

Codice: Politica CO	
Rev. 04	Pag. 1 di 5
Riservatezza: Documento Pubblico	

POLITICA PER LA CONTINUITÀ OPERATIVA

<i>Rev.</i>	<i>Data</i>	<i>Descrizione Modifica</i>
01	10/04/2025	Prima emissione
02	30/07/2025	Minor changes
03	10/06/2026	Aggiornamenti minori
04	08/10/2026	Inserimento concetto Handover nel documento

Tinexta Cyber SpA, nell'ambito delle strategie aziendali adottate a garanzia del suo sviluppo, riconosce che la **Continuità Operativa** sia fondamentale per garantire la resilienza dell'azienda e la soddisfazione dei Clienti. La capacità di mantenere l'erogazione dei servizi critici, anche in situazioni di emergenza o interruzione, è considerata un elemento chiave per raggiungere traguardi ambiziosi in termini di fatturato, redditività e reputazione.

In questo contesto, Tinexta Cyber S.p.A. (da ora solo "Tinexta Cyber"), garantisce l'impegno costante di tutta l'organizzazione per l'adozione e il miglioramento continuo del proprio Sistema di Gestione per la Continuità Operativa, in conformità con lo standard ISO 22301. Questo impegno è volto a proteggere gli interessi dei Clienti e degli stakeholder, assicurando che l'azienda possa rispondere efficacemente a qualsiasi evento che possa compromettere le sue operazioni.

Al fine di perseguire tali obiettivi, le aree di intervento nelle quali intende operare sono:

- ricerca di un'offerta di prodotti e servizi con un elevato rapporto qualità/prezzo, al fine di porsi come azienda di riferimento sul mercato nazionale per i settori nei quali opera;
- l'impegno nell'assicurare, con un approccio olistico, la capacità di prevenire eventi interruttivi, garantendo l'erogazione dei processi e servizi critici secondo livelli di servizio predefiniti, salvaguardando gli interessi dei diversi stakeholder;
- aumento dell'efficienza e della flessibilità produttiva, attraverso il controllo dei processi;
- riconoscimento al Personale del ruolo di risorsa fondamentale per l'Azienda, incentivandone la formazione tecnica, la motivazione e la condivisione degli obiettivi aziendali, la crescita professionale con l'affidamento di sempre maggiori responsabilità gratificanti. Tinexta Cyber, inoltre, nel perseguire le azioni necessarie al miglioramento dei servizi e dei processi aziendali in termini di efficacia ed efficienza, al fine di proporre nuove soluzioni per un mercato in costante cambiamento, intende affiancare le risorse con percorsi di formazione professionale e manageriale specifici. Tali percorsi sono finalizzati allo sviluppo delle competenze necessarie a perseguire gli obiettivi definiti per le linee di business previste dal Piano Industriale;
- definizione di linee guida, procedure e piani finalizzati alla ricerca e mantenimento di un livello di aggiornamento costante e competitivo in merito alle tecnologie innovative che possono conferire benefici in termini economici e qualitativi sui prodotti e sui servizi offerti.

Tinexta Cyber e la Direzione assume la responsabilità e la volontà di:

- integrare la continuità operativa nella strategia aziendale e nei processi decisionali;
- implementare e mantenere processi sistematici per l'analisi dell'impatto operativo e dei rischi derivanti da scenari di interruzione che possono impattare la capacità dell'organizzazione di erogare i prodotti e servizi essenziali;
- Garantire le risorse necessarie per sviluppare, attuare, mantenere e migliorare continuamente il Sistema di Gestione per la Continuità Operativa in conformità alla norma ISO 22301;
- promuovere una cultura per la gestione della continuità operativa, tramite attività di formazione e sensibilizzazione, a tutti i livelli dell'organizzazione assicurando che contribuiscano all'efficacia del Sistema di Gestione della Continuità Operativa;

Codice: Politica CO	
Rev. 04	Pag. 3 di 5
Riservatezza: Documento Pubblico	

- sviluppare idonei strumenti di controllo e di monitoraggio dei processi, definendo obiettivi misurabili per la continuità operativa;
- promuovere e sviluppare i processi e le procedure aziendali con l'obiettivo di garantire e tenere sotto controllo l'applicazione dei regolamenti interni e del Codice Etico e di condotta di Gruppo;
- supportare esercitazioni, test e revisioni periodiche per assicurare l'efficacia dei piani di continuità in coerenza con le linee guida della Capogruppo per la Gestione degli eventi di Crisi;
- segnalare prontamente eventuali eventi che possano compromettere la normale operatività ed attuare le procedure previste nei piani di continuità in caso di evento di interruzione, incidente o emergenza;
- rispettare i requisiti legali, normativi e contrattuali applicabili;
- rispettare il Regolamento in materia di Esercizio del Potere di Direzione e Coordinamento da parte della Capogruppo.

Nel rispetto degli obiettivi aziendali e di quelli condivisi con la Capogruppo, l'attenzione della Direzione è rivolta ad ottenere e migliorare i processi interni ed esterni per un Sistema di Gestione per la Continuità Operativa sempre più:

- *integrato*, in quanto ogni procedura deve raccogliere e fornire le metodologie e gli strumenti necessari per la gestione delle attività aziendali;
- *visibile*, per cui ogni risorsa trovi un riscontro fra quanto definito nei processi e quanto applicato nell'operatività quotidiana;
- *utile*, capace di fornire idonei strumenti informatici e di supporto, necessari per la gestione delle proprie attività;
- *didattico*, utilizzabile sia per dimostrare al Cliente le modalità operative aziendali, ma anche per essere uno strumento di diffusione del know-how operativo aziendale;
- *manageriale*, adatto al monitoraggio e controllo delle attività aziendali, per individuare i punti di forza e le opportunità di miglioramento in un'ottica di efficacia ed efficienza;
- *migliorato*, attraverso la progettazione e realizzazione di processi in applicazione della normativa ISO 22301 e dei suoi aggiornamenti.

La gestione della Politica per la Continuità Operativa applicata da Tinexta Cyber si basa, inoltre, sul concetto del **Miglioramento Continuo**, attuato con l'ausilio derivato dall'elaborazione della documentazione della Politica stessa, comprensiva degli obiettivi e degli impegni per la Continuità Operativa, nonché l'assicurazione che essa sia compresa, attuata e sostenuta a tutti i livelli aziendali, compresi i nuovi assunti.

Nel perseguimento di tali obiettivi, Tinexta Cyber opera secondo strategie indirizzate ai seguenti aspetti:

Verso i **Clienti**:

- seguire l'andamento del mercato ed analizzarne i mutamenti, al fine di fornire al Cliente le soluzioni più adeguate e innovative;

Codice: Politica CO	
Rev. 04	Pag. 4 di 5
Riservatezza: Documento Pubblico	

- assicurare la continuità, l'efficienza e la qualità dei servizi erogati al Cliente mediante il controllo dei processi e la gestione strutturata degli eventuali passaggi di consegne (handover), senza pregiudicare l'operatività del Cliente;
- garantire il miglioramento continuo in termini di Continuità Operativa del servizio/prodotto;
- promuovere iniziative volte a monitorare e migliorare il grado di soddisfazione dei Clienti, anche attraverso il raggiungimento dei livelli di servizio concordati;
- ricercare e mantenere un livello di aggiornamento costante in merito agli ambiti normativi e di competenze specifiche che possono conferire benefici in termini di efficacia ed efficienza dei prodotti e servizi offerti;
- recepire e comprendere i requisiti e le aspettative dei Clienti per fornire servizi e prodotti che rispondano pienamente alle loro esigenze e a quelle di mercato;
- verificare la soddisfazione delle aspettative dei Clienti, garantendo l'erogazione nel continuo dei propri prodotti/servizi;
- monitorare i livelli di soddisfazione raggiunti, attraverso una continua attività di relazione e ascolto;
- garantire l'applicazione e il rispetto del Codice Etico e di Condotta di Gruppo, adottato dall'Azienda.

*Verso le **Risorse Umane**:*

- riconoscere al Personale il ruolo di risorsa fondamentale per l'Azienda, incentivandone la formazione tecnica, la motivazione e la condivisione degli obiettivi aziendali, la crescita professionale con l'affidamento di sempre maggiori responsabilità gratificanti;
- favorire la diffusione di una cultura orientata alla Continuità Operativa e alla ricerca del miglioramento continuo;
- garantire che il processo di formazione risponda alle esigenze richieste dai servizi erogati ai Clienti e al fabbisogno formativo espresso dallo sviluppo di nuovi servizi ed esigenze di mercato e aziendali;
- garantire una costante crescita professionale del Personale, in modo che esso possa rispondere in maniera adeguata alle esigenze del mercato esterno e sia pronto a recepire le innovazioni che si decida di introdurre in Azienda.

*Verso i **Fornitori**:*

- assicurare metodologie di selezione e qualificazione dei Fornitori trasparenti e oggettive;
- assicurare la collaborazione dei Fornitori nelle attività di continuità operativa, inclusi gli eventuali processi di handover, al fine di preservare la continuità dei servizi e il rispetto dei requisiti contrattuali e operativi reciprocamente assunti;
- favorire il coinvolgimento dei Fornitori nella promozione della Continuità Operativa quale strumento indispensabile del progresso comune.

Gli obiettivi generali indicati nel presente documento vengono più analiticamente correlati ai diversi processi ed attività aziendali, e periodicamente monitorati dalla Direzione in occasione dei Riesami previsti nel corso dell'anno.

Codice: Politica CO	
Rev. 04	Pag. 5 di 5
Riservatezza: Documento Pubblico	

Tinexta Cyber ha definito un processo di revisione di tutti i documenti interni, comprese le politiche e i documenti di pratica.

I documenti sono periodicamente rivisti sotto la responsabilità del management di Tinexta, al fine di valutarne la conformità ai requisiti nazionali e internazionali, agli standard, alla legislazione cogente, ai regolamenti vigenti, alle particolari esigenze imposte dall'evoluzione tecnica e tecnologica e all'evoluzione del contesto aziendale.

Il riesame e l'eventuale aggiornamento avvengono almeno una volta all'anno, oppure ogni qualvolta si verifichi una delle seguenti circostanze:

- cambiamenti organizzativi interni che impattano sul sistema;
- modifiche rilevanti dell'architettura hardware o software;
- aggiornamenti normativi;
- cambiamenti nelle procedure, nelle metodologie o nel contesto aziendale.