



Data Security and Data Privacy Policy

NUCIDA Group

English Version

NUCIDA Group

E: info@nucida.com
W: <https://nucida.com>

Companies / Unternehmen

NUCIDA LLC
NUCIDA Ltd.
NUCIDA Beratung GbR
NUCIDA Part. Ltd

Imprint / Impressum

<https://nucida.com/imprint.php>

NUCIDA DS DPP 2025-1

Date / Datum: 17.09.25
Version: 2025.1
Page / Seite: 1 / 11



1. Introduction

NUCIDA Group is a leading consulting firm specializing in software quality assurance, digital transformation, artificial intelligence (AI) integration, and software testing services. As part of our commitment to delivering high-quality, reliable services to our clients, we prioritize the protection of information assets, including personal data. This Data Security and Data Privacy Policy (the "Policy") outlines our approach to managing information security and data privacy in alignment with the ISO/IEC 27001:2022 standard for Information Security Management Systems (ISMS).

The Policy ensures that NUCIDA Group maintains confidentiality, integrity, and availability of information while respecting data privacy principles, including compliance with the General Data Protection Regulation (GDPR) and other applicable laws. By implementing this Policy, we mitigate risks associated with our operations in software testing, AI-driven solutions, and consulting services.

2. Scope

This Policy applies to all information assets owned, managed, or processed by NUCIDA Group, including:

- Digital data (e.g., client project files, test data, AI model outputs).
- Physical assets (e.g., servers, documents).
- Personnel, processes, and third-party relationships involved in our services.

It covers all employees, contractors, affiliates, and partners of NUCIDA Group, as well as all locations where our activities are conducted. The Policy encompasses the entire lifecycle of information, from collection to disposal.

3. References

- ISO/IEC 27001:2022 (Information Security Management Systems) Requirements.
- ISO/IEC 27002:2022 (Information Security, Cybersecurity and Privacy Protection) Information Security Controls.
- Regulation (EU) 2016/679 (GDPR) General Data Protection Regulation.
- Applicable national data protection laws.

4. Definitions

- **Information Security:** Preservation of confidentiality, integrity, and availability of information.
- **Personal Data:** Any information relating to an identified or identifiable natural person (as defined in GDPR).
- **ISMS:** Information Security Management System, as per ISO 27001.
- **Risk:** Effect of uncertainty on objectives, assessed in terms of likelihood and impact.



5. Policy Statements

5.1 Information Security Objectives

NUCIDA Group commits to:

- Establishing and maintaining an ISMS to systematically manage information security risks.
- Protecting information assets against unauthorized access, disclosure, alteration, or destruction.
- Ensuring business continuity and resilience in our software testing and AI services.
- Continuously improving security measures through regular audits and reviews.

These objectives align with ISO 27001 Clause 6.2, ensuring they are measurable, monitored, and communicated.

5.2 Data Privacy Principles

In processing personal data (e.g., client contact details, employee information), we adhere to:

- **Lawfulness, Fairness, and Transparency:** Data processing is based on consent, contract, or legitimate interest.
- **Purpose Limitation:** Data is collected only for specified, explicit, and legitimate purposes (e.g., project delivery, internal HR).
- **Data Minimization:** Only necessary data is processed.
- **Accuracy:** Data is kept up-to-date and accurate.
- **Storage Limitation:** Data is retained only as long as required.
- **Integrity and Confidentiality:** Secure processing to prevent unauthorized access.
- **Accountability:** We demonstrate compliance through records and audits.

These principles reflect GDPR Articles 5–10 and ISO 27001 controls in Annex A.18 (Compliance).

6. Responsibilities

- **Management Board:** Overall accountability for the ISMS, policy approval, and resource allocation.
- **Information Security Officer (ISO):** Leads ISMS implementation, risk assessments, and compliance monitoring.
- **Employees and Contractors:** Comply with this Policy, report incidents, and participate in training.
- **Data Protection Officer (DPO):** Oversees data privacy compliance, handles data subject requests, and liaises with supervisory authorities.
- **Third Parties:** Must adhere to equivalent security and privacy standards via contracts.

Roles are defined per ISO 27001 Clause 5.3 (Organizational Roles).



7. Risk Management

NUCIDA Group follows a risk-based approach as per ISO 27001 Clause 6.1:

- **Identification:** Regular identification of risks to information assets (e.g., cyber threats in AI testing, data breaches in client projects).
- **Assessment:** Evaluate risks based on likelihood and impact, using qualitative and quantitative methods.
- **Treatment:** Select and implement controls from ISO 27001 Annex A to mitigate risks (e.g., access controls, encryption).
- **Monitoring:** Ongoing review of risks through internal audits and management reviews.

A Statement of Applicability (SoA) documents selected controls.

8. Security Controls

We implement controls from ISO 27001 Annex A, tailored to our consulting operations:

- **Organizational Controls (A.5):** Policies for information security, including segregation of duties in test environments.
- **People Controls (A.6):** Screening, training, and disciplinary processes for personnel handling sensitive data.
- **Physical Controls (A.7):** Secure facilities for hardware and media protection.
- **Technological Controls (A.8):** Access control (e.g., multi-factor authentication for tools like TESTRAIL), cryptography for data in transit/rest, and secure development practices for AI solutions.
- **Operational Controls (A.5 in legacy, now integrated):** Incident management, backup procedures, and vulnerability management.

Specific to our services: Encryption for test data management and secure AI model training to prevent data leakage.

9. Data Privacy

9.1 Data Processing

Personal data is processed securely:

- Lawful bases are documented in Data Processing Agreements (DPAs) with clients.
- Data transfers outside the EU/EEA comply with adequacy decisions or Standard Contractual Clauses (SCCs).

9.2 Data Subject Rights

We facilitate rights under GDPR Article 15–22:

- Access, rectification, erasure, restriction, portability, and objection.



- Requests are handled within one month, free of charge unless excessive.

9.3 Data Breaches

Breaches are reported to the DPO and, if required, to supervisory authorities within 72 hours.

10. Incident Response

Per ISO 27001 A.5.24 (now integrated):

- **Detection and Reporting:** All incidents (e.g., unauthorized access to client test data) must be reported immediately to the ISO.
- **Response Plan:** Assess, contain, eradicate, recover, and review incidents.
- **Lessons Learned:** Post-incident reviews to improve the ISMS.

11. Training and Awareness

All personnel receive annual training on:

- Information security best practices.
- Data privacy obligations.
- Handling of sensitive information in software testing and AI contexts.

Training aligns with ISO 27001 Clause 7.2 (Competence) and A.6.3 (Information Security Awareness).

12. Monitoring and Review

- **Internal Audits:** Conducted annually to verify ISMS effectiveness (ISO 27001 Clause 9.2).
- **Management Review:** Biennial reviews by the Management Board.
- **Metrics:** Key performance indicators (KPIs) include incident rates, audit findings, and compliance scores.
- **Updates:** This Policy is reviewed annually or following significant changes (e.g., new AI tools).

13. Compliance and Enforcement

Non-compliance may result in disciplinary action. We commit to legal compliance and pursue ISO 27001 certification. Violations of data privacy laws will be reported as required.

For inquiries, contact:

- Information Security Officer: security@nucida.com
- Data Protection Officer: dpo@nucida.com



Datensicherheits- und Datenschutzrichtlinie

NUCIDA Group

Deutsche Version

NUCIDA Group

E: info@nucida.com
W: <https://nucida.com>

Companies / Unternehmen

NUCIDA LLC
NUCIDA Ltd.
NUCIDA Beratung GbR
NUCIDA Part. Ltd

Imprint / Impressum

<https://nucida.com/imprint.php>

NUCIDA DS DPP 2025-1

Date / Datum: 17.09.25
Version: 2025.1
Page / Seite: 6 / 11



1. Einleitung

Die NUCIDA Group ist ein führendes Beratungsunternehmen, das sich auf Software-Qualitätssicherung, digitale Transformation, Integration künstlicher Intelligenz (KI) und Software-Testing-Dienste spezialisiert hat. Im Rahmen unseres Engagements für die Bereitstellung hochwertiger, zuverlässiger Dienstleistungen für unsere Kunden legen wir höchsten Wert auf den Schutz von Informationsassets, einschließlich personenbezogener Daten. Diese Datensicherheits- und Datenschutzrichtlinie (die „Richtlinie“) beschreibt unseren Ansatz zur Verwaltung der Informationssicherheit und des Datenschutzes in Übereinstimmung mit der ISO/IEC 27001:2022-Norm für Informationssicherheits-Managementsysteme (ISMS).

Die Richtlinie stellt sicher, dass die NUCIDA Group die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen aufrechterhält und Datenschutzprinzipien respektiert, einschließlich der Einhaltung der Datenschutz-Grundverordnung (DSGVO) und anderer geltender Gesetze. Durch die Umsetzung dieser Richtlinie mildern wir Risiken im Zusammenhang mit unseren Aktivitäten im Bereich Software-Testing, KI-gestützter Lösungen und Beratungsdienste ab.

2. Geltungsbereich

Diese Richtlinie gilt für alle von der NUCIDA Group besessenen, verwalteten oder verarbeiteten Informationsassets, einschließlich:

- Digitaler Daten (z. B. Kundenprojekt-Dateien, Testdaten, KI-Modell-Ausgaben).
- Physischer Assets (z. B. Server, Dokumente).
- Personal, Prozesse und Drittanbieter-Beziehungen, die in unseren Dienstleistungen involviert sind.

Sie umfasst alle Mitarbeiter, Auftragnehmer, Affiliates und Partner der NUCIDA Group sowie alle Standorte, an denen unsere Aktivitäten durchgeführt werden. Die Richtlinie deckt den gesamten Lebenszyklus der Information ab, von der Sammlung bis zur Vernichtung.

3. Referenzen

- ISO/IEC 27001:2022 – Informationssicherheits-Managementsysteme – Anforderungen.
- ISO/IEC 27002:2022 – Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitskontrollen.
- Verordnung (EU) 2016/679 (DSGVO) – Datenschutz-Grundverordnung.
- Geltende nationale Datenschutzgesetze (z. B. Bundesdatenschutzgesetz – BDSG).



4. Definitionen

- **Informationssicherheit:** Erhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.
- **Personenbezogene Daten:** Jede Information, die sich auf eine identifizierte oder identifizierbare natürliche Person bezieht (wie in der DSGVO definiert).
- **ISMS:** Informationssicherheits-Managementsystem gemäß ISO 27001.
- **Risiko:** Auswirkung der Unsicherheit auf Ziele, bewertet hinsichtlich Wahrscheinlichkeit und Auswirkung.

5. Richtlinienenerklärungen

5.1 Ziele der Informationssicherheit

Die NUCIDA Group verpflichtet sich zu:

- Etablierung und Aufrechterhaltung eines ISMS zur systematischen Bewältigung von Informationssicherheitsrisiken.
- Schutz von Informationsassets vor unbefugtem Zugriff, Offenlegung, Änderung oder Zerstörung.
- Sicherstellung der Geschäftskontinuität und Resilienz in unseren Software-Testing- und KI-Diensten.
- Kontinuierlicher Verbesserung der Sicherheitsmaßnahmen durch regelmäßige Audits und Überprüfungen.

Diese Ziele entsprechen der ISO 27001 Klausel 6.2 und stellen sicher, dass sie messbar, überwacht und kommuniziert werden.

5.2 Datenschutzprinzipien

Bei der Verarbeitung personenbezogener Daten (z. B. Kundenkontaktinformationen, Mitarbeiterdaten) halten wir uns an:

- **Rechtmäßigkeit, Fairness und Transparenz:** Die Datenverarbeitung basiert auf Einwilligung, Vertrag oder berechtigtem Interesse.
- **Zweckbindung:** Daten werden nur für festgelegte, explizite und legitime Zwecke erhoben (z. B. Projektabwicklung, interne Personalabteilung).
- **Datensparsamkeit:** Nur notwendige Daten werden verarbeitet.
- **Genauigkeit:** Daten werden aktuell und korrekt gehalten.
- **Speicherbegrenzung:** Daten werden nur so lange aufbewahrt, wie erforderlich.
- **Integrität und Vertraulichkeit:** Sichere Verarbeitung zur Verhinderung unbefugten Zugriffs.
- **Rechenschaftspflicht:** Wir weisen die Einhaltung durch Aufzeichnungen und Audits nach.

Diese Prinzipien spiegeln die DSGVO-Artikel 5–10 und die ISO 27001-Kontrollen in Anhang A.18 (Einhaltung) wider.



6. Verantwortlichkeiten

- **Vorstand:** Gesamte Verantwortung für das ISMS, Richtlinienfreigabe und Ressourcenbereitstellung.
- **Informationssicherheitsbeauftragter (ISO):** Leitet die ISMS-Umsetzung, Risikobewertungen und Compliance-Überwachung.
- **Mitarbeiter und Auftragnehmer:** Einhaltung dieser Richtlinie, Meldung von Vorfällen und Teilnahme an Schulungen.
- **Datenschutzbeauftragter (DSB):** Überwacht die Datenschutzkonformität, bearbeitet Anfragen betroffener Personen und koordiniert mit Aufsichtsbehörden.
- **Drittanbieter:** Müssen äquivalente Sicherheits- und Datenschutzstandards durch Verträge einhalten.

Rollen sind gemäß ISO 27001 Klausel 5.3 (Organisatorische Rollen) definiert.

7. Risikomanagement

Die NUCIDA Group folgt einem risikobasierten Ansatz gemäß ISO 27001 Klausel 6.1:

- **Identifikation:** Regelmäßige Identifikation von Risiken für Informationsassets (z. B. Cyberbedrohungen im KI-Testing, Datendiebstähle in Kundenprojekten).
- **Bewertung:** Bewertung von Risiken basierend auf Wahrscheinlichkeit und Auswirkung unter Verwendung qualitativer und quantitativer Methoden.
- **Behandlung:** Auswahl und Umsetzung von Kontrollen aus dem ISO 27001 Anhang A zur Risikominderung (z. B. Zugriffssteuerung, Verschlüsselung).
- **Überwachung:** Laufende Überprüfung von Risiken durch interne Audits und Managementüberprüfungen.

Eine Anwendbarkeitserklärung (SoA) dokumentiert ausgewählte Kontrollen.

8. Sicherheitskontrollen

Wir setzen Kontrollen aus dem ISO 27001 Anhang A um, angepasst an unsere Beratungsaktivitäten:

- **Organisatorische Kontrollen (A.5):** Richtlinien für Informationssicherheit, einschließlich Trennung von Pflichten in Testumgebungen.
- **Personalbezogene Kontrollen (A.6):** Überprüfung, Schulung und disziplinarische Prozesse für Personen, die sensible Daten handhaben.
- **Physische Kontrollen (A.7):** Sichere Einrichtungen für den Schutz von Hardware und Medien.
- **Technologische Kontrollen (A.8):** Zugriffssteuerung (z. B. Multifaktorauthentifizierung für Tools und Anwendungen), Kryptographie für Daten im Transit/Ruhe und sichere Entwicklungspraktiken für KI-Lösungen.
- **Betriebliche Kontrollen (A.5 in der Legacy, nun integriert):** Vorfallmanagement, Backup-Verfahren und Schwachstellenmanagement.



Spezifisch für unsere Dienste: Verschlüsselung für Testdatenmanagement und sichere KI-Modelltrainings zur Verhinderung von Datenlecks.

9. Datenschutz

9.1 Datenverarbeitung

Personenbezogene Daten werden sicher verarbeitet:

- Rechtliche Grundlagen werden in Auftragsverarbeitungsverträgen (AVV) mit Kunden dokumentiert.
- Datenübermittlungen außerhalb der EU/EWR entsprechen Angemessenheitsbescheiden oder Standardvertragsklauseln (SVK).

9.2 Rechte der Betroffenen

Wir erleichtern Rechte gemäß DSGVO Artikel 15–22:

- Auskunft, Berichtigung, Löschung, Einschränkung, Übertragbarkeit und Widerspruch.
- Anfragen werden innerhalb eines Monats, kostenlos, es sei denn, sie sind übermäßig, bearbeitet.

9.3 Datenschutzverletzungen

Verletzungen, welche dem DPO gemeldet werden, werden den zuständigen Aufsichtsbehörden innerhalb von 72 Stunden gemeldet, wenn gemäß der gesetzlichen Vorgaben erforderlich.

10. Reaktion auf Vorfälle

Gemäß ISO 27001 A.5.24 (nun integriert):

- **Erkennung und Meldung:** Alle Vorfälle (z. B. unbefugter Zugriff auf Kundentestdaten) müssen sofort dem ISO gemeldet werden.
- **Reaktionsplan:** Bewerten, Eindämmen, Beseitigen, Wiederherstellen und Überprüfen von Vorfällen.
- **Lernprozesse:** Nach-Vorfall-Überprüfungen zur Verbesserung des ISMS.

11. Schulung und Sensibilisierung

Alles Personal erhält jährliche Schulungen zu:

- Best Practices der Informationssicherheit.
- Datenschutzpflichten.
- Handhabung sensibler Informationen im Kontext von Software-Testing und KI.

Schulungen entsprechen der ISO 27001 Klausel 7.2 (Kompetenz) und A.6.3 (Bewusstsein für Informationssicherheit).



12. Überwachung und Überprüfung

- **Interne Audits:** Jährlich durchgeführt, um die Wirksamkeit des ISMS zu überprüfen (ISO 27001 Klausel 9.2).
- **Managementüberprüfung:** Zweijährlich durch den Vorstand.
- **Kennzahlen:** Wichtige Leistungsindikatoren (KPIs) umfassen Vorfalldaten, Audit-Befunde und Konformitätswerte.
- **Aktualisierungen:** Diese Richtlinie wird jährlich oder nach wesentlichen Änderungen (z. B. neue KI-Tools) überprüft.

13. Einhaltung und Durchsetzung

Nicht-Einhaltung kann zu disziplinarischen Maßnahmen führen. Wir verpflichten uns zur gesetzlichen Einhaltung und streben die ISO 27001-Zertifizierung an. Verstöße gegen Datenschutzgesetze werden wie erforderlich gemeldet.

Für Anfragen kontaktieren Sie:

- Informationssicherheitsbeauftragter: security@nucida.com
- Datenschutzbeauftragter: dpo@nucida.com