

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. This policy has been written to provide a mechanism to establish procedures to protect against security threats and minimise the impact of security incidents.

The Chief Executive has approved the Information Security Policy

The purpose of this Policy 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 on paper, stored on tapes and diskettes or spoken in conversation or over the telephone.

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.

IT IS THE POLICY OF THE COMPANY TO ENSURE THAT:

Information will be **protected against unauthorised access**

Confidentiality of information is assured.

Integrity of information is maintained.

Regularity 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 **Security Policy Review Team**.

Signed: _____

Title: _____ *Date:* _____