

Information Security Policy

At New Alternative Path Ltd, we recognize that protecting the confidentiality, integrity, and availability of information is critical to maintaining trust with our students, partners, and stakeholders. This policy sets out our commitment to safeguarding all personal, academic, and organizational information against unauthorized access, disclosure, alteration, and loss.

Scope

This policy applies to all employees, consultants, contractors, systems, processes, and third parties that handle or have access to information owned or managed by the consultancy.

The policy covers student application and enrolment information, identity and financial records, staff information, partner agreements and business records, in electronic, paper or verbal form. It applies to office and remote work within the documented ISMS scope.

Objectives

1. Confidentiality – Ensure that sensitive information (e.g., student records, financial data, institutional agreements) is only accessible to authorized individuals.
2. Integrity – Protect information from unauthorized modification to guarantee accuracy and reliability.
3. Availability – Ensure that critical information and systems are available to authorized users whenever needed.

These principles provide the framework for measurable information security objectives.

Management sets responsibilities, measures, targets and review arrangements in the ISMS objectives register. Progress is monitored and evaluated through management review, using the relevant operational records.

Policy Commitments

1. Applicable Requirements and Data Protection – New Alternative Path Ltd commits to satisfying all applicable legal, statutory, regulatory, contractual and other information security requirements, including requirements for protecting personal information. Relevant obligations are maintained in the legal register and reflected in policies and operating procedures.



2. Access Control – Access to information and systems will be restricted based on roles and responsibilities, using strong authentication and authorization mechanisms.
3. Secure Communication – Confidential data will be transmitted through secure, encrypted channels.
4. Incident Management – Any information security incident (e.g., data breach, unauthorized access) will be promptly reported, investigated, and resolved to minimize impact.
5. Awareness & Training – All staff and contractors will receive regular training on information security best practices and their responsibilities.
6. Third-Party Security – Partners and service providers handling sensitive data must adhere to equivalent security standards.
7. Monitoring & Review – Security controls, risks, and policies will be regularly reviewed and updated to address evolving threats.

Risk Management – Information security risks are assessed using the approved methodology and confidentiality, integrity and availability criteria in the QMS and ISMS risk register. Risk owners approve treatment plans and accept residual risks within their assigned authority. Necessary controls, applicability decisions and implementation status are documented in the Statement of Applicability. Assessments are reviewed at planned intervals and following significant changes.

8. Business Continuity – Measures will be in place to ensure the continued operation of critical services in the event of system failures or disasters.

Continual Improvement – New Alternative Path Ltd is committed to continually improving the suitability, adequacy and effectiveness of its information security management system through monitoring, internal audits, management reviews, incident learning and corrective actions.

Responsibility

- Gotse Gyorshevski, Managing Director, approves this policy, provides direction and resources, and retains overall accountability for information security. Managers implement the policy within their areas of responsibility.
- Employees and contractors are responsible for adhering to security practices and reporting incidents.



NEW ALTERNATIVE PATH
YOUR STEPPING STONE TO SUCCESS

✉ office@newalternative.co.uk ☎ 07365 22517 🌐 <https://newalternative.co.uk/>

- The assigned IT personnel and managers coordinate risk management, maintain the ISMS and report its performance to the Managing Director, in line with the Information Security Roles and Responsibilities document and the SoA. Naveena Dhera maintains the controlled policy and its revision record.

Communication and Availability

This policy is communicated to all relevant personnel through induction, security awareness activities and notification of changes. Relevant personnel acknowledge the policy and their responsibilities. The controlled version is available in the approved document repository. It is made available to relevant interested parties, including suppliers and partners, as appropriate to their relationship with NAP and subject to information-access requirements.

Policy Review

This policy is reviewed at least annually and when significant changes occur in the organisation, risks, services, technology, applicable requirements or security incidents. Management reviews and approves revisions; superseded versions are retained under document-control arrangements.

Authorised By: Gotse Gyorshevski- Managing Director