Reference	247 POL 29
Version	1.0
Issue Date	18/01/2022
Approved	MD
Review Date	05/01/2027

247 ALLIANCE LTD

INFORMATION SECURITY POLICY

INTRODUCTION:

This information security policy outlines 247 ALLIANCE's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the 247 ALLIANCE's information systems. Supporting policies, codes of practice, procedures and guidelines provide further details.

247 ALLIANCE is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity, and availability of its data. The principles defined in this policy will be applied to all the physical and electronic information assets for which the 247 ALLIANCE is responsible.

POLICY

- The policy's goal is to protect the organisation's information assets against all Internal, External, deliberate, or accidental threats including Interested Parties as identified within the Context of the Organisation & the Risk Assessment.
- Management have approved this Information Security Policy & shall strive to continually improve the ISMS.
- The Information Security Policy has been reviewed to incorporate the General Data Protection Act and has updated its associated objectives in accordance with GDPR legislation:

Information will be protected against **unauthorised access.**

Confidentiality of information is processed in the manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures ('integrity and confidentiality') in line with the GDPR.

Integrity of information will be maintained.

Availability of information for business processes will be maintained and allocated on a need-to-know basis;

Legislative and regulatory requirements within the guidelines of the GDPR are met.
Business continuity plans will be developed, maintained, and tested.
Information security training will be given to all new and existing employees,
BREACH NOTIFICATIONS The company recognises our obligation and duty to report data breaches in certain instances. All staff have been made aware of the Company's responsibilities and we have developed strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without delay.

- **All actual or suspected information security breaches** All data breaches will be investigated, even in instances where notifications and reporting are not required, and we retain a full record of all data breaches to ensure that gap and pattern analysis are available and used. Where a system or process failure has given rise to a data breach, revision to any such process is recorded in the Change Management and Document Control records. Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the employee (s) held.
- Procedures exist to support this policy, including virus control measures, passwords, continuity plans and effective risk management.
- Business requirements for availability of information systems will be met.
- The Managing Director is responsible for maintaining the policy and providing support and advice during its implementation.
- All managers are directly responsible for implementing this policy and ensuring staff compliance in the respective departments.
- Compliance with contractual security obligations is mandatory.
- Compliance with the Information Security Policy is mandatory.

Malik Mustafa
Director
05/01/2026

Signed 

Review Date: 05/01/2027