APPLICATION CONTROL POLICY

POLICY STATEMENT

We are committed to ensuring, so far as is reasonably practicable, the protection and security of company and client data stored on electronic data processing and storage systems owned and used by the company. This extends to ensuring that application control is implemented on all workstations and servers to restrict the execution of executables to an approved set.

AIMS AND OBJECTIVES

In recognising the importance of preventing unauthorised access to company systems, we will implement application control and security measures to prevent attacks on applications by mitigating risks due to application vulnerabilities and security issues.

We will ensure that applications are assessed regularly, and carry out application security assessments to identify, monitor and prioritise any security-related issues in a timely manner based on severity.

RESPONSIBILITIES

Management of the company are responsible for the development and implementation of application control and security measures to achieve the selected maturity level for each mitigation strategyin line with the Australian Cyber Security Centre (ACSC) Essential Eight and associated maturity levels.

All users of company systems must adhere to all mitigation strategies to the maturity level prescribed by management for the particular strategy, and to not act in any way which may result in application vulnerabilities or application security issues.

IMPLEMENTATION

Mitigation strategies to prevent malware delivery and execution will be based on the ACSC Essential Eight prioritised mitigation strategies including application control; patching, updating or mitigating security vulnerabilities; configuring macro settings in applications such as Microsoft Office; and application hardening.

We will aim for a minimum Maturity Level of at least Two for each mitigation strategy while working towards a desired Maturity Level Three unless a higher level is required by the ACSC.

AUTHORISED BY

Signed: _____   Date: _____