

NICMA COMPANY riconosce l'importanza strategica dei servizi cloud per il supporto delle proprie attività operative e si impegna ad adottare adeguate misure di sicurezza per garantire la protezione delle informazioni trattate, archiviate o trasmesse attraverso infrastrutture, piattaforme e applicazioni cloud.

L'utilizzo di servizi cloud è preventivamente autorizzato dalla Direzione e dalle funzioni competenti, sulla base di una valutazione dei rischi che consideri aspetti di sicurezza, conformità normativa, protezione dei dati personali, continuità operativa e localizzazione delle informazioni.

PRINCIPI GENERALI

Il presente documento stabilisce che tutte le informazioni riguardanti NICMA COMPANY che devono essere protette contro la diffusione non autorizzata, la modifica, la compromissione e la distruzione.

Queste protezioni sono implementate secondo il principio del "need-to-know", ovvero le informazioni

classificate devono essere condivise solamente con chi ha una legittima necessità di business di accedere alle stesse.

I criteri per identificare secondo quale livello le informazioni siano da classificare, derivano direttamente:

- Dal rischio di generici danni nel caso di diffusione erronea o dolosa all'esterno delle società;
- Dalle leggi/norme sui segreti commerciali ed industriali;
- Dalle leggi/norme sulla protezione dei dati personali.

La Politica di Sicurezza è basata su alcuni principi fondamentali, di seguito elencati:

- I dati Aziendali devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati stessi, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (Integrità e Riservatezza) e resi disponibili laddove dove richiesto dal business NICMA COMPANY (Disponibilità)
- L'accesso ai dati aziendali deve essere fornito in relazione all'attività ed al ruolo dell'utente;
- L'accesso agli utenti deve essere autorizzato dagli Asset Owner (responsabili di Processo e/o di Funzione);
- Tutte le normative legali, statutarie e contrattuali devono essere rispettate;
- Tutti gli utenti che accedono ai dati aziendali devono essere identificati.

Si precisa che il concetto di corretta conservazione dei dati e delle informazioni (Data Retention) è indissolubilmente legato al concetto di sicurezza dei dati e delle informazioni stesse.

Per **NICMA COMPANY**, sono vietati e non rientrano nell'ambito della presente Politica tutti gli strumenti e asset (hardware e software) che gli utenti possono scaricare, installare o utilizzare autonomamente (senza previa autorizzazione dell'azienda) o con l'aiuto di terzi mediante gli strumenti aziendali (notebook, smartphone, tablet), nonché eventuali software open source e dispositivi hardware (es. IoT, chiavette USB, hard disk, fotocamere) senza autorizzazione esplicita da parte dell'azienda, o di cui l'azienda non abbia conoscenza o che non siano stati formalmente censiti e approvati. L'azienda adotta comunque misure tecniche ed organizzative per rilevare e gestire tali asset non autorizzati, inclusi controlli periodici, monitoraggi dei sistemi e audit.

OBIETTIVI

La presente politica mira a proteggere la riservatezza, l'integrità e la disponibilità delle informazioni,

garantendo che siano al sicuro da minacce interne ed esterne, deliberate o accidentali.

Questa politica si applica quindi a tutti i dati aziendali creati, ricevuti o gestiti dall'azienda, inclusi documenti elettronici, e-mail, registrazioni cartacee e altri formati di dati.

NICMA COMPANY considera la protezione del proprio patrimonio di informazioni elemento fondamentale per la tutela e la continuità del proprio business.

Rev.	Emissione	COD	Pagina
0	03/08/2026	SIC.10.MO	1 di 4

Altro obiettivo del presente documento è quello di definire i principi e le linee guida da adottare, nonché i ruoli, le funzioni e le responsabilità nella realizzazione di un efficace sistema di protezione delle informazioni, che devono essere rispettate da tutte le persone che operano all'interno di **NICMA COMPANY**. In questo ambito, la sicurezza dell'informazione è vista un tutt'uno come un insieme di processi e tecnologie, misure organizzative e comportamentali finalizzate alla garanzia degli aspetti di Riservatezza, Integrità e Disponibilità delle informazioni, ed alla loro corretta condivisione, in funzione del ruolo e del profilo dell'utente.

In ottica di Data Retention (conservazione dei dati e delle informazioni) ulteriore obiettivo di questa politica è anche quello di definire le linee guida per la conservazione e l'eliminazione dei dati aziendali, garantendo la conformità alle normative legali e la protezione delle informazioni sensibili.

Nello specifico, le finalità del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) da conseguire sono:

- a) assicurare l'evidenza dei processi autorizzativi e delle attività svolte a fini legali, fiscali ed operativi
- b) garantire la protezione delle informazioni aziendali e la continuità delle attività lavorative, assicurando che il livello di protezione previsto sia attuato in funzione della criticità delle informazioni da proteggere;
- c) garantire l'attuazione pratica della Politica Aziendale per la Sicurezza e Protezione dei dati e del rispetto della Privacy integrando i requisiti del Sistema di Gestione per la Sicurezza delle informazioni nei processi dell'organizzazione con la finalità di soddisfare i requisiti stessi e fissando un quadro di riferimento per identificare e gestire i relativi obiettivi;
- e) garantire la confidenzialità, l'integrità e la disponibilità delle informazioni su tutto il ciclo di trattamento gestito;
- f) garantire un'adeguata sicurezza logica e fisica nella gestione ed erogazione dei servizi salvaguardando i prodotti ed i relativi servizi contrastando nel contempo la criminalità informatica (virus, attacchi in rete, etc.);
- g) garantire elevati livelli di affidabilità dei propri sistemi informativi al fine di minimizzare le potenziali indisponibilità dei servizi;
- h) redigere, diffondere, organizzare e verificare procedure e risorse per affrontare eventi di natura disastrosa e garantire la continuità operativa;
- i) individuare e gestire rischi e opportunità per assicurare il raggiungimento degli obiettivi minimizzando gli effetti indesiderati e massimizzando le ricadute positive.

Per quanto riguarda la Data Retention si possono identificare ulteriori obiettivi che nel caso di NICMA COMPANY si possono riassumere con quelli sotto riportati:

- a) Conformità Legale: Assicurare che l'azienda rispetti tutte le leggi e i regolamenti relativi alla conservazione dei dati, evitando sanzioni e responsabilità legali.
- b) Protezione dei Dati: Salvaguardare le informazioni sensibili e personali da accessi non autorizzati, perdite o violazioni.
- c) Efficienza Operativa: Ottimizzare la gestione dei dati, riducendo il volume di informazioni obsolete o non necessarie, migliorando così l'efficienza dei sistemi informatici.
- d) Recupero dei Dati: Facilitare il recupero rapido e accurato dei dati necessari per le operazioni aziendali, le decisioni strategiche e le richieste legali.
- e) Riduzione dei Costi: Minimizzare i costi associati alla conservazione e alla gestione dei dati, eliminando quelli non più necessari

Ogni scostamento dalla presente Politica, non è riconosciuto come volontà della Direzione Aziendale ed è oggetto di indagine ed eventuale azione disciplinare.

SICUREZZA DEI SERVIZI CLOUD

Ai fini della ISO/IEC 27018 la presente Politica si applica ai dati personali trattati mediante servizi di cloud pubblico quando il Cloud Service Provider opera, per conto di NICMA COMPANY, in qualità di responsabile del trattamento. I relativi requisiti sono applicati in funzione dei ruoli privacy effettivamente assunti dalle parti, delle istruzioni documentate impartite al fornitore e dei rischi associati al trattamento.

Nell'ambito della gestione dei servizi cloud, NICMA COMPANY adotta i seguenti principi:

Rev.	Emissione	COD	Pagina
0	03/08/2026	SIC.10.MO	2 di 4

a) *Ruoli e Responsabilità*: definizione chiara e documentata dei ruoli e delle responsabilità tra NICMA COMPANY e il *Cloud Service Provider (CSP)*, in conformità al modello di responsabilità condivisa applicabile al servizio utilizzato.

Per ogni servizio cloud che comporti il trattamento di dati personali, NICMA COMPANY identifica e documenta i ruoli privacy delle parti, le categorie di interessati e di dati trattati, le finalità e la durata del trattamento, le operazioni autorizzate e le istruzioni impartite al Cloud Service Provider. Il fornitore tratta i dati personali esclusivamente sulla base di tali istruzioni, salvo obblighi di legge applicabili, e segnala senza ritardo eventuali istruzioni che ritenga in contrasto con la normativa vigente.

b) *Selezione e Valutazione dei Fornitori Cloud*: i fornitori di servizi cloud sono sottoposti a processi di qualifica e valutazione che tengano conto delle certificazioni possedute, delle misure di sicurezza e protezione dei dati adottate, delle garanzie contrattuali offerte, della capacità di rispettare i requisiti normativi applicabili, dei luoghi di trattamento, dell'impiego di sub-responsabili, delle modalità di restituzione e cancellazione dei dati e del supporto fornito a NICMA COMPANY nell'esercizio dei propri obblighi verso gli interessati e le autorità competenti.

c) *Protezione delle Informazioni nel Cloud*: Le informazioni archiviate o elaborate nei servizi cloud sono protette mediante adeguati controlli di sicurezza, inclusi meccanismi di autenticazione, autorizzazione, cifratura, segregazione dei dati e monitoraggio degli accessi.

d) *Gestione degli Accessi*: accesso ai servizi cloud limitato agli utenti autorizzati secondo il principio del minimo privilegio e del need-to-know.

e) *Gestione degli Ambienti Virtuali*: ambienti virtualizzati utilizzati per l'erogazione dei servizi cloud sono adeguatamente configurati, monitorati e protetti contro accessi non autorizzati, vulnerabilità e minacce informatiche.

I dati personali affidati a un Cloud Service Provider non possono essere utilizzati per finalità proprie del fornitore, incluse attività pubblicitarie, commerciali, di profilazione o di analisi non necessarie all'erogazione del servizio, salvo preventiva autorizzazione documentata di NICMA COMPANY e presenza di un'idonea base giuridica. Ogni comunicazione a terzi deve essere limitata a quanto autorizzato o richiesto dalla legge e deve essere tracciabile.

NICMA COMPANY acquisisce e mantiene informazioni aggiornate sui Paesi e sulle aree geografiche in cui i dati personali sono archiviati, elaborati o sottoposti a backup. Ogni trasferimento o accesso da Paesi terzi è preventivamente valutato e gestito mediante idonee garanzie legali, contrattuali e tecniche, nel rispetto della normativa applicabile e degli impegni assunti verso gli interessati.

Il ricorso a sub-responsabili da parte del Cloud Service Provider è soggetto alle condizioni contrattuali definite da NICMA COMPANY. Il fornitore rende disponibile l'elenco aggiornato dei sub-responsabili, comunica preventivamente le variazioni significative e assicura che ciascun sub-responsabile sia vincolato a obblighi di sicurezza, riservatezza, protezione dei dati, restituzione e cancellazione non inferiori a quelli applicabili al fornitore principale.

f) *Monitoraggio e Registrazione degli Eventi*: raccolti, conservati e periodicamente analizzati i log relativi all'utilizzo dei servizi cloud, agli accessi, alle modifiche di configurazione e agli eventi di sicurezza, nel rispetto delle normative vigenti.

Qualora riceva una richiesta giuridicamente vincolante di divulgazione dei dati personali da parte di un'autorità, il Cloud Service Provider informa tempestivamente NICMA COMPANY prima della comunicazione, salvo espresso divieto di legge. Il fornitore verifica la legittimità e la portata della richiesta, limita la divulgazione ai soli dati necessari e conserva evidenza delle valutazioni e delle comunicazioni effettuate.

g) *Continuità Operativa e Backup*: i servizi cloud considerati critici sono previste adeguate misure di backup, disaster recovery e business continuity, garantendo la disponibilità e il ripristino delle informazioni entro tempi compatibili con le esigenze aziendali.

h) *Restituzione e Cancellazione dei Dati*: alla cessazione del rapporto contrattuale, alla scadenza dei termini di conservazione o quando i dati non siano più necessari, i dati personali conservati presso il Cloud Service Provider sono restituiti a NICMA COMPANY in un formato concordato e successivamente cancellati in modo sicuro dai sistemi, dalle copie e dai supporti sotto il controllo del fornitore, fatti salvi gli obblighi di legge. Il completamento della cancellazione è attestato mediante evidenze verificabili; eventuali dati residui contenuti nei backup restano protetti, non sono ulteriormente trattati e sono eliminati secondo i cicli documentati di sovrascrittura.

Rev.	Emissione	COD	Pagina
0	03/08/2026	SIC.10.MO	3 di 4

i) *Gestione degli Incidenti di Sicurezza e delle Violazioni di Dati Personali*: gli incidenti che coinvolgono servizi cloud sono tempestivamente rilevati, contenuti, segnalati, gestiti e documentati secondo le procedure aziendali. Il Cloud Service Provider informa NICMA COMPANY senza ingiustificato ritardo di ogni violazione di dati personali, fornendo le informazioni disponibili su natura dell'evento, dati e interessati coinvolti, probabili conseguenze, misure adottate o proposte, tempi, aggiornamenti successivi ed evidenze utili alla valutazione e agli eventuali adempimenti verso autorità e interessati.

Il Cloud Service Provider assicura a NICMA COMPANY un'assistenza tempestiva e documentata per la gestione delle richieste degli interessati, incluse le attività di accesso, rettifica, cancellazione, limitazione, opposizione e portabilità applicabili. Il fornitore non risponde direttamente all'interessato, salvo autorizzazione o obbligo di legge, e mette a disposizione funzioni, informazioni ed evidenze che consentano di rispettare i termini normativi.

j) *Conformità e Audit*: NICMA COMPANY si riserva il diritto di verificare, direttamente o tramite evidenze documentali e certificazioni riconosciute, l'efficacia delle misure di sicurezza adottate dai fornitori cloud e la loro conformità ai requisiti contrattuali, normativi e aziendali.

La progettazione, configurazione e modifica dei servizi cloud applica i principi di protezione dei dati fin dalla progettazione e per impostazione predefinita. Sono raccolti e trattati soltanto i dati personali adeguati, pertinenti e necessari alle finalità autorizzate; le configurazioni predefinite limitano accessi, conservazione, copie, funzionalità e visibilità dei dati al minimo necessario. Quando appropriato in base al rischio, sono adottate tecniche di pseudonimizzazione o anonimizzazione.

k) *Utilizzo Sicuro dei Servizi Cloud*: Gli utenti autorizzati devono utilizzare i servizi cloud esclusivamente per finalità aziendali, nel rispetto delle politiche interne di sicurezza delle informazioni, delle procedure operative e delle istruzioni fornite dall'organizzazione.

La presente Politica rappresenta l'impegno dell'Organizzazione verso la tutela delle informazioni, dei dati personali e dei servizi cloud attraverso l'applicazione dei principi di sicurezza e protezione dei dati, la gestione dei rischi, il rispetto degli obblighi legali, contrattuali e normativi e il miglioramento continuo del Sistema di Gestione, in coerenza con ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018.

03/08/2026

NICMA COMPANY SRL SB

Rev.	Emissione	COD	Pagina
0	03/08/2026	SIC.10.MO	4 di 4

PUBBLICA