Security and Resilience Business Continuity
Policy & Processes

Security and Resilience Management

ACS ensures security and resilience management plays an integral part of our core business functions. It is fully incorporated into the operatonal and management processes at every level of our organisation and driven from the top down. Effective security and resilience management requires a reporting and review structure to ensure risks are effectively identified, assessed and appropriate controls are in place. ACS carries out regular audits to identify opportunities for improvement, our Risk Management Plan is an important part of our Security and Resilience Business Continuity Plan it details our strategy for dealing with risks specific to our business. By understanding potential risks and findings ways to minimise theirimpact, this would help ACS recover quickly ifan incident occurred.

Business Continuity Management Programme

Continuity of service is fundamental to any business therefore a robust Disaster Recovery and Business ContinuityPlan is of the upmost importance. Business continuity planning is a process that identifies potential impacts which threaten an organisation.

Our Plan is a fully integrated component of our management process it identifies, in advance, the potential impacts of sudden disruptions or drastic changes caused by natural and man-made disasters. All our sites are expected to implement preventive measures to minimise network failure and continue our business activities with minimal internal impact and without knock-on effect to our customers. It provides details of our resilience in allowing ACSto survive the loss of part or all our operational capability, we carry out annual testing of our Plan.

Our IT data is securely stored off-site and maintained by a third party and only Chris Campbell has access to directly extract data from the system. Regular back-ups are carried out to ensure all essential data and software can be recovered following a disruptive event. We can also emulate all operational services to our Ireland office whichcould take over in the unlikely event of catastrophic failure. A full audit trail is kept of all system amends and eventsto ensure ACS has full traceability of activity. We test our process are using a 3rd Party Cyber Essentials Plus.

We can operate from any location with internet access meaning we are not tied to one locality. We also have flexibility within our supply chain to enable orders to be delivered out of several warehouses around the UK. Stock remains off site in several hubs to minimise disruption of service levels in the event of an issue.

Harry Stevenson our Commercial Director would be ultimately responsible for managing our response in the event of a disruption. He would be in regular contact with our customers to provide updates on estimated timescales for a resolution.

Since ACS was formed, we have not had any situations where our Plan has been put into action. However, we continue to simulate situations to test our disaster recovery processes and business continuity planning.

Harry Stevenson
Commercial Director