SECURITY & COMPLIANCE

Sintesi incident response e vulnerability disclosure

Canali, triage, comunicazione e divulgazione responsabile.

Prodotto	Andrea AI
Codice	AND-PUB-12-IT
Edizione documentale	Edizione del 29 luglio 2026
Efficacia / riesame	2026-07-29 / 2027-01-29
Titolare del documento	Niltech Europe S.r.l. · Compliance & Security
Classificazione	Pubblico

Preambolo, natura ed efficacia del documento

Niltech Europe S.r.l., con sede legale in Via Calmaggiore 5, 31100 Treviso (TV), Italia, P. IVA IT 05614380268 (di seguito «Niltech»), adotta il presente documento al fine di spiegare come segnalare vulnerabilità e come Niltech governa incidenti, data breach, comunicazioni e miglioramento senza divulgare dettagli sensibili.

Il documento è un atto societario di trasparenza e accountability. Non costituisce certificazione di terza parte, parere legale destinato a soggetti diversi dalla società, garanzia assoluta di sicurezza o dichiarazione generalizzata di conformità; gli impegni contrattuali derivano esclusivamente dagli accordi applicabili.

Il documento coordina la gestione degli incidenti con gli articoli 33 e 34 GDPR, con gli obblighi contrattuali e, ove applicabili al soggetto o al cliente, con NIS2, DORA e Cyber Resilience Act. La qualificazione dell'evento e gli obblighi di notifica sono accertati caso per caso.

Ambito soggettivo e oggettivo

Il perimetro oggettivo comprende Andrea AI, le relative interfacce pubbliche e i trattamenti strettamente connessi alle funzionalità descritte. Il sito commerciale e la libreria documentale sono pubblicati su andreaaiagent.com e utilizzano infrastruttura Bluehost, MySQL e il trasporto di posta del server. L'applicazione è resa disponibile sul distinto dominio andreaai.net mediante infrastruttura Hetzner; Pinecone, Cloudflare, OpenAI e Google Gemini intervengono nei limiti delle funzioni e degli accordi applicabili.

Le operazioni considerate riguardano acquisizione e analisi di documenti e immagini, supporto alla lettura di polizze, stime e bozze di relazione, organizzazione del fascicolo e indicatori ESG solo quando fondati su dati verificabili. Le categorie di informazioni potenzialmente interessate sono: dati di contatto e prospect sul sito; nell'applicazione, dati di pratica, documenti, immagini, note, metadati tecnici e output assistiti dall'IA secondo configurazione e contratto. L'effettivo ruolo privacy, il titolo giuridico e l'ampiezza del trattamento dipendono dal rapporto contrattuale e dalle istruzioni lecite del soggetto che determina finalità e mezzi essenziali.

Definizioni e criteri interpretativi

- «Servizio»: l'insieme delle funzionalità di Andrea AI rese disponibili in base al contratto.
- «Cliente»: la persona giuridica o il professionista che conclude il contratto con Niltech.
- «Utente autorizzato»: la persona fisica abilitata dal Cliente a utilizzare il Servizio sotto la sua responsabilità.
- «Dati del Cliente»: dati, documenti, immagini, istruzioni e ogni altro contenuto conferito o generato per conto del Cliente.
- «Output assistito»: risultato elaborato mediante regole automatizzate o componenti di intelligenza artificiale, soggetto ai controlli indicati.
- «Fornitore ulteriore»: soggetto terzo che presta a Niltech un servizio tecnico rilevante per il perimetro documentato.

- «Incidente»: evento che compromette o può compromettere riservatezza, integrità, disponibilità, autenticità o resilienza.
- «Giorno lavorativo»: ogni giorno diverso da sabato, domenica o festività nazionale italiana.

Obblighi e presidi specifici

1. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a fornire un canale monitorato e informazioni minime per la segnalazione. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

2. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a registrare ora di conoscenza, sistemi, dati, impatto e owner. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

3. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a eseguire triage, contenimento, conservazione delle prove e recupero. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

4. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a valutare ruoli, soglie e termini di notifica applicabili. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

5. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a coordinare comunicazioni accurate evitando speculazioni o pregiudizio. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

6. Niltech, nei limiti del ruolo assunto e ferme le responsabilità del Cliente, provvede a chiudere con cause, azioni, verifica e lessons learned. Owner, perimetro, dipendenze, criterio di accettazione ed evidenza sono identificati nel fascicolo applicabile; in loro assenza il presidio non è considerato dimostrato.

Segnalazioni

Incidenti o vulnerabilità possono essere segnalati a info@nil-tech.net indicando prodotto, impatto osservato, passaggi riproducibili e recapito. Non includere dati personali o segreti non necessari.

Gestione

Il processo prevede registrazione, triage, contenimento, preservazione delle evidenze, correzione, recupero, valutazione delle notifiche e riesame. Priorità e comunicazioni dipendono dall’impatto verificato.

Coordinamento

Il segnalante deve evitare accesso persistente, esfiltrazione, interruzione, ingegneria sociale e pubblicazione prematura. Niltech coordina aggiornamenti in buona fede senza promettere ricompense o tempi non concordati.

Notifiche normative

GDPR, NIS2, DORA, CRA e obblighi contrattuali sono valutati per applicabilità, ruolo e termini a partire dal momento di conoscenza documentato.

Segnalazione responsabile e coordinamento

Le segnalazioni devono descrivere asset o URL, impatto ipotizzato, passi riproducibili e contatto del segnalante, evitando accesso persistente, esfiltrazione, alterazione, indisponibilità, social engineering e divulgazione anticipata. L’invio non autorizza attività vietate dalla legge; Niltech valuta in buona fede la segnalazione e coordina tempi di rimedio e comunicazione.

Il canale pubblico non sostituisce i canali di emergenza o quelli contrattuali del Cliente. Informazioni che potrebbero aggravare il rischio sono scambiate in modo riservato e limitate a chi deve intervenire.

Valutazione giuridica e termini applicabili

Ogni evento è distinto, secondo i fatti, in incidente di sicurezza, violazione di dati personali, vulnerabilità attivamente sfruttata, incidente NIS2 o incidente ICT rilevante per un Cliente soggetto a DORA. Le soglie, i destinatari e i termini non sono intercambiabili; il runbook conserva cronologia, fonti, decisione e notifiche.

Ai sensi del GDPR, Niltech quale responsabile informa il titolare senza ingiustificato ritardo; il titolare valuta notifica all'autorità entro settantadue ore ove richiesta e comunicazione agli interessati in caso di rischio elevato. Il D.lgs. 138/2024 si applica soltanto ai soggetti e servizi nel relativo perimetro. Gli obblighi di reporting del Cyber Resilience Act decorrono dall'11 settembre 2026 per i soggetti e prodotti cui il regolamento si applica; la relativa preparazione non equivale ad ammissione di applicabilità.

Ripartizione delle responsabilità e limiti di affidamento

Il Cliente garantisce, per quanto di propria competenza, la liceità dei dati e delle istruzioni conferite, l'abilitazione degli utenti, l'adeguatezza delle basi giuridiche e delle informative, nonché la verifica professionale degli output. Niltech resta responsabile delle attività direttamente poste sotto il proprio controllo e non assume le funzioni regolamentari, deontologiche o decisionali proprie del Cliente.

Gli output di Andrea AI hanno natura ausiliaria. Salvo patto espresso e le norme inderogabili, essi non costituiscono parere legale, perizia, decisione assicurativa, determinazione di responsabilità, valutazione creditizia o altro atto riservato. Il destinatario deve esaminare fonti, completezza, coerenza e conseguenze prima di utilizzarli.

Nessuna clausola limita responsabilità che non possa essere esclusa per legge. Fuori da tali ipotesi, imputazione, rimedi, limiti e criteri di quantificazione seguono il contratto applicabile, tenuto conto del concorso del danneggiato, dell'obbligo di mitigazione e della prevedibilità del danno secondo la legge regolatrice.

Prova, riesame, richieste e legge applicabile

Ogni affermazione materiale deve poter essere ricondotta a un contratto, una configurazione approvata, un registro, un verbale, un test, un log o altra evidenza attendibile. Dichiarazioni del fornitore e controlli propri di Niltech sono mantenuti distinti. L'assenza di incidenti non prova, da sola, l'efficacia di una misura.

Le revisioni sono datate, motivate e approvate. Una revisione successiva non modifica retroattivamente i fatti o gli impegni applicabili a periodi precedenti. Le copie pubblicate sono identificate mediante codice, data e impronta crittografica; tali elementi provano l'integrità della copia, non l'efficacia sostanziale dei controlli descritti.

Segnalazioni, richieste di chiarimento, esercizio di diritti e contestazioni possono essere inviati a info@nil-tech.net. Niltech verifica l'identità e la legittimazione quando necessario, registra la richiesta, risponde nei termini applicabili e comunica eventuali proroghe o dinieghi motivati.

Salvo diversa disposizione inderogabile o pattuizione scritta, la legge italiana disciplina l'interpretazione del documento. La versione italiana costituisce il testo di riferimento; la traduzione inglese è fornita per agevolare la consultazione.

Fonti ufficiali e data normativa

Riferimenti verificati al 2026-07-29. L'applicabilità, il ruolo e le eventuali decorrenze devono essere nuovamente accertati sul caso concreto.

- Regolamento (UE) 2016/679 (GDPR)
- EDPB — Linee guida 01/2021 sugli esempi di notifica delle violazioni di dati personali
- Direttiva (UE) 2022/2555 (NIS2)
- D.lgs. 4 settembre 2024, n. 138 — recepimento NIS2 in Italia
- Regolamento (UE) 2022/2554 (DORA)
- Regolamento (UE) 2024/2847 (Cyber Resilience Act)
- Commissione europea — Quadro di attuazione e scadenze del Cyber Resilience Act, 27 luglio 2026