



General Information Security Policy

Antwerp, 16 May 2025

Information Security: General Guidelines

We protect the company's informational and IT assets (including but not limited to computers, mobile devices, networking equipment, software, and sensitive data) against internal, external, intentional, or accidental threats. We aim to mitigate risks associated with theft, loss, misuse, damage, or abuse of these systems.

Confidentiality, Integrity & Availability

- Confidentiality: Information is protected from unauthorized disclosure. Users will only have access to resources they are specifically authorized to use. Access rights are strictly controlled and reviewed regularly.
- Integrity: Information is safeguarded from unauthorized modification.
- Availability: Authorized users must be able to access information when needed to support business processes.

Legal Compliance & Business Continuity

We comply with, and where possible exceed, national legal and regulatory requirements, industry standards and best practices.

Business continuity plans are developed, maintained and tested regularly to ensure we remain operational under all circumstances.

Awareness & Reporting

Security awareness training is provided to all employees. Responsibilities are embedded in job descriptions, and compliance with security policies is expected as part of our culture.

No action will be taken against any employee who raises an information security concern either by reporting it or by contacting the Information Security Management Leader unless it clearly involves illegal activity, gross negligence, or repeated, wilful misconduct.

All actual or suspected information security breaches must be reported to IT.helpdesk@aprojects.com or via the form linked in POL_APS_017_V01 Incident Management, Appendix A.

Enforcement, Exceptions and Complaints

Non-conformance to policy and standard statements in this Policy could result in disciplinary action including, but not limited to, informal or formal warnings, up to termination of contract. Any exceptions to what is governed will require written authorization by email from the Information Security Management Leader. Exceptions granted will be issued a policy waiver for a defined period of time.

All target users of this Policy can submit complaints about its contents to the Information Security Management Leader at any point. All complaints will be filed and processed accordingly where the Information Security Management Leader will respond within 14 days of initial submission. Requests for exceptions to this Policy as well as complaint submissions will be addressed to the Information Security Management Leader at IT.helpdesk@aprojects.com.