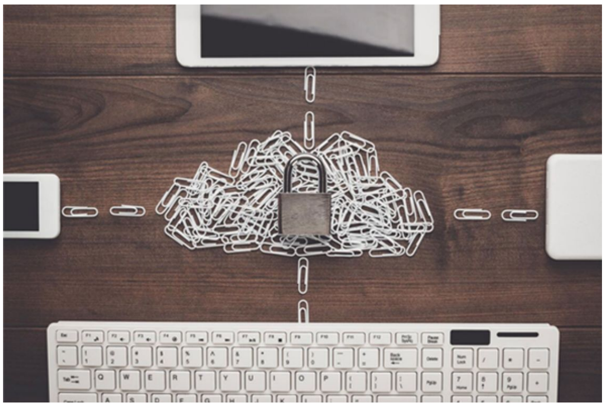
Security Policy

“We’ve got you secured”

At Nucleoo, we understand the importance of managing your valuable data assets securely.

In this document, we outline the Nucleoo data platform security details. Data security, availability and privacy are key features when delivering data solutions either in the cloud or on-premise. In addition to the existing foundation of industry standard technologies and leading cloud players (Azure and AWS), Nucleoo wields its own safeguards and custom configuration to strengthen existing security features.



Encryption at rest

All our data - SQL structured, No-SQL and big data in Data Lakes - is encrypted at rest using AES256 (ISO/IEC 18033 Information technology – Security techniques – Encryption algorithms [1] certified).

Encryption in transit

Information in transit is encrypted in transit using SSL SHA-256 with RSA-2048 encrypted certificates (FIPS PUB 180-4, CRYPTREC, NESSIE certified algorithm [2]).

All information that is transferred between the infrastructure components and not strictly needed from outside is also isolated in private subnetworks, that are non-accessible from the public internet.

JWT encryption

JWT tokens are encrypted with a unique and periodically rotated salt, using HS256, as recommended by ISO/IEC 27001:2017 [3] standard for tokenisation.

ISO

Nucleoo and its team is ISO/IEC 27001:2017 [3] certified. This certification specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. Every 6 months, audits are conducted to control the implementation and continuous improvement of the security measures in place.

Data isolation and key vaults

All client stored information is stored under separate logic containers and subcontainers within the cloud architecture. These containers are only accessible by the client sub-infrastructure, providing a set of key vaults, also isolated, which secure the credentials. This configuration grants data access protection, complete logical isolation and ensures the integrity of data.

PEN tests

Penetration (PEN) tests are periodically (every 6 months) executed against the Nucleoo infrastructure, to ensure existing and new threats are tested against the platform.

The PEN tool is Tenable Nessus [4], one of the most reliable penetration tools in the market, providing the lowest false positive rate with six-sigma accuracy and the deepest and broadest vulnerability coverage in the industry.

Findings are internally patched and publicly disclosed in the next release notes of the platform, to ensure transparency and traceability of patched vulnerabilities.

[1] https://www.iso.org/standard/76156.html
[2] https://en.wikipedia.org/wiki/SHA-2
[3] https://www.iso.org/standard/54534.html
[4] https://www.tenable.com/products/nessus