



# 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. 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 auditor to be compliant with the international standard for Information Security Management, ISO/IEC 27001. ANS are also certified compliant to the ISO 27017 & 27018 Cloud Security standards; adding further rigour to our cloud security stance. 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.

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. 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, improve, and conform to the standard required by our external accreditor.

ANS is committed to continual improvement; objectives are managed within both a directed and a 'ground-up' framework. Top level objectives are agreed with senior management and are based around multiple inputs and outputs e.g. new objectives derived from audit and assessment, new business need or risk assessment.

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.

"The security of your data is our number one priority. As the number of cyber-attacks increases every day, we ensure the confidentiality, integrity and availability of your business-critical data. ANS security controls are closely aligned to ISO/IEC standards that are internationally recognised as best practice. Along with my colleagues on the Senior Management Team, I fully endorse our Information Security Policy and expect the controls to be implemented consistently throughout ANS."

A handwritten signature in black ink, appearing to read 'Chris Hodgson', written in a cursive style.

Chris Hodgson, Chief Operating Officer