SECURITY & COMPLIANCE

Software lifecycle security, vulnerabilities and updates

Development lifecycle, dependency management and vulnerability remediation.

Product	Andrea AI
Code	AND-PUB-20-EN
Document edition	Edition dated 29 July 2026
Effective / review	2026-07-29 / 2027-01-29
Document owner	Niltech Europe S.r.l. · Compliance & Security
Classification	Public

Preamble, nature and effect of this document

Niltech 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 describe how requirements, code, dependencies, testing, distributions, vulnerabilities and updates are governed through development.

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 governs security throughout the software lifecycle, including requirements, design, implementation, verification, distribution, maintenance and vulnerability handling, consistently with protection by design and, where applicable, the Cyber Resilience Act.

Personal and material scope

The objective scope includes Andrea AI, its public interfaces and processing strictly connected with the described functions. The commercial website and document library are published on andreaaiagent.com and use Bluehost infrastructure, MySQL and server mail transport. The application is made available through the separate andreaai.net domain on Hetzner infrastructure; Pinecone, Cloudflare, OpenAI and Google Gemini are involved only within the functions and agreements applicable to them.

The relevant operations concern document and image intake and analysis, policy-reading support, estimates and report drafts, case-file organisation, and ESG indicators only where supported by verifiable data. Potential information categories are: contact and prospect data on the website; in the application, case data, documents, images, notes, technical metadata and AI-assisted outputs according to configuration and contract. 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 Andrea AI 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 translate risks and requirements into verifiable acceptance criteria. 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 protect repositories, branches, reviews, pipelines and secrets. 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 analyse dependencies, licences, components and vulnerabilities. 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 perform proportionate functional, security, privacy and regression tests. 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 distribution identified artefacts with rollback and segregation. 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 receive, assess, remediate and communicate vulnerabilities and updates. The applicable file identifies the owner, scope, dependencies, acceptance criterion and evidence; absent those elements, the safeguard is not treated as demonstrated.

Change lifecycle

Requirements, design, review, testing, approval, distribution and rollback are proportionate to risk. Environments and access are separated as provided by the architecture.

Controls

- input validation, output encoding and server-side authorisation
- secret and dependency management without credentials in code
- proportionate automated tests, review and scanning
- logging without unnecessary data or secrets

Vulnerabilities

Reports are validated, classified by impact and exploitability, remediated, tested and distributiond under control. Actual priorities depend on risk and fix availability.

Updates and support

Supported components, dependencies, exceptions and end of support are tracked in the technical register. CRA duties are assessed by role and product qualification.

Scope, audience and status of this document

This document is intended for customers, prospects, authorised users, advisers and control functions needing to understand the Andrea AI scope. Its specific objective is to describe how requirements, code, dependencies, testing, distributions, vulnerabilities and updates are governed through development. 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 commercial website and document library are published on andreaaiagent.com and use Bluehost infrastructure, MySQL and server mail transport. The application is made available through the separate andreaai.net domain on Hetzner infrastructure; Pinecone, Cloudflare, OpenAI and Google Gemini are involved only within the functions and agreements applicable to them.

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: The documented scope includes the commercial website, the public library and, where expressly stated, processing connected with the application.

- 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

Lifecycle and security by design

Security and data-protection requirements are defined before change, mapped to assets and threats, verified through review, testing and approval and maintained over time. Changes to authentication, authorisation, encryption, logs, uploads, AI processing, dependencies or deletion require analysis proportionate to impact.

Credentials and secrets are not included in code or public artefacts. Components and dependencies are inventoried with provenance and conditions; known vulnerabilities are assessed for exploitability and impact, not only an abstract score.

Cyber Resilience Act and vulnerability handling

Classification as a product with digital elements, manufacturer status and exclusions are assessed against the product and distribution model. The main Cyber Resilience Act requirements apply from 11 December 2027, while the Regulation's reporting duties apply from 11 September 2026. Preparation covers classification, documentation, support period, coordinated handling and reporting channels without claiming conformity before applicable evidence and procedures exist.

A vulnerability is triaged, contained, remediated, verified and communicated according to risk, exploitation and duties. Exceptions have an owner, reason, compensating measure and expiry. Emergency fixes undergo subsequent review and do not replace root-cause analysis.

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 Andrea AI 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 2026-07-29. Applicability, role and any relevant commencement dates must be reassessed against the concrete facts.

- Regulation (EU) 2016/679 (GDPR)
- Directive (EU) 2022/2555 (NIS2)
- Italian Legislative Decree No. 138 of 4 September 2024 — NIS2 implementation
- Regulation (EU) 2024/2847 (Cyber Resilience Act)
- European Commission — Cyber Resilience Act implementation framework and dates, 27 July 2026