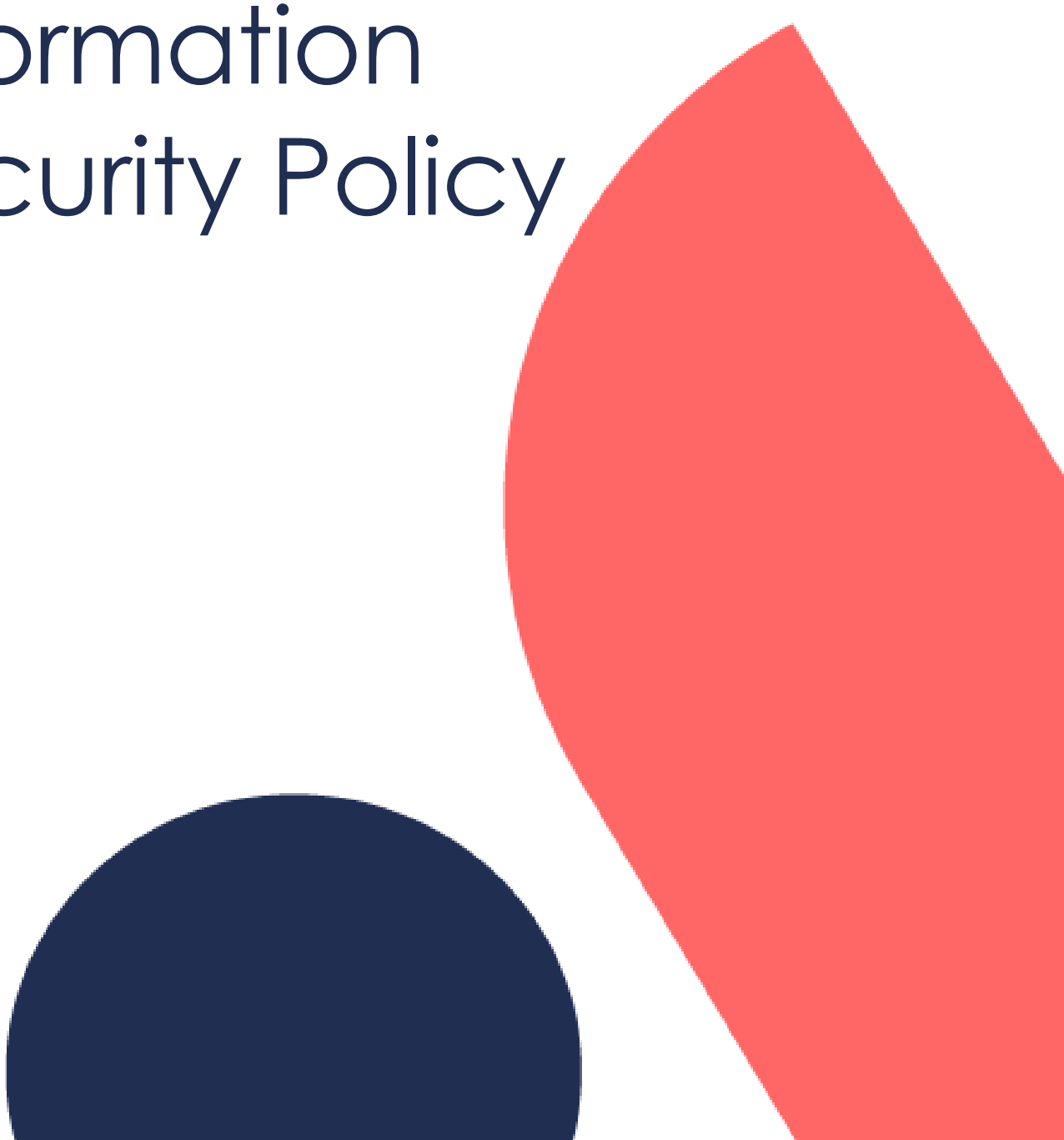
Information Security Policy



Contents

1. Policy Statement

ANS and its subsidiary companies are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout ANS in order to preserve competitive edge, cash-flow, profitability, legal, regulatory, contractual, compliance and commercial image.

2. Purpose

The purpose of this document is to set out ANS's and its subsidiary companies aims and a framework for setting objectives for the management of information security through the organization including cloud solutions. Clear Information and information security requirements will continue to be aligned with ANS objectives and ISMS.

3. Scope

The Information Security Policy applies to all information assets owned by ANS or which are on any networks or Cloud Services managed fully by ANS. The guidelines in the Information Security Policy, apply to all information which ANS processes, irrespective of ownership or form. All employees of ANS and certain external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy. All staff, and certain external parties, will receive and/or be required to provide appropriate training.

The ISMS is subject to continuous, systematic review and improvement.

4. Framework

ANS's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and the maintenance of the ISMS.

The risk assessment, Statement of Applicability and risk treatment plan identify how information-related risks are controlled in relation to ISO 27001 and ISO 27017/27018.

The Compliance Team is responsible for the management and maintenance of the risk treatment plan and the responsibility of creating and distributing security policies and procedures.

5. Data Protection

The issue of data protection is at the forefront of ANS's objectives for the future, especially in relation to UK GDPR and where applicable, GDPR. For this reason, ANS has enhanced its ISMS to comply with the ISO 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) to help satisfy the legal requirement of abiding by the regulation.

Control objectives for each of these areas are supported by specific, documented policies and procedures. Where cloud platforms are provisioned to clients and ANS is acting as data processor, contractual agreements will clearly define the responsibilities between ANS and the client.

ANS will never share client data in respect of which it is data processor with any third parties and will not utilise sub-contractors to access client data within your solution unless you expressly grant such access. ANS hold client data within client solutions and should their solution no longer be functioning then it is kept for 30 days following the termination of contract before it is destroyed.

In the case of Professional and/or Managed Services delivered with the support of our Indian subsidiary Preact Consulting Services Private Limited, where provided under your contract terms or where you have consented, if a transfer of your personal information is required to perform our Professional and/or Managed Services, for example your name and contact information contained within support tickets, ANS will comply with all legal obligations in relation to your personal data, including having a lawful basis for transferring personal data and putting appropriate safeguards in place to ensure an adequate level of protection for the personal data. We will take reasonable steps to ensure the security of your personal data in accordance with applicable data protection laws. Standard contractual clauses approved by the European Commission which give personal data the same protection it has in Europe and/or the UK are in place with Preact Consulting Services Private Limited. Please note this does not affect or change the location in which your client solution is hosted. ANS does not have access to client data within a client solution unless expressly granted by you.

If clients have any issues concerning the protection of PII data, please contact DPO@ans.co.uk.

6. Objectives

This policy sets out the foundation of the information security objectives for the year ahead, the objectives listed in a separate document titled "ISMS Objectives". Within this document are the objectives for the year, derived from the internal & external issues and requirements of the board. Each objective is consistent with this policy in terms of achieving or maintaining the triad of information security (Confidentiality, Integrity, and Availability), measurable where possible, have owners or updaters, and be based on the risk assessment results of the organisation.

7. Security Working Group

ANS has established a Security Working Group (SWG) chaired by the Head of Information Security & Compliance who will invite attendees from around the business to feedback on the information security programme of ANS, its overall effectiveness and any suggestions for improvement.

For more details on how to participate in the SWG email: information.security@ans.co.uk.

ANS is committed to maintaining its ISMS and continually improving the system. A full, up to date list of ANS's certifications can be found here. ANS also maintain a secure cardholder data environment on its service delivery network along with robust physical security controls for the ANS Campus sites and the Data Centres.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan, annually, as a minimum.

In this policy, "information security" is defined as: *preserving*.

This means that management, all full time or part time staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the ISMS. The consequences of security policy violations are described in ANS's disciplinary policy. All staff will receive information security awareness training and more specialized staff will receive appropriately specialized information security training.

8. Confidentiality

"Property that information is not made available or disclosed to unauthorized individuals, entities, or processes."

This involves ensuring that information is only accessible to those authorised to access it and therefore preventing both deliberate and accidental unauthorised access to ANS's information and proprietary knowledge and its systems including its network, websites and e-commerce systems.

9. Integrity

"Property of accuracy and completeness."

This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency including for network, e-commerce systems, web sites, and

data back-up plans, and security incident reporting. ANS must comply with all relevant data-related legislation in those jurisdictions within which it operates.

10. Availability

"Property of being accessible and usable on demand by an authorised entity."

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The ANS network must be resilient and ANS must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity and resilience plans.

10.1. Of the physical assets

The physical assets of ANS including but not limited to premises, computer hardware, data cabling, telephone systems, filing systems and physical data files.

10.2. Information assets

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, web site(s), intranet(s), PCs, laptops, mobile phones and PDAs as well as on CD ROMs, USB sticks, back-up drives and any other digital or magnetic media, and information transmitted electronically by any means. In this context "data" also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.).

11. ANS

ANS and such partners that are part of our integrated network and have signed up to our security policy and have accepted our ISMS.

A SECURITY BREACH is any incident or activity that causes or may cause a break down in the availability, confidentiality or integrity of the physical or electronic information assets of ANS. If you think you have caused a security breach, or detected one. Please send all details to information.security@ans.co.uk.

12. AI

ANS utilise AI for its own internal use to supports its employees in their day to day role. ANS has an AIMS in place which aligns to ISO 42001 and is externally auduited against this standard. ANS have standalone policies for AI and its usage – a summary of these is provided below, but does not override the AI policies themselves, which can be found here in Internal and External

Policies IMS - Home

All AI systems must adhere to ANS's Information Security Management System (ISMS) and relevant standards, including ISO 27001 and ISO 42001, ensuring robust security controls throughout their lifecycle.

AI systems must only process authorised data and implement strict access controls to prevent unauthorised disclosure or misuse of sensitive information.

AI-related risks, including adversarial attacks, data poisoning, and model drift, must be assessed during design and reviewed periodically. Continuous monitoring for vulnerabilities and emerging threats is mandatory.

AI must be deployed in line with ANS's ethical guidelines, avoiding bias, discrimination, or misuse. All decisions influenced by AI should remain subject to human oversight.

Any AI-related security incident must be reported immediately through ANS's established incident reporting process. Breaches will be handled under the existing disciplinary framework.

Employees must complete AI security awareness training annually. Technical teams must receive specialised training on secure AI development and deployment practices.

External AI providers must comply with ANS's security requirements and contractual obligations. Due diligence and risk assessments are required before onboarding any third-party AI solution.