

Statement of Intent Information Security Policy



DMN is committed to exercising due care and diligence to protect Information Systems relating to our vehicle movement and delivery service and other fleet services from unauthorised access, use, disclosure, destruction, modification, disruption or distribution at all times.

This will ensure that our reputation with our clients and all related interested parties is maintained through confidentiality, integrity and availability.

Our Senior Management Team will ensure commitment to all legal, regulatory, and other applicable business requirements, including contractual security obligations, are considered, and risk assessments against agreed criteria are regularly undertaken.

The Senior Management Team is responsible for establishing and maintaining systems and processes to ensure information security and integrity through instruction, policies, procedures and training to ensure that each employee properly understands what is required of them.

Equally, every employee, contractor or other individual working for or on behalf of DMN is individually responsible for maintaining the security and integrity of all information and data they come into contact with throughout their work.

Our policy of continual improvement and objective setting aligns with the ISO 27001:2017 standard requirements for Information Security Management Systems.

We will define objectives and targets to meet the requirements of this policy and review them at management reviews to enable continual improvement. The policy will be made available to interested parties as appropriate.

The Information Security Management System will be monitored regularly under the Management Team's ultimate responsibility, with regular reporting of the status and effectiveness at all levels.