# INFORMATION SECURITY POLICY STATEMENT

Information is an important business asset of significant value to the company and needs to be protected from threats that could potentially disrupt business continuity. Our Management Team bears the responsibility for establishing and maintaining the Information Security Management System and ensures its integrity is maintained through instruction and training of our personnel so that each employee understands what is required of them.

**The purpose** of the Information Security Policy POL-006 is to protect the company's information assets from all threats, whether internal or external, deliberate or accidental.

**The policy scope** covers physical security and encompasses all forms of Information Security such as data stored on computers, transmitted across networks, printed or written documents and data physically stored on static and mobile devices.

All managers are **directly responsible** for implementing the Policy within their business areas and for adherence by their staff.

It is the responsibility of **each** employee to adhere to the policy. Disciplinary processes will be applicable in those instances where staff fail to abide by this security policy.

**THE COMPANY WILL ENSURE THAT:**

- Information is **protected against unauthorised access**
- **Confidentiality** of information is assured
- **Integrity** of information is maintained
- **Regulatory**and **legislative** requirements regarding intellectual property rights, data protection and privacy of personal information are met
- **Business Continuity plans** will be produced, maintained and tested
- Staff receive sufficient **Information Security training**
- **All breaches of information security**, actual or suspected are reported and investigated by the **Data Protection Team.**

Our Organisation has a Policy of Continuous Improvement and Objective setting in line with the ISO 27001:2013 International Standard.

*Signed*: _____ *Date: 31/08/2021*

*Title: Executive Chair*