SECURITY & COMPLIANCE

Incident response and vulnerability disclosure summary

Channels, triage, communication and responsible disclosure.

Product	ClaimEvidence
Code	CLE-PUB-12-EN
Document edition	Edition dated 30 August 2026
Effective / review	2026-08-30 / 2027-02-28
Document owner	Nil Tech Europe S.r.l. · Compliance & Security
Classification	Public

Preamble, nature and effect of this document

Nil Tech Europe S.r.l., with registered office at Via Calmaggiore 5, 31100 Treviso (TV), Italia, VAT No. IT 05614380268 (“Niltech”), adopts this document in order to explain vulnerability reporting and how Niltech governs incidents, breaches, communications and improvement without disclosing sensitive details.

This document is a corporate transparency and accountability record. It is not a third-party certification, legal opinion addressed to persons other than the company, absolute security warranty or blanket compliance statement; contractual commitments arise solely from the applicable agreements.

This document coordinates incident management with Articles 33 and 34 GDPR, contractual duties and, where applicable to the relevant entity or customer, NIS2, DORA and the Cyber Resilience Act. Event qualification and notification duties are determined case by case.

Personal and material scope

The objective scope includes ClaimEvidence, its public interfaces and processing strictly connected with the described functions. The corporate website and document library are published on claimevidence.tech; the application service is available through the separate app.claimevidence.tech domain. Hostinger provides infrastructure and, according to the applicable configuration, mail transport. MySQL/MariaDB is software running in the controlled environment and not a separate subprocessor unless a distinct managed service is used. OpenAI provides API services only for enabled functions; any separate email provider must be identified and assessed before use.

The relevant operations concern guided photo and document collection, case organisation, completeness checks, configurable analytical support, human review and export. Potential information categories are: demo and security-pack requests on the site; in the application, case identifiers, authorised contacts, photographs, documents, notes, session metadata and assisted outputs. The actual privacy role, lawful basis and extent of processing depend on the contractual relationship and the lawful instructions of the party determining purposes and essential means.

Definitions and interpretation

- “Service” means the ClaimEvidence functions made available under the agreement.
- “Customer” means the legal person or professional entering into the agreement with Niltech.
- “Authorised User” means an individual enabled by the Customer to use the Service under its responsibility.
- “Customer Data” means data, documents, images, instructions and other content submitted or generated on the Customer’s behalf.

- “Assisted Output” means a result produced through automated rules or artificial-intelligence components and subject to the stated controls.
- “Further Supplier” means a third party providing Niltech with a technical service relevant to the documented scope.
- “Incident” means an event compromising or capable of compromising confidentiality, integrity, availability, authenticity or resilience.
- “Business Day” means a day other than Saturday, Sunday or an Italian national public holiday.

Specific duties and safeguards

1. Within its assigned role and without prejudice to the Customer’s responsibilities, Niltech shall provide a monitored channel and minimum reporting information. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

2. Within its assigned role and without prejudice to the Customer’s responsibilities, Niltech shall record awareness time, systems, data, impact and owner. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

3. Within its assigned role and without prejudice to the Customer’s responsibilities, Niltech shall perform triage, containment, evidence preservation and recovery. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

4. Within its assigned role and without prejudice to the Customer’s responsibilities, Niltech shall assess applicable roles, thresholds and notification deadlines. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

5. Within its assigned role and without prejudice to the Customer’s responsibilities, Niltech shall coordinate accurate communications avoiding speculation or prejudice. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

6. Within its assigned role and without prejudice to the Customer’s responsibilities, Niltech shall close with causes, actions, verification and lessons learned. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

Reports

Incidents or vulnerabilities may be reported to info@nil-tech.net with product, observed impact, reproducible steps and contact details. Do not include unnecessary personal data or secrets.

Handling

The process includes recording, triage, containment, evidence preservation, remediation, recovery, notification assessment and review. Priority and communications depend on verified impact.

Coordination

The reporter must avoid persistence, exfiltration, disruption, social engineering and premature publication. Niltech coordinates good-faith updates without promising rewards or unagreed times.

Regulatory notifications

GDPR, NIS2, DORA, CRA and contractual duties are assessed for applicability, role and deadlines from the documented awareness time.

Scope, audience and status of this document

This document is intended for customers, prospects, authorised users, advisers and control functions needing to understand the ClaimEvidence scope. Its specific objective is to explain vulnerability reporting and how Niltech governs incidents, breaches, communications and improvement without disclosing sensitive details. It applies to the stated document revision and date and must be read with the applicable agreement, order, DPA, technical specifications and controlled procedures.

The corporate website and document library are published on claimevidence.tech; the application service is available through the separate app.claimevidence.tech domain. Hostinger provides infrastructure and, according to the applicable configuration, mail transport. MySQL/MariaDB is software running in the controlled environment and not a separate subprocessor unless a distinct managed service is used. OpenAI provides API services only for enabled functions; any separate email provider must be identified and assessed before use.

Executed agreements and actually approved configurations prevail in case of inconsistency. Public information describes the control programme; it does not turn optional provider capabilities into Niltech controls or automatically attest legal applicability or satisfaction.

Exceptions, non-conformity and escalation

A deviation is not accepted by custom. The owner records the affected requirement, cause, impact, exposed data and persons, compensating measures, approver, expiry and closure criterion. The exception is reviewed if risk changes or a measure does not work as expected.

Incidents, possible unlawful processing, loss of data control, outputs with severe impact, contractual breaches, unapproved suppliers or unreliable evidence must be escalated without delay. Current Legal and functional scope: Payment services are outside the scope described by this documentation.

- contain risk and suspend the affected phase where needed
- preserve evidence, timing, decisions and communications
- involve privacy, security, product, legal or management owners as appropriate
- resume only after measure verification and documented authorisation

Review, change and improvement

The document is reviewed at least every six months and earlier when purpose, audience, data, GDPR or AI Act role, supplier, model, architecture, location, contractual terms or legal requirements change. Incidents, complaints, failed tests and new vulnerabilities trigger an extraordinary review.

Each review records inputs, participants, decision, changes, superseded evidence, remaining gaps and next date. Material corrections are published without retroactively altering the prior document revision. Contact and requests: info@nil-tech.net.

- check change register and related documents
- retest affected controls
- update manifest, PDF, HTML and hashes
- notify recipients where the change affects their rights or duties

Responsible reporting and coordination

Reports should identify the asset or URL, suspected impact, reproducible steps and reporter contact while avoiding persistent access, exfiltration, alteration, unavailability, social engineering and premature disclosure. Submission does not authorise unlawful activity; Niltech assesses the report in good faith and coordinates remediation and disclosure timing.

The public channel does not replace emergency channels or the Customer’s contractual channels. Information capable of increasing risk is exchanged confidentially and limited to those who must act.

Legal assessment and applicable deadlines

Each event is classified on the facts as a security incident, personal-data breach, actively exploited vulnerability, NIS2 incident or ICT incident relevant to a DORA-regulated Customer. Thresholds, recipients and deadlines are not interchangeable; the runbook preserves timeline, sources, decision and notifications.

Under the GDPR, Niltech as processor informs the controller without undue delay; the controller assesses notification to the authority within seventy-two hours where required and communication to individuals in cases of high risk. Italian Legislative Decree 138/2024 applies only to entities and services within its scope. Cyber Resilience Act reporting duties apply from 11 September 2026 to entities and products within that Regulation's scope; preparation does not amount to an admission of applicability.

Allocation of responsibility and reliance limitations

Within its sphere of responsibility, the Customer warrants the lawfulness of submitted data and instructions, user authorisation, suitable lawful bases and notices, and professional verification of outputs. Niltech remains responsible for activities directly under its control and does not assume the Customer's regulatory, professional or decision-making functions.

Outputs from ClaimEvidence are auxiliary. Unless expressly agreed and subject to mandatory law, they are not legal advice, an expert determination, insurance decision, liability finding, credit assessment or other reserved professional act. The recipient must examine sources, completeness, consistency and consequences before use.

Nothing excludes liability that cannot lawfully be excluded. Outside those cases, attribution, remedies, limitations and quantification principles follow the applicable agreement, taking account of contributory conduct, mitigation duties and foreseeability under the governing law.

Evidence, review, requests and governing law

Every material assertion must be traceable to a contract, approved configuration, register, minutes, test, log or other reliable evidence. Supplier statements and Niltech controls are kept distinct. Absence of incidents is not, by itself, proof that a measure is effective.

Revisions are dated, reasoned and approved. A later revision does not retroactively alter facts or commitments applicable to earlier periods. Published copies are identified by code, date and cryptographic digest; those elements evidence copy integrity, not the substantive effectiveness of described controls.

Reports, clarification requests, rights requests and complaints may be sent to info@nil-tech.net. Niltech verifies identity and authority where necessary, records the request, responds within applicable periods and communicates any reasoned extension or refusal.

Unless mandatory law or a written agreement provides otherwise, Italian law governs interpretation. The Italian text is controlling; the English translation is provided for convenience.

Official sources and legal date

References checked on 2026-08-30. Applicability, role and any relevant commencement dates must be reassessed against the concrete facts.

- Regulation (EU) 2016/679 (GDPR)
- EDPB — Guidelines 01/2021 on examples regarding personal data breach notification
- Directive (EU) 2022/2555 (NIS2)
- Italian Legislative Decree No. 138 of 4 September 2024 — NIS2 implementation
- Regulation (EU) 2022/2554 (DORA)
- Regulation (EU) 2024/2847 (Cyber Resilience Act)
- European Commission — Cyber Resilience Act implementation framework and dates, 27 July 2026

Document control: the copy identified in the manifest through its SHA-256 digest is the document edition published on the stated date. The header seal is neutral corporate artwork and is not a digital signature, third-party attestation or certification.