



Actavo is committed to managing Information Security including Data Protection matters as an integral part of its business activities. It is our policy to ensure that all aspects of Information Security and Data Protection management across all business units protects the information and data that we handle, manage and control on a daily basis. This includes our management of Information Security by employees and subcontractors, as well as our interaction with customers and the public who come in contact with our business. In order to achieve this, Actavo will adhere to the following principles:

- Ensure compliance with relevant legislative requirements (including GDPR), standards and codes of practice through the implementation of ISO 27001. The Information Security Management System will form an integrated element of our Integrated Management System.
- Implement and maintain appropriate systems and procedures to prevent activities or actions that pose a threat to the security of our information and data, including that held and managed on behalf of and/or by customers, staff, contractors and suppliers.
- Systems and Procedures will be designed around the principles of Confidentiality, Integrity and Availability of information within the business that allows for the efficient operation of the business, while maintaining these core principles.
- Ensure that systems for identifying, assessing, eliminating and controlling risks to which information and data may be exposed are established, implemented and adhered to.
- Develop and maintain a positive Information Security awareness within the business based on a culture oriented on these aspects of our business both within the company and with external organisations, including customers' and suppliers', through communication, partnership and learning activities.
- Review customers' requirements and contract specifications in order to deliver a service that meets the customers' Information and Security needs and expectations.
- Evaluate and select suppliers of goods and services based on their ability to assist us in achieving our objectives set out in this ISMS policy.
- Provide equipment and infrastructure to ensure compliance with our Information Security Policy and procedures.
- Strive to ensure that our Information Security Systems are monitored and managed to ensure the safety of information and data held by and on behalf of the business.
- Pursue the continuous development and improvement of our Integrated Management System through constant performance evaluation based around the setting of SMART objectives, which are measured through reactive and pro-active monitoring.
- Foster an ethos of transparency and dialogue with our customers, employees, sub-contractors and the general public by the communication of this Policy and the implementation of our Integrated Management System procedures.

Keith Tobin
Chief Executive Officer
1st January 2025