

Reference	247 POL 47
Version	1.0
Issue Date	19/01/2024
Approved	MD
Review Date	05/01/2027

# 247 Alliance Ltd

## Cyber Security Policy

---

### Purpose

The purpose of this policy is to protect 247 Alliance Ltd's information systems, digital assets, and sensitive data from cyber threats, unauthorized access, loss, or damage, while ensuring business continuity and compliance with regulatory and contractual obligations.

### Scope

This policy applies to all employees, contractors, and temporary staff, and covers all IT systems, networks, devices, and data owned, leased, or managed by 247 Alliance Ltd.

### Policy Statement

247 Alliance Ltd is committed to maintaining the confidentiality, integrity, and availability of its information assets. Cyber Security risks will be managed through preventative controls, staff awareness, secure system management, and continuous monitoring.

### Governance and Responsibilities

Senior Management is responsible for approving this policy and ensuring that adequate resources are allocated. Employees and contractors must comply with this policy and report incidents immediately.

### Risk Management

Cyber risks are identified, assessed, and recorded in the company risk register and reviewed regularly.

### Access Control

Access is granted on a least-privilege basis. Strong passwords and MFA are used where possible.

### Device and Network Security

Company devices must be protected, encrypted where possible, and maintained with up-to-date security software.

### Data Protection

All data must be handled in line with GDPR and the company's data protection policies.

### Email and Internet Use

Users must remain vigilant against phishing and malicious activity.

### Incident Management

Cyber incidents must be reported immediately and investigated.

Reference	247 POL 47
Version	1.0
Issue Date	19/01/2024
Approved	MD
Review Date	05/01/2027

# 247 Alliance Ltd

## Cyber Security Policy

---

### **Backup and Business Continuity**

Critical data is backed up regularly and securely.

### **Training and Awareness**

Cyber Security training is provided and recorded.

### **Monitoring and Review**

Compliance is monitored through audits and management review.

### **Disciplinary Action**

Failure to comply may result in disciplinary action.

### **Policy Review**

This policy is reviewed annually or following a significant change.

**Malik Mustafa**

Director

05/01/2026

Signed:



**Review Date:** 05/01/2027