INFORMATION SECURITY POLICY

Information is an important business asset of significant value to **SYNETIQ Limited** and needs to be protected from threats. This policy has been written to provide a mechanism to establish procedures to protect against threats and minimise the impact of any incidents.

The Managing Director has approved the Information Security Policy

The purpose of this Policy is to protect **SYNETIQ Limited's** information assets from all threats, whether internal or external, deliberate or accidental. The Policy Scope covers 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 and also encompasses Physical Security

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 SYNETIQ LIMITED TO ENSURE THAT:

Information will be **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.

Richard Martin - M.D.  16st July 2021