Rev	Del	Descrizione	Redazione	Approvazione
0	14/01/2011	Prima emissione.	Roberto Monti	Giuliano Maggi
1	30/06/2011	Modifica ambito	Roberto Monti	Giuliano Maggi
2	05/11/2014	Aggiornamento alla norma ISO/IEC 27001:2013	Roberto Monti	Giuliano Maggi
3	14/03/2017	Modifica ambito	Roberto Monti	Giuliano Maggi
4	01/06/2018	Adeguamento GDPR	Roberto Monti	Giuliano Maggi
5	15/11/2019	Aggiornamento con aggiunta dell'allegato sull'analisi del contesto	Roberto Monti	Giuliano Maggi
6	14/12/2020	Revisione per correzione tipo e eliminazione dichiarazione	Roberto Monti	Giuliano Maggi
7	01/06/2023	Aggiornamento a Sistema di Gestione Interato ISO/IEC 27001, ISO 22301, ISO 9001, ISO 37001 e GDPR	Roberto Monti	Giuliano Maggi
8	30/09/2025	Aggiornamento template, campo di applicazione	Roberto Baudizzone	Giuliano Maggi

Il contenuto del presente documento è di esclusiva proprietà della CompEd Servizi. Il presente documento può essere utilizzato solo per lo scopo per il quale viene trasmesso e non per scopi lesivi o pregiudizievoli dei diritti e aspettative della CompEd Servizi e/o di terzi. Senza preventiva autorizzazione scritta della CompEd Servizi il presente documento non potrà venire comunicato a terzi né riprodotto in tutto o in parte. CompEd Servizi tutela i propri diritti a norma di legge.

INDICE

INDICE 2
1. INTRODUZIONE 3
1.1 Scopo 3
1.2 Applicabilità 3
1.3 Definizioni, Acronimi, Abbreviazioni 3
1.4 Documenti di riferimento 4
2. IMPOSTAZIONE DELLA POLITICA 4
3. POLITICA INTEGRATA 5
4. AMBITO DI APPLICAZIONE 7
5. ANALISI E VALUTAZIONE DEI RISCHI 7
6. COMPLIANCE GDPR 8
7. ANTICORRUZIONE 9
8. RESPONSABILITÀ 11

1. INTRODUZIONE

1.1 Scopo

La presente Politica ha lo scopo di sensibilizzare l'intera Organizzazione sui principi di Sicurezza delle Informazioni e Protezione dei Dati personali, Continuità Operativa e Prevenzione della Corruzione, attraverso la definizione, l'attuazione, il monitoraggio e il mantenimento di un Sistema di Gestione Integrato (di seguito "SGI") conforme alle norme ISO 9001, ISO/IEC 27001, ISO 22301 e ISO 37001 (nelle loro ultime versioni) oltre che in riferimento al Regolamento Europeo sulla Protezione dei Dati EU 2016/679 (GDPR) ed al "Codice Privacy" D.Lgs. 196/2003 e s.m.i.
La Politica ha carattere generale ed intende esprimere la volontà della Direzione aziendale di garantire la qualità, la sicurezza delle informazioni, la continuità nella fornitura dei propri prodotti e nell'erogazione dei propri servizi e la trasparenza nelle proprie attività operative, perseguendo il miglioramento continuo di tutti i processi aziendali e dei servizi erogati tenendo in considerazione, nella definizione delle attività, le necessità e le aspettative di tutti gli Stakeholders.

1.2 Applicabilità

La presente politica si applica a tutto il personale aziendale e ai clienti e fornitori coinvolti nel campo di applicazione del Sistema di Gestione Integrato.

1.3 Definizioni, Acronimi, Abbreviazioni

BIA	Business Impact Analysis
CED	Centro Elaborazione Dati
CI	Configuration Item
CMDB	Configuration Management Data Base
D. Lgs.	Decreto Legislativo
DR	Disaster Recovery
GDPR	General Data Protection Regulation
ICT	Information & Communication Technology
RID	Riservatezza, Integrità, Disponibilità
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SGCO	Sistema di Gestione della Continuità Operativa
SGI	Sistema di Gestione Integrato
SGQ	Sistema di Gestione della Qualità
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
SGA	Sistema di Gestione per la Prevenzione della Corruzione

1.4 Documenti di riferimento

ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements
ISO 9001:2015	Sistemi di Gestione per la Qualità - Requisiti
ISO 22313:2020	Sicurezza e resilienza – Sistemi di gestione per la continuità operativa - Guida all'utilizzo della ISO 22301
GDPR	Regolamento Generale sulla Protezione dei Dati EU 2016/679.
D.Lgs. 196/2003	Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
ISO 37001:2016	Norma ISO 37001:2016 – Sistema di Gestione per la prevenzione della Corruzione

POI304 Procedura Whistleblowing
POI001 Gestione del Contesto

2. IMPOSTAZIONE DELLA POLITICA

L'impostazione che è alla base di un Sistema di Gestione Integrato (SGI) di CompEd Servizi si basa sulla consapevolezza che la sicurezza deve essere gestita da un punto di vista tecnologico, organizzativo ed economico; pertanto, l'approccio al problema passa per l'identificazione di un insieme di processi che permettano di garantire un costante e continuo miglioramento.
CompEd Servizi si impegna a salvaguardare tutte le risorse che sottendono ai processi strategici e che sono attentamente elencate nell'asset inventory aziendale. Le categorie principali sono:

- dati/documenti
- asset fisici
- asset logici
- prodotti/servizi
- personale.

Relativamente all'ambito della delivery di servizi ed in conformità alle norme ISO/IEC 27001 e ISO 22313 viene condotta, con frequenza annuale, un'analisi dei rischi che incombono sugli asset aziendali e sui servizi. Tale analisi tiene in considerazione gli obiettivi strategici espressi nella presente politica, gli incidenti occorsi, i cambiamenti di business e di tecnologia avvenuti nel corso del periodo.
Inoltre, CompEd Servizi effettua, in conformità alla ISO 37001, una valutazione annuale dei rischi di corruzione che possano compromettere i processi aziendali più esposti.

Lo sviluppo di applicazioni che erogano servizi tramite le reti telematiche e il crescente sviluppo tecnologico e informativo hanno determinato una sempre più ampia necessità di mantenere interconnessioni sicure e affidabili per consentire lo scambio di informazioni.

Per CompEd Servizi, che basa il suo business principalmente nel campo della gestione documentale, con servizi che coprono ogni esigenza di firma digitale, conservazione digitale, spedizione automatica "multi-carrier", è fondamentale seguire linee guida definite a livello internazionale e consolidate nel tempo, e che consentono di acquisire coscienza della necessità di sviluppare la "cultura della sicurezza".

L'azienda ha percepito in maniera chiara dalla Direzione che la cultura della sicurezza deve essere diffusa e, pertanto, ha assunto un ruolo attivo e incoraggiante nelle attività di impostazione e di implementazione di un Sistema di Gestione Integrato (SGI).
La Direzione definisce, quindi, in maniera chiara e puntuale la Politica del Sistema Integrato che l'Azienda intende perseguire, dandone specifica relazione ai rischi, alle minacce e alle vulnerabilità e tenendo conto del tipo di business esercitato.

3. POLITICA INTEGRATA

La CompEd Servizi ha definito un Sistema di Gestione Integrato che consenta di implementare e governare l'insieme delle misure organizzative, fisiche e logiche necessarie a garantire la qualità del servizio, la protezione delle informazioni aziendali ivi compresi i dati personali e garantisca la sicurezza e disponibilità dei servizi offerti, il tutto proteggendo il patrimonio informativo aziendale da minacce, interne o esterne, intenzionali o accidentali, ed erogando i propri servizi hardware e software nel pieno rispetto della sicurezza delle informazioni e della trasparenza.

Questo documento delinea i principi strategici ai quali CompEd Servizi intende ispirarsi per raggiungere i propri obiettivi. Tali principi possono essere sintetizzati in:

1. orientamento al cliente
2. garanzia di riservatezza, integrità e disponibilità
3. continuità operativa dei servizi anche durante eventi disastrosi
4. cultura dell'integrità e della trasparenza
5. leadership
6. coinvolgimento delle persone
7. approccio per processi
8. approccio sistematico alla gestione
9. miglioramento continuo
10. decisioni basate su dati di fatto
11. rapporti di reciproco beneficio con i fornitori.

L'attuazione della presente politica consente di garantire ai Clienti che la CompEd Servizi si è adoperata perché i propri prodotti e servizi non causino direttamente un aumento dei rischi per i Clienti che li utilizzano.

È scopo della CompEd Servizi assicurare che:

- le informazioni siano protette da accessi non autorizzati;
- le informazioni non vengano divulgate a persone non autorizzate a seguito di azioni deliberate o per incuria;
- vengano definiti programmi formativi sul SGI e sulle indicazioni della normativa vigente e cogente per tutti i dipendenti interni e per tutto il personale esterno che opera per prolungati periodi all'interno dell'organizzazione;
- vengano definite procedure per la sicurezza degli apparati all'esterno dell'Organizzazione stabilendo le modalità di assegnazione degli accessi;
- vengano attuate procedure per le necessarie autorizzazioni a portare fuori dall'azienda informazioni critiche, apparati e/o Software;
- l'integrità delle informazioni sia protetta e salvaguardata da modifiche non autorizzate;
- la sicurezza dell'informazione e del software scambiato all'interno dell'Organizzazione con qualunque parte esterna venga mantenuta;
- venga definita, documentata e riesaminata periodicamente una politica per il controllo degli accessi all'informazione basata sui requisiti per l'accesso relativi alla sicurezza e all'attività dell'azienda;
- venga divulgata l'importanza di segretezza e uso della password ed istituito un processo per l'assegnazione e il controllo della modifica;
- venga definita e documentata la procedura per la comunicazione tempestiva e per la gestione degli incidenti in caso di minaccia alla sicurezza dell'informazione. Siano pertanto immediatamente riconoscibili i responsabili e le azioni correttive da intraprendere;
- vengano definite adeguate linee guida per operare nelle aree ritenute particolarmente critiche e identificate queste aree in base alla valutazione dei rischi;
- l'azienda ottemperi ai requisiti cogenti;
- le informazioni siano a disposizione degli utenti autorizzati quando ne hanno bisogno;
- venga definito un formalismo centralizzato per le procedure operative per il business al fine della rintracciabilità e omogeneità di informazione;
- un sistema di back up delle informazioni sia uniformemente gestito e monitorato;
- vengano redatti piani per la continuità dell'attività aziendale, e che tali piani siano il più possibile tenuti aggiornati e controllati;
- il personale riceva comunicazioni aggiornate e adeguata formazione circa l'attuazione del SGI e del Sistema Privacy (GDPR);
- tutte le violazioni della sicurezza delle informazioni e possibili punti deboli vengano riferiti a chi di dovere ed indagati;
- quando è concesso l'accesso alle informazioni o agli asset dell'Organizzazione da parte di terzi vengano attuati controlli appropriati prima di concedere l'accesso;
- la continuità dei prodotti e dei servizi sia salvaguardata, grazie ad una adeguata allocazione di risorse atte a garantire l'identificazione e l'impatto di potenziali perdite, il mantenimento dei piani e delle strategie di ripristino;
- il livello di sensibilità e la competenza sui temi di sicurezza attraverso sia sempre continuo, attraverso comunicazioni aggiornate e adeguata formazione per tutto il personale, circa l'attuazione del SGI;
- l'organizzazione tenda al miglioramento continuo;

- siano definite e mantenute sotto controllo, per quanto riguarda l'erogazione di servizi in modalità cloud le modalità di erogazione del servizio in cloud: IaaS e PaaS; la gestione degli accessi ai servizi erogati in modalità cloud, le comunicazioni ai customer in caso di change e agli interessati in caso di data breach; il ciclo di vita degli account; il recepimento nell'analisi del rischio dei rischi aggiuntivi derivanti dall'erogazione di una infrastruttura cloud;
- sia vietata ogni forma di corruzione (attiva/passiva, diretta/indiretta) e, anzi, venga incoraggiato tutto il personale alla segnalazione di sospetti, in buona fede, senza timore di ritorsioni, anche attraverso l'utilizzo degli appositi canali messi a disposizione dall'organizzazione (vedere la "POI304 Procedura Whistleblowing");
- la trasparenza e la legalità siano considerate un valore aggiunto da integrare nei processi con gli opportuni controlli e le azioni di miglioramento necessarie a gestire la prevenzione della corruzione;
- siano avviate, quando necessario, le opportune azioni disciplinari o legali nei confronti dei soggetti che abbiano tenuto un comportamento illegittimo, in contrasto con i principi della presente politica e/o del Sistema di Gestione per la Prevenzione della Corruzione.

La presente politica sarà riesaminata periodicamente e a seguito dell'attuazione di modifiche al business o alla gestione aziendale che la possano influenzare oppure ogni qual volta vi siano cambiamenti significativi all'implementazione del SGI, per accertarsi che permanga idonea all'attività e alla capacità di mantenere elevato il grado di sicurezza e, di conseguenza, il grado di soddisfazione dei Clienti.

4. AMBITO DI APPLICAZIONE

Lo scopo del Sistema di Gestione Integrato di CompEd Servizi è quello di fornire a tutta l'Organizzazione i principi, le procedure, le istruzioni e le indicazioni relativi alla politica, agli obiettivi strategici (per la qualità, la sicurezza delle informazioni e protezione dei dati personali, la continuità dei servizi e la trasparenza), alla pianificazione, al controllo e al miglioramento continuo del Sistema.

Il Campo di Applicazione del Sistema di gestione integrato è il seguente:
"Servizi di conservazione digitale a valore fiscale e legale, servizi di firma elettronica avanzata, digitale e grafometrica, oltre che il processo di progettazione e dematerializzazione massiva dei documenti (certificazione di processo)"

L'azienda intende infatti offrire ai propri clienti le maggiori esperienze e professionalità del settore dei documenti informatici, curando tutti gli aspetti: gestionali, tecnologici, infrastrutturali, giuridici, fiscali. In tale ambito, quindi, diventa di estrema importanza una corretta gestione del flusso delle informazioni, come definito nel documento che definisce il Contesto dell'Organizzazione (vedere "POI001 Gestione del Contesto").

5. ANALISI E VALUTAZIONE DEI RISCHI

La Direzione istituisce e attua un approccio basato sulla valutazione quantitativa e qualitativa dei rischi associati alle risorse esistenti in Azienda, ai processi e agli obiettivi definiti nel sistema, ai

trattamenti dei dati personali. Tale metodo consente di determinare valori oggettivi che permettono di definire le relative contromisure che devono essere adottate per abbattere e rendere accettabile il valore del rischio residuo.
In tal senso, vengono adottati strumenti informatici e metodi deterministici che permettono, oltre che ad implementare e gestire l'inventario degli asset aziendali, il registro dei trattamenti dei dati e l'elenco dei processi sensibili in ottica di rischio corruzione, di misurare l'efficacia dell'applicazione delle azioni e soprattutto la replicabilità della valutazione al fine di mantenere il processo di miglioramento. Inoltre, l'analisi dei rischi costituisce strumento fondamentale a supporto delle decisioni dell'organizzazione, al fine di evitare i rischi e cogliere le opportunità.
Tutte le analisi di rischio effettuate ed i relativi piani di trattamento sono presentati e valutati ad ogni riesame della Direzione, al fine di individuare opportunità di miglioramento e definire misure di sicurezza e presidi. Essi hanno lo scopo di "contrastare", "prevenire", "dissuadere", "rilevare", "attenuare", "ripristinare" o "correggere" le minacce che possono incombere sui sistemi informativi ed i processi aziendali.
La Direzione, tenendo conto dei contratti esistenti con le terze parti, ha identificato i rischi derivanti da rapporti con esterni inserendoli all'interno della valutazione di rischio sulla sicurezza delle informazioni e sulla prevenzione della corruzione.

6. COMPLIANCE GDPR

CompEd Servizi si impegna ad adempiere agli obblighi di adeguamento al Regolamento Generale sulla Protezione dei Dati UE 2016/679 e dal D.lgs. 196/2033 come novellato dal D.lgs. 101/2018 di armonizzazione della normativa privacy nazionale al GDPR, e nella fattispecie tra l'altro nelle attività di:

- elaborazione di registro delle attività di trattamento;
- valutazione approfondita d'impatto sulla protezione dei dati, laddove applicabile;
- applicazione di misure tecniche ed organizzative adeguate intese a garantire la sicurezza dei dati;
- designazione di un Responsabile della Protezione dei Dati (RPD) e definizione all'interno di CompEd Servizi di ruoli e responsabilità relativi al trattamento dei dati laddove opportuno (Artt. 37, 38 e 39 GDPR).

CompEd Servizi si impegna ad attenersi ai principi di protezione dei dati contenuti nel GDPR per garantire che tutti i dati siano tra l'altro:

- trattati garantendo l'accountability e potendolo provare, nel rispetto dei principi di privacy by design e by default (Art. 25 GDPR);
- trattati in modo lecito, corretto e trasparente;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e non sovrabbondanti;
- accurati e mantenuti aggiornati;
- non conservati più a lungo del necessario;
- trattati in conformità dei diritti dell'interessato;
- sicuri;

- non trasferiti all'estero senza adeguata protezione.

In CompEd Servizi sono state stabilite la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che effettui direttamente o che altri effettuino per suo conto. In particolare, mettendo in atto misure adeguate ed efficaci, così da essere in grado di dimostrare la conformità delle attività di trattamento con il GDPR, si impegna a:

- rispettare tutti i requisiti di legge, i regolamenti, le direttive (locali, nazionali e comunitarie) applicabili alla realtà dell'Organizzazione, nel rispetto di tutte le parti interessate e delle esigenze dalle stesse espresse durante l'erogazione del servizio;
- rendere disponibile il presente documento a tutte le parti interessate, attivando adeguati canali di comunicazione al proprio interno e verso l'esterno;
- definire e documentare procedure per la comunicazione tempestiva e la gestione di incidenti in caso di minaccia alla Sicurezza delle Informazioni, adempiendo a quanto prescritto in tema di Data Breach;
- in accordo al GDPR definire politica di gestione processi della Formazione del personale che ha accesso al trattamento di dati personali;
- in accordo al GDPR definire e descrivere tra i trattamenti la classificazione dei dati personali su diversi livelli di significatività, che permettano di definirne diversi gradi di accessibilità e rilevanza all'uopo anche elaborando e tenendo sempre aggiornato il registro delle attività di trattamento;
- in accordo al GDPR (Art. 5 par.1) definire una politica che dettagli modalità di conservazione dei dati personali includendone il periodo e limitando al minimo tempo necessario il loro possibile utilizzo che consenta l'identificazione degli interessati; dettagliare modalità di conservazione/retention e politica di back-up ai fini del trattamento dei dati personali;
- definire regolamento di utilizzo delle risorse IT, di internet ed e-mail con attenzione ai dati personali;
- dettagliare modalità e preparare modulistica di richiesta di consenso dell'interessato al trattamento dei dati personali a seguito di informativa da fornire all'interessato;
- in accordo al GDPR (Art.32 Par.1) assicurare su base permanente la riservatezza, l'integrità e la disponibilità del dato personale trattato e le azioni di remediation in caso di perdita accidentale;
- in accordo al GDPR (Artt.28 e 29) controllare che i trattamenti affidati in parte o in toto a Soggetti terzi, siano gestiti a livello contrattuale, applicando misure tecniche e organizzative di monitoraggio del livello di sicurezza di tali Soggetti.
- in accordo al GDPR (Artt. 33 e 34 GDPR) attuare una procedura di gestione eventi di violazione dati personali integrata nel più generale processo di gestione eventi e incidenti di sicurezza delle informazioni.

7. ANTICORRUZIONE

CompEd Servizi si impegna in un'attività costante di monitoraggio di strumenti e presidi volti a contrastare ogni forma di corruzione, attiva e passiva, diretta e indiretta che coinvolga il personale di CompEd e ciascun soggetto che svolga attività per conto della stessa.

Garantisce, inoltre, il rispetto delle normative vigenti, sia nei rapporti fra privati che nei confronti della Pubblica Amministrazione.
Per rafforzare questo impegno, la Società ha adottato un proprio sistema di gestione anticorruzione in conformità alla norma ISO 37001 – Sistema di gestione per la prevenzione della corruzione, pubblicata nel 2016. I principi anticorruzione riportati nella presente Politica Integrata, sono parte integrante di un più ampio sistema di etica d'impresa e di controllo interno, finalizzato a garantire la compliance alle norme e agli standard nazionali e internazionali e a tutelare la reputazione dell'impresa. Essa concorre ad aumentare il grado di conformità generale alle leggi, ai regolamenti e alle buone pratiche internazionali applicabili e, al fine di dare concreta attuazione ad una cultura aziendale ispirata al valore dell'onestà, ai comportamenti eticamente corretti, alla prevenzione e al contrasto della corruzione.

Ciascun soggetto che effettui attività per conto di CompEd è tenuto a leggere e comprendere i contenuti della presente Politica Integrata e a comportarsi in conformità a quanto da essa stabilito.

Il personale di CompEd deve svolgere le proprie attività, rispettando i principi etici di trasparenza, chiarezza, correttezza, integrità ed equità. In particolare, nei rapporti e nelle relazioni d'affari, sono proibiti comportamenti e pratiche collusive, pagamenti che possano apparire illeciti, tentativi di corruzione e favoritismi, sollecitazioni, dirette o indirette, di vantaggi personali e di carriera per sé o per altri e più in generale atti contrari alle leggi e ai regolamenti applicabili.
L'organo direttivo di CompEd si impegna a garantire un adeguato sistema di controllo interno e a guidare tutta l'organizzazione nel raggiungimento di performance previste per la prevenzione della corruzione in coerenza con le seguenti linee guida:

- garantire un impegno continuo a condurre le proprie attività nel pieno rispetto degli obblighi normativi, verificando costantemente la corretta ed adeguata applicazione delle norme in materia di contrasto alla corruzione e dei requisiti del Sistema di gestione Anticorruzione;
- vietare ogni forma di corruzione e anzi incoraggiare i dipendenti alla segnalazione di sospetti in buona fede senza timore di ritorsioni e considerare la trasparenza e la legalità un valore aggiunto, integrando nei propri processi i controlli e le azioni di miglioramento necessarie a gestire la prevenzione della corruzione;
- adire le opportune azioni disciplinari o legali nei confronti dei soggetti che abbiano tenuto un comportamento illegittimo in contrasto con i principi della presente politica.

Tali indirizzi sono tradotti in obiettivi operativi definiti in uno specifico documento, costantemente monitorati in sede di Riesame dell'Alta Direzione e comunicati a tutta l'organizzazione nei mezzi e canali opportuni.
La Società si impegna a migliorare continuamente il proprio Sistema di Gestione per la Prevenzione della Corruzione e garantisce l'autorità (definita attraverso le responsabilità attribuite alla funzione e rese note a tutto il personale aziendale) e l'indipendenza della Funzione di Conformità per la prevenzione della corruzione, nominata dall'Alta Direzione.

Chi opera in nome e per conto di CompEd è consapevole di incorrere, in caso di comportamenti di tipo corruttivo e di violazione delle Legge in materia di corruzione, in illeciti sanzionabili non solo sul piano penale e amministrativo, ma anche sul piano disciplinare aziendale.

CompEd richiede ai propri "Soci in affari" il rispetto delle Leggi vigenti e della presente Politica Integrata, sulla base di clausole la cui inosservanza implica la risoluzione del contratto.

CompEd, ritenendo lo strumento della segnalazione efficace per contrastare il fenomeno corruttivo, incoraggia le segnalazioni, anche in forma anonima, di presunti fenomeni di corruzione attraverso una specifica procedura aziendale che ne descrive le modalità attuative.

Le segnalazioni in oggetto possono essere inviate con la seguente modalità:

- E-mail all'indirizzo: segnalazione@compedservizi.it
- Lettera all'indirizzo di posta cartacea: Via delle Fabbriche 30E/14

L'Alta Direzione CompEd dà alla presente Politica Integrata la massima diffusione, assicurandosi che sia compresa e attuata da tutto il personale dipendente; a tale scopo essa è resa disponibile sul sito internet aziendale.

8. RESPONSABILITÀ

La presente politica è stata formulata dal RSGI e dal Referente Privacy su incarico della Direzione ed estende la responsabilità su tutti i Sistemi di Gestione. Sarà riesaminata secondo i piani stabiliti direttamente dalla Direzione stessa, almeno annualmente ad ogni riesame della Direzione e comunque al verificarsi di cambiamenti significativi.

Responsabile dell'attuazione della presente Politica è tutto il personale della CompEd Servizi.

La Direzione garantisce il pieno supporto nel consentire l'attuazione della presente politica, affidando alle diverse funzioni compiti di implementazione, gestione e monitoraggio dell'efficacia ed efficienza del sistema integrato. All'interno di ogni funzione è stabilita la definizione degli opportuni ruoli per la gestione SGI e bisogna definire dei momenti di confronto e di condivisione.

Il RSGI e il Referente Privacy facilitano l'attuazione della presente politica attraverso norme e procedure appropriate.

Tutto il personale cui sono assegnati precisi ruoli e responsabilità deve avere un'adeguata competenza per svolgere i compiti richiesti; pertanto, deve essere informato e formato adeguatamente riguardo agli obiettivi dell'Azienda in tema di sicurezza delle informazioni, protezione dei dati personali, continuità operativa e prevenzione della corruzione; inoltre, ha la responsabilità di reagire prontamente agli incidenti di sicurezza e/o non conformità del prodotto/servizio e a segnalare alla Direzione qualsiasi punto debole individuato nel sistema.

Qualsiasi atto o azione non conforme alla presente politica aziendale che metta a rischio la sicurezza delle informazioni e la gestione dei servizi di proprietà della CompEd Servizi o dei suoi Clienti e fornitori sarà soggetto ad azione disciplinare e/o legale, come appropriato, in coerenza con le disposizioni di legge.