Xenia Gestione Documentale S.r.l. (XGD), nata nel 2007 come divisione specializzata in ambito documentale della società Xenia Progetti, oggi può vantare una consolidata esperienza e competenza, acquisita grazie a solide partnership tecnologiche, e alle numerose soluzioni realizzate e servizi forniti ad aziende pubbliche e private. Allo scopo di indirizzare le proprie risorse, personali e fisiche, verso il miglioramento continuo, la Direzione della società stabilisce, attua e mantiene la presente politica aziendale.

La Direzione ha deciso di implementare all'interno della propria struttura organizzativa un **Sistema di Gestione Integrato, conforme alle norme UNI EN ISO 9001, ISO/IEC 27001, con integrazione delle ISO 27017 e ISO 27018, e UNI ISO 37001:2025**.

Per competere nel mercato e svilupparsi nel rispetto delle condizioni di economicità e redditività, la Direzione ritiene indispensabile il processo di "**miglioramento**", che si traduce **nell'impegno da parte di tutte le parti interessate a perseguire la completa soddisfazione delle esigenze e delle aspettative del Cliente**.

Inoltre, considerata la natura del core business di Xenia Gestione Documentale, la Direzione ha ritenuto indispensabile dotarsi di **Information Security Management System**, per garantire a tutti gli stakeholders(dipendenti, clienti e fornitori)i requisiti di **protezione, riservatezza, integrità e disponibilità** del patrimonio informativo nel corso del tempo, con l'obiettivo di assicurare la continuità del business e ridurre al minimo i danni eventuali, prevenendo e riducendo al minimo l'impatto degli incidenti di sicurezza.

L'Organizzazione fa espressamente divieto degli atteggiamenti e dei comportamenti condizionati da pagamenti agevolativi e/o condizionati dalla prospettiva di vantaggi non connessi al regolare funzionamento della attività economica e del business; per raggiungere tale scopo ha ritenuto necessario dotarsi di un **Anti-Bribery Management System.**

Il SGQSIA, si prefigge pertanto il raggiungimento dei seguenti scopi:

QUALITÀ DEI SERVIZI E CUSTOMER CARE

- ✓ Garantire la completa soddisfazione delle esigenze del Cliente e degli stakeholder, migliorando continuamente il servizio in termini di innovazione tecnica e organizzativa;
- ✓ Assicurare al Cliente la omogeneità, la costanza e la continuità del livello qualitativo del prodotto/servizio fornito, razionalizzando nel contempo i costi;
- ✓ Effettuare un monitoraggio continuo sui progetti e servizi erogati, con azioni ideate ad hoc per mantenere un elevato grado di fidelizzazione del Cliente
- ✓ Attuare una comunicazione assertiva e sempre focalizzata al cliente, che miri a mantenere rapporti professionali e di cordialità con la controparte, evitando i conflitti, anche in caso di problemi o reclami;

SICUREZZA DELLE INFORMAZIONI

- ✓ Garantire che le informazioni vengano tutelate e protette da accessi non autorizzati;
- ✓ Assicurare che siano mantenuti nel tempo i requisiti di **autenticità, integrità, affidabilità, leggibilità, e reperibilità** di informazioni e documenti tramite l'insieme di azioni di tutela che l'organizzazione ha attivato;
- ✓ Garantire l'ottemperanza di tutti I trattamenti dei dati alla normativa vigente in termine di privacy (GDPR);

- ✓ Indagare, assicurare, tracciare, trattare e gestire tutte le potenziali, sospette o reali, aree di rischio o vulnerabilità di sicurezza e trattamento delle informazioni, nell'ottica del miglioramento continuo;
- ✓ Proteggere gli asset dell'organizzazione (beni e informazioni) da rischi e/o vulnerabilità esterne, interne, volontarie ed accidentali che possano compromettere l'immagine e la continuità aziendale;
- ✓ Istituire, mantenere e periodicamente testare il piano di Disaster Recovery e Business Continuity, sviluppato secondo le reali esigenze dell'organizzazione;
- ✓ Adottare, mantenere e aggiornare specifiche procedure, norme comportamentali, infrastrutture e dispositivi hardware e software per supportare ed attuare la Politica, inclusi sistemi antivirus, password e piani di continuità
- ✓ Adottare sistemi di sicurezza informatica e cybersicurezza, volti a scongiurare danni provocati da virus, maleware, data breach, manomissioni, intromissioni non autorizzate, che mirino a screditare la reputazione aziendale e a minare il patrimonio informativo dell'azienda e dei clienti che si affidano all'azienda;

CLOUD SERVICE COSTUMER E PROVIDER

- ✓ Valutare e selezionare CSP affidabili e certificati, sottoponendoli a verifica periodica;
- ✓ Verificare che le risorse manutenute all'interno del cloud computing siano in accordo con il gli standard più elevati di sicurezza;
- ✓ Che i dati siano trattati secondo la vigente normativa in tema di protezione dei dati personali;
- ✓ Applicare i requisiti di sicurezza informatica alla progettazione e all'implementazione del servizio cloud, rispettando le esigenze del cliente;
- ✓ Effettuare periodicamente una valutazione dei rischi connessi al cloud computing;
- ✓ Provvedere all'isolamento multi-tenancy e dei clienti dei servizi cloud;
- ✓ Comunicare prontamente ai clienti tutti i cambiamenti rilevanti relativi al servizio cloud erogato;
- ✓ Gestire, manutenere, monitorare e aggiornare il ciclo di vita degli account dei clienti dei servizi cloud.

PERSONALLY IDENTIFIABLE INFORMATION NEI SERVIZI DI PUBLIC CLOUD

- ✓ Verificare e mantenere la conformità alla legislazione applicabile in materia di protezione dei dati personali;
- ✓ Che i dati personali conservati all'interno del cloud pubblico siano protetti adeguatamente secondo la normativa vigente;
- ✓ Che il trattamento dei dati personali venga effettuato solo su istruzione del CSC;
- ✓ Provvedere a notificare prontamente eventuali data breach secondo quanto previsto dalla normativa vigente;
- ✓ Che il personale incaricato sia soggetto agli obblighi di riservatezza e che sia periodicamente formato secondo le attuali normative vigenti.

RELAZIONE CON LE PARTI INTERESSATE

- ✓ Migliorare l'impatto sulla Società Civile (accoglimento stagisti, convegni, iniziative di solidarietà, ecc.);
- ✓ Incrementare l'espansione territoriale dell'azienda e l'ingresso in nuove aree di mercato;
- ✓ Rafforzare il legame tra le strategie aziendali, assetti organizzativi, correttezza e coerenza nei processi primari e di supporto;

- ✓ Creare e mantenere le condizioni per una concreta e duratura partnership con i Fornitori;
- ✓ Favorire un clima lavorativo improntato sulla collaborazione e sul confronto, allo scopo di consentire a tutti i dipendenti di contribuire in maniera attiva al perseguimento dei risultati;
- ✓ Migliorare continuamente la sicurezza nell'ambiente di lavoro, anche in considerazione della prevenzione del diffondersi di eventuali contagi;
- ✓ Limitare i danni provocati dai cambiamenti climatici, adottando strutture in grado di resistere in caso di catastrofi e adeguati strumenti di protezione assicurativa;
- ✓ Ridurre l'impatto ambientale, promuovendo servizi che permettano la riduzione del consumo di carta e di CO2, tramite il rafforzamento della cultura e diffusione dei documenti digitali, aventi valore probatorio.

MANTENERE E MIGLIORARE UN SISTEMA PER LA PREVENZIONE DELLA CORRUZIONE

- ✓ Prevenire la corruzione all'interno dell'organizzazione in maniera tale che non si compiano atti corruttivi;
- ✓ Le transazioni, le relazioni, i rapporti e i contratti interni ed esterni dell'organizzazione devono essere conformi ai principi di **trasparenza**, di **onestà** suscitati dalla nostra legislazione e **conformi** ai requisiti di legge stabiliti dalla nostra Costituzione e disciplinati dal Codice Civile in tutti gli ambiti: lavoro, aspetti societari, commercio, aspetti tributari, ecc.
- ✓ Perseguire la **conformità** del sistema alla Norma e ai requisiti stabiliti nelle procedure, l'**idoneità** delle risorse umane a gestire il sistema, in relazione alla loro formazione, alla loro consapevolezza e al loro grado di coinvolgimento nella comunicazione conformità, l'**adeguatezza** dei processi di prevenzione nell'affrontare la quantità di rischio rilevata e l'**efficacia** nella gestione del rischio di corruzione derivante dal contesto, dai soci in affari coinvolti nelle attività e nei progetti che l'organizzazione conduce
- ✓ Prescrivere il rispetto delle leggi anticorruzione applicabili;
- ✓ Fornire un quadro di riferimento per l'impostazione, la revisione e il raggiungimento degli obiettivi anticorruzione;
- ✓ Aumentare l'impegno a soddisfare i requisiti dell'Anti-Bribery Management System;
- ✓ Incoraggiare le segnalazioni di eventuali sospetti relativi al comportamento del personale e delle persone esterne con cui l'organizzazione lavora, in sicurezza e senza timore di distorsioni;
- ✓ Aumentare l'impegno al miglioramento continuo dell'Anti-Bribery Management System;
- ✓ Mantenere l'autorità e l'indipendenza della Funzione di Conformità del Sistema di Gestione per la Prevenzione della Corruzione;
- ✓ Rispettare le Policy Anticorruzione, rese disponibili a tutti gli stakeholder come Informazione Documentata ed espresse con un linguaggio appropriato.

La presente politica è soggetta a revisione annuale o in seguito a cambiamenti normativi, tecnologici o organizzativi significativi.

Tutti i dipendenti di Xenia Gestione Documentale pensano e agiscono come parte dei processi e quindi - nell'ambito delle loro responsabilità e nel rispetto dei principi guida espressi dalla presente Politica, si impegnano a raggiungere gli obiettivi aziendali.

Tutto il personale, inoltre, è formato regolarmente sui temi della **sicurezza informatica**, della **protezione dei dati personali** e delle **best practice cloud.**

Il nostro obiettivo è rispondere prontamente alle esigenze del Cliente, garantire condizioni di sicurezza nella gestione e nel trattamento dei dati e prevenire la corruzione all'interno dell'organizzazione in maniera tale che non si compiano atti corruttivi.

I comportamenti non conformi a tale politica di prevenzione saranno oggetto di indagine, eventuali sanzioni interne e, nelle ipotesi di reato, verranno denunciati all'autorità giudiziaria

Aci Castello 26/10/2026

La Direzione
Dott. Fabio Massimo Cutuli

FABIO
MASSIMO
CUTULI
26.10.2026
08:07:33
GMT+01:00