nel Sistema Integrato di Gestione.
I documenti che contengono questo tipo di informazioni sono classificati come "Pubblici".

Tutte le informazioni derivate da contatti con i clienti, compresi i documenti portati in conservazione e i dati personali delle registrazioni ai servizi, sono considerate informazioni fondamentali, accessibili solo a un pubblico ristretto, e sono pertanto classificate come riservate.

Le informazioni riguardanti gli utenti dei servizi Entaksi pertanto non sono assolutamente oggetto di divulgazione al di fuori degli addetti al servizio stesso, e sono soggette a cifratura.

4.1. Sistema di conservazione

Viene definito per il sistema di conservazione il ruolo di "Produttore", ossia la persona fisica o giuridica responsabile della creazione del Pacchetto di Versamento (PDV) e del suo invio verso il sistema di conservazione.

I produttori dei documenti sono considerati un pubblico ristretto, e le informazioni versate nel sistema come "fondamentali".

Per questo motivo tutti i dati provenienti dai produttori inseriti nel sistema di conservazione sono considerati come "Informazioni riservate", e non sono oggetto di divulgazione al di fuori del rapporto tra i produttori e i responsabili individuati per il sistema di conservazione.

5. Procedure e politiche relative alla sicurezza delle informazioni

Vengono di seguito riportati gli specifici indirizzi operativi e le indicazioni definite da Entaksi per perseguire le politiche di sicurezza delle informazioni.

5.1. Protezione dei dati

Entaksi Solutions segue la normativa nazionale ed Europea per quanto concerne la protezione dei dati personali.

La società è organizzata nel modo seguente:

- **Titolare del trattamento:** esercita il potere decisionale sulle finalità e sulle modalità del trattamento ivi compreso il profilo della sicurezza; questi è responsabile delle scelte in materia di sicurezza dei dati trattati della cui mancata adozione risponde anche penalmente;
- **Responsabili del trattamento:** sono scelti fra le figure aziendali che forniscono idonea garanzia del pieno rispetto delle disposizioni in materia di protezione dei dati personali, ivi compreso il profilo della sicurezza; i responsabili agiscono in base alle istruzioni specifiche ricevute dal titolare e rispondono della loro ingiustificata inosservanza, e hanno obblighi specifici circa la comunicazione di eventuali problematiche la cui risoluzione comporta l'intervento decisionale del titolare;
- **Amministratori di Sistema:** sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi è affidato spesso anche il compito di vigilare sulla protezione dei sistemi informatici di un'azienda o di una pubblica amministrazione;
- **Incaricati:** soggetti che, nominati direttamente dal titolare o dal responsabile, operano sotto la loro diretta autorità nel rispetto delle istruzioni da questi ricevute e condivise.

Il **Titolare del trattamento dati** è: Entaksi Solutions Srl

La sede legale è sita in Via la Piana n. 76, (51028) Frazione Pontepetri - San Marcello Piteglio (PT).

Entaksi fornisce ai propri dipendenti, collaboratori, fornitori o consulenti, istruzioni organizzative e tecniche che consentano l'osservanza degli obblighi di legge relativi alla protezione dei dati personali. Per questi obblighi delinea il quadro di sicurezza adottato per il sistema informativo, e definisce tutte le misure per garantire l'affidabilità delle componenti hardware e software ai fini della tutela dei dati personali trattati.

Inoltre provvede a informare gli utenti di prodotti e servizi delle misure messe in atto per proteggere e conservare i dati personali attraverso le apposite informative.

5.2. Accessi

Entaksi garantisce la protezione delle credenziali attraverso l'utilizzo del protocollo OAuth 2.0 e gestisce le credenziali single sign-on attraverso il software Open Source Keycloak.

Ai servizi forniti da Entaksi viene applicata una gestione degli accessi che prevede la creazione di differenti comunità di utenti, i cui privilegi di accesso sono assegnati in base alla logica RBAC (Role Based Access Control). I privilegi vengono assegnati in base a dei ruoli, creati in base alle funzioni eseguibili nel servizio. I permessi per eseguire specifiche operazioni sono assegnate non per singolo utente ma in base a specifici ruoli.

I privilegi e i ruoli ad essi connessi vengono definiti nei documenti delle specifiche tecniche di ogni servizio.

Per ogni servizio devono essere presenti i seguenti ruoli:

- amministratore: utenti con accesso alle configurazioni del sistema.
- utenti: fruitori del sistema, che non hanno accesso alle configurazioni del sistema.
- auditor: utenti con accesso in sola lettura.

La definizione dei privilegi per ogni gruppo, dei ruoli, la gestione delle richieste di credenziali, delle loro revoche e dei tempi necessari alle stesse, sono gestite dal Responsabile del Servizio. Se il Responsabile del Servizio lo ritiene necessario possono essere creati più ruoli rispetto a quelli descritti.

Il Responsabile ICT si occupa della procedura di registrazione dei dati di accesso in un apposito registro, e della sua integrità.

La procedura di recupero delle password per gli utenti è automatizzata, e in nessun caso un dipendente Entaksi è autorizzato a

chiedere la password personale dell'utente.

L'account viene bloccato dopo 30 tentativi di accesso non andati a buon fine. Le sessioni hanno un tempo di scadenza fissato a 30 minuti.

Quando la password o il nome utente inseriti sono errati, il sistema non fornisce informazioni sul tipo di errore, ma risponde solo con un "Accesso negato".

Per ogni ruolo possono essere configurate specifiche notifiche, che comprendono almeno:

- notifica di modifica della password;
- notifica di tentativo di accesso non andato a buon fine;
- notifica della modifica dei dati personali di accesso (nome utente, email).

Il canale per la comunicazione di tale notifiche è costituito dall'email dell'utente, verificata al primo accesso.

In caso di inattività dell'utente i servizi sono configurati per invalidare la sessione dopo un certo tempo calibrato intorno alle modalità d'uso del servizio (tipicamente 30 minuti).

5.3. Password

Le password sono una componente fondamentale della sicurezza delle informazioni, in quanto servono a proteggere adeguatamente tutti gli account connessi all'utente. Tuttavia una password mal costruita e mal protetta può comportare la compromissione della sicurezza delle informazioni.

Sono quindi fornite all'interno di questa disposizione le linee guide per la creazione di una password sicura, e per la sua corretta conservazione.

I dipendenti di Entaksi Solutions Srl sono tenuti a garantire che le informazioni sensibili, siano esse in formato cartaceo o elettronico, siano conservate in modo sicuro, e protette da password efficaci.

5.3.1. Creazione della password

Per quanto riguarda la creazione di una password, in ottemperanza a quanto descritto nell'Allegato B al Codice della Privacy, "Disciplinare tecnico in materia di misure minime di sicurezza":

- La password deve essere formata dal almeno 8 caratteri alfanumerici.
- Deve contenere sia lettere maiuscole che minuscole.
- Deve contenere almeno un numero.
- Non deve contenere informazioni personali.
- Non deve contenere informazioni legate al lavoro.
- Non deve contenere modelli riconoscibili.

La selezione della parola chiave dovrebbe essere governata da criteri di casualità.

A titolo di esempio, ecco alcune sequenze che NON vanno utilizzate:

- il nome di login (o codice di identificazione personale) in qualsiasi forma (ad esempio: invertito, in maiuscole, duplicato, ecc.);
- il proprio nome, il nome del coniuge, dei propri figli e relativi acronimi;
- il nome del sistema operativo che si sta usando;
- il numero di telefono;
- la data di nascita;
- altre informazioni facilmente ricavabili dall'indirizzo, o parti del codice fiscale;
- nomi di città, nomi propri;
- la targa automobilistica;
- semplici composizioni quali ad esempio "qwerty";
- caratteri sequenziali ripetuti (ad esempio 1111, aaaa, ecc.);
- cifre in progressivo ordine crescente o decrescente;
- parole di senso compiuto in lingua italiana o in una lingua straniera diffusa;
- informazioni legate al lavoro quali nomi di software, hardware, nomi di prodotti o servizi;
- le ultime quattro password;

Per quanto riguarda la creazione della password per l'accesso ai servizi, all'utente sono indicate, al momento della creazione

del profilo utente, le medesime linee guida.

Sono inoltre applicati controlli restrittivi al momento della formazione, per i quali una password sotto gli 8 caratteri, che non contiene almeno un numero e lettere sia maiuscole che minuscole, viene rifiutata.

Per i dipendenti Entaksi è inoltre obbligatoria l'autenticazione a due fattori, che è comunque consigliata anche agli utenti che si iscrivono ai servizi erogati.

5.3.2. Gestione della password

Non dovrebbe essere necessario scrivere la password, ma nel caso ci sia bisogno di scriverla va conservata o in un file criptato o se annotata su supporto cartaceo in un luogo accessibile solo al proprietario, meglio se in forma camuffata. Il modo migliore per mantenere segreta la password è memorizzarla.

Per quanto riguarda la conservazione della password:

- Non va utilizzata la stessa password di accesso ad account Entaksi e ad account personali dell'utente.
- Se possibile gli utenti dovrebbero utilizzare diverse password per i diversi accessi aziendali.

Come criteri generali:

- Se il sistema utilizza parole chiave di default, esse debbono esser cambiate subito; non consentire che i controlli di sicurezza siano governati da parola chiave fornite dal fabbricante o dall'installatore.
- Cambiare la parola chiave ogni volta che si ha il sospetto che essa, per un motivo qualsiasi, sia venuta a conoscenza di terzi (ad esempio, per osservazione indiscreta).
- Non inserire le password in programmi ed altri file dove possono essere rintracciate.
- Non condividerle con alcuno. Se una parola chiave deve essere divulgata o viene comunque a conoscenza di terzi, bisogna cambiarla subito.

5.4. Gestione della documentazione

La gestione interna della documentazione di Entaksi è soggetta ai principi generali enunciati per la sicurezza delle informazioni.

Tutte le informazioni documentate, ossia tutti i documenti prodotti o ricevuti da Entaksi nello svolgimento delle sue attività, devono essere classificate e conseguentemente gestite all'interno dell'organizzazione come enunciato nei capitoli precedenti.



Le indicazioni interne relative alla gestione della documentazione sono contenute in "MAN ISO 20130920 Gestione documenti SIG".

5.4.1. Schermo e scrivania puliti

"Schermo e scrivania puliti" significa trattare gli spazi di lavoro in modo tale per cui non siano mai visibili informazioni sensibili, anche in maniera accidentale. Al fine di proteggere tutti i dati sensibili e confidenziali Entaksi indica ai suoi dipendenti quali accorgimenti utilizzare affinché gli spazi di lavoro non rendano visibili informazioni sensibili.

La postazione di lavoro è intesa come desktop, ma anche come scrivania, nel caso siano presenti documenti cartacei, e più in generale qualsiasi luogo nel quale siano contenute informazioni sensibili relative a Entaksi Solutions Srl, siano esse di proprietà dell'azienda, relative ai dipendenti, ai clienti o ai fornitori.

- La zona di lavoro deve essere costantemente presidiata, e resa sicura al termine della giornata di lavoro.
- Le postazioni computer devono essere bloccate o spente quando non utilizzate.
- I dati cartacei devono essere resi inaccessibili a terzi quanto non si è presenti alla postazione.
- Nel caso dei dati, in qualsiasi forma, vengano conservati in luoghi chiusi a chiave, le chiavi non devono mai essere lasciate incustodite.
- Le password non vanno mai scritte su foglietti lasciati accanto alla postazione di lavoro, e non vanno conservate in una posizione accessibile (anche un file sul computer non criptato è considerato accessibile).
- I computer vanno impostati in modo che automaticamente si blocchino e richiedano la password dopo più di cinque minuti di inutilizzo.
- Nel caso il proprio cellulare o altri dispositivi siano connessi ad attività aziendali (es. email) le regole per la postazione si applicano anche a loro.
- Nel caso il cellulare sia connesso ad attività aziendale si richiede che esso sia protetto con un codice PIN di almeno 5 cifre,

o lettura dell'impronta digitale, o disegno ad almeno 9 punti. È sconsigliato l'utilizzo del riconoscimento facciale.

- Le sessioni sui sistemi gestiti da Entaksi hanno una durata massima di 30 minuti, dopo la quale la sessione risulta scaduta. Questa impostazione permette, in caso di sessioni lasciate aperte su altre dispositivi, di impedire l'accesso a terzi. Pertanto, al fine di rendere questa impostazione effettivamente operativa, è vietato memorizzare la password per servizi Entaksi su asset esterni a quelli in dotazione.

5.4.2. Documenti cartacei

Entaksi ha individuato un luogo sicuro ove sono di norma custoditi i documenti contenenti dati personali; come regola generale, tali documenti non devono essere asportati da tale luogo sicuro e, ove ciò avvenga, l'asportazione deve essere ridotta al minimo tempo necessario per effettuare le operazioni di trattamento.

Il trattamento delle informazioni cartacee segue gli stessi principi delle informazioni elettroniche, e la loro protezione è da assicurarsi tramite il presidio dell'informazione (custodia in luogo sicuro) e in modo che il suo trasporto non ne metta a repentaglio la riservatezza, l'integrità e la disponibilità. Pertanto:

- I documenti cartacei vanno custoditi in un luogo sicuro.
- Per tutto il periodo in cui i documenti sono all'esterno del luogo sicuro, l'incaricato non deve mai perderli di vista, adempiendo ad un preciso obbligo di custodia dei documenti stessi.
- Tutte le informazioni stampate devono essere rimosse dalla stampante non appena prodotte.
- I dispositivi quali stampanti e fotocopiatrici vanno controllati, in modo che non trattengano informazioni (es. alcune stampanti hanno una cache che potrebbe memorizzare i file stampati).
- Una volta terminata la loro funzione i documenti cartacei contenenti informazioni sensibili devono essere triturati, in maniera tale da rendere il loro contenuto illeggibile.

5.5. Crittografia

Entaksi Solutions implementa una serie di tecniche basate su algoritmi di crittografia per l'archiviazione sicura delle informazioni, per la protezione delle informazioni quando vengono scambiate tra diversi sistemi e, in alcuni contesti, per l'autenticazione degli utenti e dei servizi.

Entaksi utilizza il protocollo Transport Layer Security (TLS) versione 1.1 o superiore per le comunicazioni cifrate con i servizi esposti dall'infrastruttura sulla rete pubblica.

Gli ambiti di applicazione di questo protocollo sono:

1. Protezione delle connessioni ai servizi veicolati tramite protocollo HTTP
2. Protezione delle connessioni ai servizi di posta elettronica o altri servizi basati su connessioni TCP
3. Protezione delle connessioni VPN
4. Protezione di altri canali di interconnessione tra servizi interni all'infrastruttura basati su TLS

Negli ambiti 1 e 2, per la configurazione vengono utilizzati certificati digitali firmati da un'autorità di certificazione terza riconosciuta dai principali browser e client di posta elettronica e, quando applicabile, da un'autorità di certificazione accreditata dall'Agenzia per l'Italia Digitale della Presidenza del Consiglio dei Ministri del Governo Italiano.

Negli ambiti 3 e 4 vengono utilizzati certificati firmati da un'autorità di certificazione privata gestita da Entaksi (denominata 'Entaksi CA') secondo le procedure descritte nei successivi paragrafi di questo documento.

Le chiavi private dei sistemi crittografici, le password di sblocco delle partizioni cifrate e tutti gli elementi di natura riservata critici per il funzionamento dei sistemi crittografici sono custoditi in modo sicuro dal responsabile tecnico in forma cifrata e sottoposte a backup. Una copia di sicurezza è fornita a tutti gli altri responsabili che sono tenuti a conservarla in modo sicuro, in forma cifrata e sottoposta a backup, per essere usata in caso di emergenza, di mancata disponibilità temporanea o permanente del responsabile tecnico.

5.6. Contromisure per attacchi informatici basati su malware/virus

Gli attacchi informatici basati sulla diffusione di malware/virus rappresentano un concreto di rischio per la sicurezza delle informazioni a tutti i livelli dell'infrastruttura, dai server, alle postazioni, ai dispositivi mobili.

La strategia di Entaksi per la riduzione di questo rischio si basa su una serie di contromisure di natura preventiva, difensiva e di intervento per il contenimento del danno.

Le misure preventive adottate sono:

- Privilegiare l'uso di sistemi operativi progettati per la sicurezza, come GNU/Linux, Apple macOS, Microsoft Windows dalla versione 10 in poi.
- Mantenere aggiornati i sistemi operativi con l'ultimo livello di patch disponibile presso fonti affidabili, ovvero repository software Linux dotati di firma GPG e la distribuzione di patch e aggiornamenti automatici per macOS e Windows.
- Privilegiare l'uso di software open source di cui è possibile verificare la sicurezza e l'affidabilità in prima persona e di concerto con la comunità di sviluppatori e utenti.

Le misure difensive adottate sono:

- Utilizzare e mantenere aggiornata la soluzione antivirus Microsoft Security Essentials sulle postazioni Windows.
- Utilizzare e mantenere aggiornata la soluzione antivirus open source ClamAV sui server Linux mediante un servizio centralizzato utilizzato dai vari componenti quali il server di posta per la scansione dei messaggi in arrivo e il sistema di conservazione elettronica per la scansione dei pacchetti di versamento ricevuti, il controllo periodico dei documenti conservati nei pacchetti di archiviazione e la verifica dei documenti distribuiti mediante pacchetti di distribuzione.
- Il controllo periodico sul software del sistema avviene una volta ogni 24 ore
- Il controllo periodico sull'archivio dei documenti avviene una volta ogni settimana

Le misure di intervento per il contenimento del danno sono:

- Isolare immediatamente i dispositivi su cui venga rilevato malware/virus.
- Disattivare le credenziali degli utenti potenzialmente violate a causa della compromissione del dispositivo.
- Ripristinare completamente il dispositivo compromesso evitando operazioni di recupero.

L'aggiornamento della soluzione antivirus Microsoft Security Essentials è garantita mediante le impostazioni sul sistema operativo e verificato nel registro del sistema.

L'aggiornamento della soluzione antivirus ClamAV è garantito dal programma `freshclam` e verificato nel log di questo programma.

5.7. Sviluppo sicuro

Entaksi ritiene che la sicurezza nello sviluppo delle applicazioni debba essere considerata componente essenziale delle procedure di progettazione e realizzazione dei prodotti e servizi, dalla iniziale analisi dei rischi, alla espressione dei requisiti, alla esecuzione dei test intermedi, fino ai test definitivi di rilascio.

Le procedure operative che implementano e regolano le varie fasi della progettazione, sviluppo e rilascio di prodotti, servizi e delle stesse procedure del SIG devono quindi recepire questa impostazione, trasformandola, in relazione alle varie fasi, in prassi adeguate alla dimensione ed alle necessità operative della struttura.

La politica di sviluppo sicuro prevede inoltre il rispetto dei regolamenti che definiscono la visibilità dei dati, la registrazione delle autorizzazioni per il loro trattamento, la pseudonimizzazione dei dati personali. In fase di sviluppo, progettazione e verifica di qualità viene ridotto al minimo indispensabile l'utilizzo di dati personali, mediante tutte le misure tecniche e organizzative disponibili.

Qualora per esigenze di test sia necessario utilizzare dati personali non anonimizzati l'ambiente di test viene sottoposto agli stessi criteri di protezione dell'ambiente di produzione. Le informazioni personali sono sempre segregate in base al cliente interessato al trattamento dei dati, e non sono condivise se non previa autorizzazione degli interessati.

5.8. Gestione degli incidenti

Si definisce "incidente di sicurezza" qualsiasi evento che comprometta o minacci di compromettere il corretto funzionamento dei sistemi e/o delle reti dell'organizzazione o l'integrità e/o la riservatezza delle informazioni in esse memorizzate od in transito, o che violi le politiche di sicurezza definite o le leggi in vigore (con particolare riferimento al Regolamento (Ue) 2016/679, al Decreto legislativo 10 agosto 2018, n. 101, alla L. 547/1993 ed alla L. 38/2006).

Il SIG di Entaksi classifica gli incidenti definendone la codifica preventiva e la gestione degli stessi.

Il processo di gestione degli incidenti è articolato nelle seguenti fasi:

- **rilevazione/identificazione/classificazione** - vengono riconosciuti uno o più eventi di sicurezza come incidente e a ogni incidente ne viene assegnato un livello di gravità. Il rilevamento avviene a valle delle segnalazioni provenienti da strumenti automatici o ancora da segnalazioni del personale dell'amministrazione;
- **contenimento** - vengono attuate le prime contromisure, allo scopo di minimizzare i danni causati dall'incidente. In genere si tratta di azioni temporanee e veloci, di cui effettuare il roll-back dopo la successiva fase di eliminazione;
- **eliminazione** - vengono eliminate le cause che hanno portato al verificarsi dell'incidente;
- **ripristino** - vengono effettuate le operazioni necessarie per riparare i danni causati dall'incidente e si effettua il roll-back delle contromisure di contenimento;
- **follow-up** - viene verificata l'adeguatezza delle procedure di gestione degli incidenti e vengono identificati i possibili punti di miglioramento.

Per le procedure di gestione degli incidenti si rimanda alla specifica implementazione nel SIG delle norme ISO/IEC 27001:2013 e TR 101 533-2 V1.3.1 (2012-04).