ANS Business Continuity Policy Statement

The Business Continuity Policy is intended to provide a guide in the case of a Business Continuity event occurring at ANS and its subsidiary companies. It is designed to show the impacts a BC event will have on ANS and its subsidiary companies (financially, physically and reputational).

The Business Continuity Plan covers all of ANS, its Data Centres and subsidiary companies this includes all government held data and Secret level data.

At ANS we aspire to be the UK's leading digital transformation specialist and leading Cloud Service Provider of choice. We aim to ensure that the services we provide embed excellence into both our and our customers' 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 make sure that the availability of this information is guaranteed according to agreed service levels and contractual agreements through our Business Continuity practices. Information is always managed in a way that meets all of our legal, regulatory and contractual obligation.

Each of the critical inward and outward facing business processes is identified and its criticality identified within the Business Impact Analysis in relation to RTO, RPO's and MTPD of the business function.

The critical information assets that are involved in each process are identified and cross-referenced to the asset registers. For each of the services, the risks (from disasters, security or equipment failures, loss of service, attacks, and loss of service availability) that ANS is facing are identified.

Also Identified, for each of the risks are the possible business continuity impacts that they will have on the business, ranging in seriousness from loss of site access through to loss of site(s). The risks are prioritised in terms of their impacts on ANS and the business continuity planning process makes arrangements to tackle these risks in order.

Identified, out of the risk assessment process, is the extent to which insurance can provide part of the continuity requirement and make appropriate arrangements.

Business continuity is the capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident. Business Continuity Management (BCM) is the process of achieving business continuity and is about preparing an organisation to deal with disruptive incidents that might otherwise prevent it from achieving its objectives. Placing BCM within the framework and disciplines of a management system creates a Business Continuity Management System (BCMS) that enables BCM to be controlled, evaluated and continually improved.

To embed these principles into our business, ANS have implemented a Business Continuity Management System (BCMS) aligned with the international standard for Business Continuity

Management, ISO/IEC 22301:2019 that is a part of a wide Integrated Management System that has been verified by our external auditor to be compliant with the international standard for all of ANS ISO certification including ISO 9001, ISO 27001, ISO 20000 and ISO 14001. This system is based on a Business Continuity policy framework; supported by detailed policies and procedures, and underpinned by the pragmatic application of industry best practice.

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 provides strategic direction to the Compliance Team. The Compliance Team ensures that the Business Continuity policy framework is regularly reviewed, communicated and that it continues to evolve and improve, and conform to the required standards.

The Business Continuity Plan addresses all the information continuity components of ANS's activities and ensures that adequate trained resources are available to provide continuity of all the identified assets, including taking appropriate steps for the protection of staff (including information processing staff) and all information processing facilities.

The Business Continuity Plan(s) is maintained within a business continuity planning framework (see below) and is subject to testing, maintenance and improvement. Developing and implementing continuity plans ANS's business continuity plan overview is drafted by the Head of Defensive Securities and Compliance and reflects considered plans that ensure business continuity in the event of any of the occurrences identified in the risk assessment process.

The ANS Executive has a high expectation for the implementation and support of this policy and supporting framework by all ANS employees, and for the Business Continuity practices of our strategic business partners to be equally robust. We regard effective Business Continuity as being everybody's responsibility to ensure it is embedded into our daily business lives. All of our staff are aware of the need to plan for the unexpected and understand their responsibilities in a crisis situation, these aspects being regularly enforced through a continuous programme of Business Continuity awareness and testing of the Business Continuity Plan (BCP).

Objectives Framework:

- Business Continuity Objectives: we will ensure that we deploy targets and procedures that address legal, regulatory and customer requirements
- Training: we will inform and educate employees and ensure they are aware of their Business Continuity responsibilities
- IT Infrastructure: we will apply fall back and alternate systems throughout the Business (protecting the confidentiality, integrity and availability of both our and our customers data)
- Supply Chain: we will ensure our third-party supply chain have implemented the Business Continuity controls necessary to support our Business Continuity objectives
- External Audit: we will ensure that Information Security policy and procedures are subject to independent and documented external audits & assessment
- Internal Audit: we will ensure that we measure, monitor and report performance of our policy and procedures through robust internal audits & assessment

- Testing: we will ensure that the Business Continuity Plan is subject to a yearly robust and rigorous internal test schedule
- Review: we will ensure the suitability, adequacy and effectiveness of the BCMS is subject to regular senior management review

All the critical business processes are identified in the plan, together with the responsibilities for restoration of service in the event of a continuity event.

The plan identifies the extent – for each of the critical services – to which service interruption is allowed before the continuity plan in invoked.

The Business Continuity Plan identifies the steps that should be taken to restore services and sets out how the Emergency Response Team will manage operations pending completion of recovery and restoration.

All staff who are involved in business continuity plans train in their roles and are involved in testing of the plans. Business continuity plans are tested and updated. Business continuity plans are classified as CONFIDENTIAL and are available only to staff authorised by the CTO (and including members of the Incident Response Team).

ANS has a single approach to business continuity planning (the BCP – made-up of a number of sub-plans) and a single business continuity planning process.

All subsidiary business continuity planning issues are dealt with in the context of that framework of a single plan with multiple sub-plans. ANS's business continuity plan and each of its sub-plans has a specific owner and, wherever possible, this owner is the individual identified in the asset register as the Owner of the asset, relationship or process.

As part of any third-party agreement where possible and/or appropriate, service providers are required to provide adequate fallback arrangements.

The BCP has a standard alert, escalation and plan invocation procedure which ensures that experienced senior executives decide on the extent to which continuity measures are required.

In a number of the sub-plans, specific criteria are identified which, when met, will automatically trigger that part of the BCP that is tied to that asset/process.

The BCP is built from a BIA that has been conducted across the business to identify which departments are a high priority and require more resource.

The BCP, and its sub-plans, place a substantial portion of discretion in the hands of the Crisis Team to determine appropriate reactions to a number of continuity events.

The BCP identifies emergency and fallback procedures, both in terms of a disaster at one or more sites and in terms of a business interruption at one or more critical processes and sets out the steps and resources required to move essential activities and services to backup locations, setting out the time scales within which services have to be returned to action.

Responsibilities are clearly identified throughout the BCP and, wherever possible, alternatives are identified.

All the required contact information is available in a single place to enable the Crisis Team to manage the response to a business interruption.

The critical resources required by the BCP have all been identified and are available at the locations where they are likely to be required. Staff training takes place on a planned basis.

"At ANS, we ensure the quality, reliability and security of the services we provide are second to none. To complement our comprehensive programme for business continuity, disaster prevention and total business recovery, ANS has implemented a Business Continuity Policy to ensure the effective availability of our services. Myself and the other members of the senior leadership team fully endorse this policy and expect the associated process and procedures to be embedded across the company."

Richard Thompson Chief Executive Officer