Information Security – nGAGE Security Policy

nGAGE is committed to maintaining and improving information security within the Company and minimising its exposure to risks. This information security policy sets out the organization's approach to managing information security.

- The confidentiality of corporate and client information shall be assured
- Sensitive information of all types including electronic, hard copy paper, verbal Shall be securely stored and protected against unauthorized access with full automated audit trail for recording system security events and the recording of access modification or deletion of confidential, sensitive or client files.
- The integrity of information shall be maintained
- Information shall be made available to authorized employees when required
- All access to information will be controlled and follow the access control policy
- Where required, regulatory and legislative requirements shall be met
- Business continuity plans for critical activities shall be tested and maintained.
- Information security policy shall be available and acknowledged by all staff.
- All breaches of information security, actual or suspected, shall be reported and investigated through the incident management procedure
- Any breaches of data will be recorded internally with full root cause analysis performed. Any breach of data that contains client data will follow the contractual requirements of the client and be reported to the client immediately the breach is discovered. All staff will report any data breach to their line manager who will follow the data breach policy and pass all details to the data protection officer to report to the ICO (if applicable).
- nGAGE's Information Security Management System shall be continually measured and improved, as per the NMPI Information Security Policy Continual Improvement and Audit Policy.
- Network security will be applied to firewalls and network intrusion solutions will be implemented to detect intrusion and prevent intrusion of the network. All network systems used that store or process sensitive data will be adequately protected including information that may be accessible from the internet of other public network
- All data backup services used will be ISO 27001 and 27001 Cloud certified. The data centre will be audited at least annually led by our Internal Audit Team
- Any confidential or sensitive information in electronic format shall not be stored on unencrypted flash drives, CDs, DVDs, or portable media devices.
- All Laptops, and portable media types (including phones and hand held devices / tablets) must be encrypted
- All client files shall be deleted or sanitized at the end of the contract or follow the contractual requirement of the client
- It is company policy to ensure we comply with any regulatory, legal or contractual obligation

The information security policy is approved by the Group CIO and is communicated to all staff and employees of the organisation, contractual third parties and agents of the organisation

I fully endorse the Information Security Policy signed by Tim Styles the CIO and sponsor of the ISMS.