



## Politica Integrata Qualità & Sicurezza

L'ente Scuola Edile Salerno (E.S.E.S.) è un centro di formazione del settore edile nato dal coordinamento tra il settore imprenditoriale ed il settore sindacale, con lo specifico obiettivo di diffondere le conoscenze tecniche e gestionali al personale delle aziende edili della provincia di Salerno necessarie per garantirne la competitività. Le imprese che si affidano all'E.S.E.S. accrescono il valore delle competenze del proprio personale che possono poi utilizzare ai fini competitivi. Inoltre l'E.S.E.S. assolve alla importante funzione sociale di diffondere presso la collettività le informazioni tecniche finalizzate ad applicare la normativa e le buone tecniche di prevenzioni degli infortuni, al fine di concorrere alla riduzione del numero e della relativa entità del danno causato. Un ulteriore fine dell'E.S.E.S. è quello di permettere la crescita delle conoscenze dei singoli individui, creando in tal modo le condizioni per il miglioramento delle proprie condizioni lavorative (sia come dipendenti che come liberi professionisti).

È maturata, progressivamente, la convinzione che l'impegno verso la Qualità è un nuovo traguardo culturale che deve caratterizzare sia la concezione complessiva che la gestione minuta del lavoro. L'obiettivo di tale impegno è dato da un continuo miglioramento dei processi e dei servizi erogati, al fine di garantire la soddisfazione del "cliente", identificato nell'allievo frequentante un corso di formazione, e delle parti interessate, nel pieno rispetto della normativa sulla sicurezza sui luoghi di lavoro e di protezione della salute dei lavoratori.

Le attività di formazione accentuano al massimo le caratteristiche che distinguono l'erogazione di un servizio dalla produzione di un bene tangibile e, in particolare, la dipendenza dei risultati dal comportamento del destinatario del servizio. E', infatti, indubbio che il risultato finale della formazione si ottiene dall'interazione di due processi: il processo di erogazione della formazione ed il processo di apprendimento realizzato da ciascun discente. Il risultato finale è, quindi, l'incontro tra queste due dimensioni ben distinte.

Per perseguire questo obiettivo prioritario l'E.S.E.S. parte dall'individuazione delle esigenze del soggetto e del contesto di riferimento e delle parti interessate e le elabora, portando ad un'offerta formativa più o meno fondata sui nuovi paradigmi pedagogici che promuovono la centralità ed il coinvolgimento attivo, partecipativo e collaborativo del discente. In questo modo il processo di apprendimento del discente si concretizza in competenze applicabili direttamente all'ambiente di lavoro.

La Direzione avendo fatto propri i principi ispiratori della qualità organizzativa, della tutela della sicurezza e salute sui luoghi di lavoro, ha inteso condividerli con tutto il personale stabilendo i seguenti impegni:

- ✓ condurre le proprie attività garantendo la conformità legislativa e le altre prescrizioni in materia di sicurezza e salute sui luoghi di lavoro;
- ✓ selezionare i propri fornitori anche in funzione della loro sensibilità in materia di sicurezza e salute sui luoghi di lavoro;
- ✓ instaurare e preservare le condizioni adeguate di sicurezza e salute sui luoghi di lavoro riducendo le cause potenziali di infortunio e di malattie professionali;
- ✓ coinvolgere, formare ed informare il proprio personale al fine di promuovere comportamenti sicuri e motivazionali finalizzati al raggiungimento degli obiettivi aziendali;
- ✓ garantire la soddisfazione dei clienti e delle parti interessate attraverso il miglioramento della capacità di rispondere alle loro richieste, nel pieno rispetto della normativa in materia di sicurezza sui luoghi di lavoro.

Gli obiettivi principali del Sistema di Gestione Integrato che l'E.S.E.S. intende perseguire possono riassumersi in:

- progettazione accurata dell'azione formativa generale e di dettaglio
- conoscenza delle aspettative degli allievi e delle parti interessate e coerenza tra quanto atteso e quanto ricevuto dai corsi, identificando quali sono i processi decisionali e le modalità con cui si è pervenuti alle scelte formative specifiche
- analisi sulla qualità percepita del servizio
- definizione delle specifiche di qualità del servizio
- monitoraggio, nella fase di erogazione, con valutazioni periodiche sull'apprendimento



- efficace comunicazione interna ed esterna in grado di informare e rendere “leggibile” l’intera attività svolta

Per perseguire questi impegni la Direzione intende seguire un programma di miglioramento continuo che prevede i seguenti punti:

- migliorare con continuità il proprio sistema di gestione integrato e le performance aziendali;
- stabilire e riesaminare periodicamente i propri obiettivi e traguardi;
- rendere disponibili le risorse necessarie a sostegno degli obiettivi stabiliti nel rispetto del necessario equilibrio economico e finanziario;
- rendere disponibile e condividere la presente politica con le parti interessate interne ed esterne;
- riesaminare periodicamente la presente politica in funzione degli impegni, degli obiettivi e delle esigenze delle parti interessate, al fine di garantirne la pertinenza e l’adeguatezza.

Salerno, 08.03.2023

Il Presidente



## Politica per la Sicurezza delle Informazioni

Per l'ente Scuola Edile Salerno (E.S.E.S.) la gestione della sicurezza delle informazioni ha come obiettivo primario preservare la riservatezza, l'integrità e la disponibilità delle informazioni, al fine di salvaguardare il patrimonio rappresentato dagli asset e dalle conoscenze aziendali, soddisfare i requisiti delle parti interessate e tutelare le persone fisiche di cui si trattano i dati personali.

Per le caratteristiche dei servizi che la società offre ai propri clienti e per il valore che rappresentano le informazioni nel proprio business, la politica per la sicurezza delle informazioni rappresenta un indirizzo strategico fondamentale e prioritario.

La politica per la sicurezza delle informazioni per la società è costituita da un insieme di attività che comprendono: l'identificazione degli asset primari, la gestione dei rischi, dei sistemi e della rete, l'identificazione delle vulnerabilità e degli incidenti, il controllo degli accessi, la gestione della privacy e della compliance, la valutazione dei danni e tutti gli altri aspetti che possono impattare sulla gestione della sicurezza delle informazioni.

La società impegna, quindi, la propria organizzazione a sviluppare e mantenere un sistema di gestione della sicurezza delle informazioni nell'ambito delle attività svolte e dei servizi erogati al fine di garantire la disponibilità l'integrità e la riservatezza dei dati.

La presente politica si applica a tutto il personale interno e quello delle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione ed erogazione di servizi formativi. La sede di riferimento è sita in Salerno (SA) - alla Via Cerzone 1.

Tutte le persone che lavorano e/o collaborano con la società sono impegnate a rispettare i seguenti principi:

1. **Riservatezza:** assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati e che le informazioni non siano rese disponibili o divulgate a persone o entità non autorizzate;
2. **Integrità:** salvaguardare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;
3. **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetture associati quando ne fanno richiesta;
4. **Controllo:** assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità:** garantire una provenienza affidabile dell'informazione;
6. **Privacy:** garantire la protezione ed il controllo dei dati personali.

La Direzione è fortemente impegnata a una grande responsabilizzazione di tutte le persone che lavorano per e con la società nel garantire la rigore del proprio operato per adempiere, con la massima attenzione, ai compiti assegnati.

In particolare, questo obiettivo è perseguito attraverso l'impegno a garantire:

- il rispetto delle leggi e normative vigenti;
- l'efficienza operativa e affidabilità dei processi di sviluppo prodotti e servizi correlati;
- le condizioni di salute e sicurezza sui luoghi di lavoro per il personale e per i collaboratori;
- la continuità e l'efficienza dei processi organizzativi e operativi al fine di prevenire e ridurre al minimo l'impatto degli incidenti volontari o casuali sulla sicurezza dei dati/informazioni gestite;



- la protezione dei mezzi resi disponibili, ed il loro corretto utilizzo;
- la riservatezza, la correttezza e la disponibilità delle informazioni gestite e la salvaguardia della proprietà intellettuale;
- l'adozione di misure di prevenzione di anomalie di processo/prodotto/servizio.

Per dare attuazione alla propria politica della sicurezza delle informazioni, la Direzione ha sviluppato e si impegna a mantenere un sistema di gestione sicura delle informazioni conforme ai requisiti specificati della Norma ISO/IEC 27001.

La Direzione con la presente politica si impegna a garantire che:

1. l'organizzazione abbia piena conoscenza delle informazioni gestite e valuti di volta in volta la loro criticità, al fine di agevolare l'implementazione di adeguati livelli di protezione;
2. l'accesso alle informazioni avvenga in modo sicuro e adatto a prevenire i trattamenti non autorizzati o realizzati senza i diritti necessari;
3. l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza;
4. l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, siano adeguatamente formate e abbiano piena consapevolezza delle problematiche relative alla sicurezza;
5. le anomalie e gli incidenti aventi ripercussioni sul sistema informativo, sui servizi e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business;
6. l'accesso alla sede ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
7. siano assicurati la conformità ai requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti;
8. la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi siano gestiti al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni;
9. la business continuity aziendale e il disaster recovery siano attuati attraverso l'applicazione di procedure di sicurezza stabilite;
10. i trattamenti dei dati personali, sia nei casi in cui la società operi in qualità di Titolare che nei casi in cui operi per conto terzi in qualità di Responsabile del Trattamento, avvengano nel rispetto del Regolamento Europeo sulla Protezione dei Dati Personali GDPR 679/2016.

La Direzione d si impegna infine a:

- adottare un sistema di gestione sicura delle informazioni conforme ai requisiti specificati della norma ISO/IEC 27001;
- mantenere costantemente monitorato il grado di conformità del sistema alle norme e leggi applicabili di natura cogente e volontaria, e gli obblighi contrattuali pertinenti l'ambito di applicazione del SGSI;
- garantire mezzi e risorse idonee al suo mantenimento e miglioramento continuo, in particolare per quanto attiene la mitigazione/riduzione dei livelli di rischio sulla sicurezza delle informazioni e l'adozione di misure idonee a prevenire situazioni anomale e di emergenza;



- rendere consapevoli tutte le persone dell'organizzazione degli obblighi e delle responsabilità di ciascuno nella gestione della sicurezza delle informazioni e delle conseguenze in caso di eventi, dolosi e colposi, relativi all'utilizzazione non autorizzata, modifica o distruzione di informazioni critiche.

La politica della sicurezza delle informazioni viene costantemente aggiornata e verificata, attraverso un riesame annuale, per assicurare la coerenza con le finalità strategiche dell'organizzazione. La politica è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso la sua pubblicazione sul sito.

Salerno, 08.03.2023

Il Presidente



## Politica per la Sicurezza delle Informazioni per i Fornitori

### Politica per la Sicurezza delle Informazioni

L'ente Scuola Edile Salerno (E.S.E.S.) implementa e mantiene un Sistema di Gestione delle Informazioni sicuro seguendo i requisiti specificati nella Norma UNI CEI EN ISO/IEC 27001:2017, così da garantire:

1. **Riservatezza:** assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati e che le informazioni non siano rese disponibili o divulgate a persone o entità non autorizzate;
2. **Integrità:** salvaguardare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;
3. **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetture associati quando ne fanno richiesta;
4. **Controllo:** assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità:** garantire una provenienza affidabile dell'informazione;
6. **Privacy:** garantire la protezione ed il controllo dei dati personali.

La mancanza di adeguati livelli di sicurezza delle informazioni può comportare il danneggiamento dell'attività del dell'E.S.E.S., la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica, finanziaria e di immagine dell'azienda e della filiera sottostante.

L'impegno della direzione dell'E.S.E.S., che si richiede applicazione anche da parte dei fornitori, si attua tramite la definizione di una struttura organizzativa adeguata a:

- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento della Sicurezza delle Informazioni;
- controllare che la politica per la Sicurezza delle Informazioni sia integrata in tutti i processi aziendali e che le procedure ed i controlli siano sviluppati coerentemente ed efficacemente;
- monitorare l'esposizione alle minacce per la sicurezza delle informazioni;
- attivare programmi per diffondere la consapevolezza e la cultura sulla sicurezza delle informazioni.

Gli obiettivi generali dell'E.S.E.S. che i fornitori dovranno a loro volta perseguire, sono quindi:

- garantire i migliori standard, ottimizzando e razionando i processi e gli strumenti aziendali;
- garantire l'efficacia delle procedure e controlli per la Sicurezza delle Informazioni;
- garantire la soddisfazione dell'E.S.E.S. in relazione alla quantità delle informazioni.

Il fornitore deve assicurare che tutto il personale deve operare per il raggiungimento degli obiettivi di sicurezza nella gestione delle informazioni e deve impiegare le tecnologie più adeguate a garantire il rispetto della presente politica.



## **Requisiti di Sicurezza delle Informazioni per i fornitori**

Lo scambio di documenti e informazioni tra l'E.S.E.S. e il Fornitore deve avvenire: per le informazioni riservate tramite e-mail come allegati in cartelle criptate con password; in entrambi i casi, sarà cura dell'E.S.E.S. fornire, attraverso canali differenti, riferimenti e credenziali alla persona indicata in NDA (o comunque autorizzata allo scambio di dati), via e-mail per tutti gli altri documenti quali informazioni non riservate etc.

Le persone che potranno ricevere informazioni dall'E.S.E.S., ad eccezione quelle pubbliche, sono quelle indicate nell'NDA se sottoscritto tra le parti o diversamente autorizzate da entrambi le parti. Il fornitore si impegna ad attuare soluzioni per la protezione da attività fraudolente, da dispute contrattuali, da divulgazioni e da modifiche non autorizzate. In caso di necessità di accesso agli asset dell'E.S.E.S. da parte del fornitore, lo stesso dovrà essere preventivamente autorizzato e informato delle modalità di utilizzo degli stessi, cui dovrà attenersi scrupolosamente e sarà soggetti ai controlli previsti dalle politiche dell'E.S.E.S..

Per i fornitori associati ai servizi e ai prodotti della filiera di fornitura per l'ICT, il fornitore deve impegnarsi a rispettare i requisiti dell'E.S.E.S. per affrontare i rischi relativi alla sicurezza delle informazioni, richiedendo preventivamente all'E.S.E.S. copia delle Politiche Applicabili.

## **Monitoraggio e riesame dei servizi erogati dal fornitore**

Al fine di avere una visibilità complessivamente sufficiente su tutti gli aspetti di sicurezza relativi alle informazioni critiche o alle strutture di elaborazione delle informazioni, l'E.S.E.S. monitora i livelli di prestazione del servizio ricevuto al fine di verificare il rispetto degli accordi. Potranno essere condotti audit ai propri fornitori, congiuntamente al riesame dei rapporti di fornitura.

## **Gestione degli accessi alla rete ed ai servizi su rete**

Qualora il servizio richiesto al fornitore richieda di operare all'interno della rete dell'E.S.E.S., allo stesso verrà fornito l'accesso con le seguenti modalità e solo per i servizi ai quali sono stati specificatamente autorizzati dai singoli accordi con l'E.S.E.S.:

- Il fornitore dovrà comunicare il nominativo degli operatori che saranno preventivamente approvati dall'E.S.E.S. per operare sulla rete
- Agli stessi verrà comunicata una password verbalmente, che non dovrà essere modificata.

## **Gestione dei log**

L'utente (operatore del fornitore) è soggetto al controllo dei Log da parte del personale ICT dell'E.S.E.S..

## **Gestione delle password**

Gli utenti si impegnano a rispettare i criteri di creazione, conservazione e gestione delle credenziali di accesso indicati all'interno di questo documento. La password è strettamente personale e non deve essere comunicata e/o condivisa con nessun'altra persona all'interno dell'organizzazione. Gli utenti devono prestare attenzione a fornire le proprie



credenziali di accesso, rispondere ad e-mail sospette e/o cliccare sui link durante la navigazione web (o nella mail) al fine di contrastare possibili frodi informatiche (come il phishing, il furto di identità etc.).

Ogni utente è responsabile di tutte le azioni e le funzioni svolte dal suo account. Qualora vi sia la ragionevole certezza che le credenziali assegnate siano state utilizzate da terzi, l'utente dovrà segnalarlo all'E.S.E.S..

Per la conservazione sicura delle credenziali di accesso è consigliabile evitare di memorizzarle su documenti cartacei o file conservati all'interno della postazione di lavoro.

## **Accessi fisici**

L'azienda ha predisposto un sistema di controllo perimetrale, con varchi di accesso per proteggere le aree che contengono informazioni critiche e strutture di elaborazione. Al fine di proteggere e limitare l'accesso ad aree che contengono informazioni critiche l'azienda ha predisposto vari sistemi anti-intrusione, il cui layout sono ad uso esclusivo dell'E.S.E.S..

## **Sanzioni**

Il mancato od il ritardato adempimento di quanto previsto dalla presente politica aziendale e/o dal contratto stipulato tra le parti, che dovessero provocare dei danni, comporteranno il conseguente obbligo di risarcimento dei danni in favore dell'E.S.E.S. oltre alle eventuali sanzioni amministrative pecuniarie e/o penali previste dal GDPR 2016/679 e/o dalla normativa vigente.

Salerno, 08.03.2023

Il Presidente