Information Security Policy Statement

Nacro, its clients and stakeholders expect its information systems to meet high industry-wide standards of **confidentiality**, **availability** and **integrity**. These standards can only be achieved by ensuring that we have a practical and pro-active system for managing our information security.

The purpose of the Information Security Policy is to protect Nacro, its employees and clients from all information security threats, whether internal or external, deliberate or accidental.

The Information Security Policy is characterised here as meeting the following criteria:

- **Confidentiality** - ensuring that information is accessible only to those authorised to have access.
- **Integrity** - safeguarding the accuracy and completeness of information and processing methods.
- **Availability** - ensuring that authorised users have access to information and associated assets when required.
- **Regulatory** - ensuring that Nacro meets its regulatory and legislative requirements.

Nacro has nominated a Security Manager to introduce and maintain policy and to provide advice and guidance in its implementation.

Nacro requires that all breaches of information security, actual or suspected, are reported to and investigated by the Security Manager, email: ictservicedesk@nacro.org.uk.

Nacro undertakes to provide appropriate information security training for all employees.

Third parties providing services to Nacro are required to ensure that the **confidentiality**, **integrity**, **availability**, and **regulatory** requirements of all business systems are met.

It is the responsibility of all users to adhere to the policy.

Signed:

Print name: Jacob Tas.

Position: CEO

Date: May 2014

Next review date: May 2015

Reference: NAC567