# ANS Security Policy Statement

At ANS we aspire to be the UK's leading Cloud Service Provider of choice. We aim to ensure that the services we provide embed excellence into both our and our customer's business, whilst maximising the Return on Investment and creating business opportunities. We are recognised as being a trustworthy, open, honest, and ethical organisation.

We recognise that our business, and that of our customers, is heavily reliant on its information and any technology used to store and process that information. This is why we take very seriously the confidentiality and integrity of this information to ensure that it is only accessible by those who are authorised and remains complete and accurate at all times. We also make sure that the availability of this information is guaranteed according to agreed service levels and contractual agreements through our resiliency and Business Continuity practices. Information is always managed in a way that meets all of our legal, regulatory and contractual obligations.

To embed these principles into our business, ANS has implemented an Information Security Management System (ISMS) that has been verified by our external accreditor to be compliant with the international standard for Information Security Management, ISO/IEC 27001. This system is a security policy framework that is supported by detailed policies and procedures, and underpinned by the pragmatic application of industry best practice.

We use this Security Policy Framework to develop a Protective Security environment, focusing on the Physical, Personnel and Information assets of our business, as well as those informational assets we hold and process on behalf of our Customers.

ANS use a practical risk based approach within our protective security environment, ensuring that protection is applied via our risk management programme in line with business requirements and goals. And while we accept a degree of risk within our business culture, we never jeopardise the integrity of our customer's information.

This policy is applied right across ANS, and is reviewed at least annually and whenever the business undergoes significant change. The ANS Executive is ultimately responsible for all company policies, and ensures that the security policy framework is regularly reviewed and that it continues to evolve and improve, and conform to the standard required by our external accreditor.

The ANS Executive has a high expectation for this policy and supporting framework to be put into practice by all ANS employees and adopted by our strategic business partners. We regard protective security as being everybody's responsibility to ensure it is embedded into our daily business lives. All of our staff are empowered to take on this responsibility from the day they join ANS via induction training, and it is regularly enforced through a continuous programme of security awareness.

To that end the ANS Executive expects conformance to the policy and the supporting framework, will use the disciplinary process to drive home the importance of this to our staff, and are prepared to use legal and contractual remedies with our business partners.

"The security of your data is our number one priority. During a time when cyber-attacks are on the rise, it has never been more important to ensure the confidentiality, integrity and availability of your business-critical data. ANS' security controls are based on ISO/IEC standards that document internationally-accepted best practice. Along with my colleagues on the senior management team, I fully endorse this information security policy and expect the controls to be implemented consistently throughout ANS."

Paul Shannon, Chief Executive Officer