

# TRANSPORTATION YOU CAN RELY ON

P31 – Information Protection Policy

01.08.2021



## **P-31 Information Protection Policy**

Information is a critical business asset and protecting the confidentiality, integrity and availability of company information assets from all threats whether internal, external, deliberate or accidental is a business priority. We will ensure we have implemented appropriate controls to secure our information assets, and those we are responsible for, using physical, procedural, staff and technical security measures.

### **Electronic Filing Systems**

The organisation has file naming conventions and a documented filing structure in place and all documents should be filed according to this guidance. All company issued documents should also be clearly labelled with file name / document number, issue version and relevant information classification. Folder filing overview documents and / or document register should be referenced to ensure files are named and saved correctly and all files should be saved to the allocated folder to ensure they are backed up. Files saved to personal documents folders or desktops may not be included in file backup systems.

### **Management of Records and Documents**

Records are defined as the data held within the files or completed forms and paperwork. A file may be defined as a single form template which in its completed form may comprise a large number of records. Records need to be managed and organised and are therefore filed as per the management of files procedure. Any records labelled '**confidential**' should be securely stored to prevent unauthorised access. All staff must ensure personal data is controlled and secure and that details are not disclosed to any other person (whether inside or outside the company) unless authorised to do so.


Filing of paper documents must be organised and properly indexed and confidential documents must be secured in locked filing cabinets when not in use.

### **Mobile Devices and Remote Access**

Information assets must not be stored on any mobile devices that have not been checked and approved by the company. Any mobile devices used to store information assets must be secured using technical and physical means at all times. Any remote access to information assets must be approved by the company following an appraisal of the security in place and once approved will be subject to ongoing monitoring. If remote access is no longer required any equipment issued should be returned and access accounts closed.

### **Protection of Information**

Protection of information is a business priority and we have ensured we have implemented appropriate controls to secure our information assets, and those we are responsible for, using physical, procedural, staff and technical security measures.



These measures include;

- **Monitoring and Backups** - ongoing monitoring of IT systems and networks and regular backups and testing of backups;
- **Data Protection** - responsibilities and procedures to ensure protection of personal data and compliance with data protection legislation;
- **Access Control** - Access to systems is granted following the principle of 'Least Privilege' and processes are in place to manage user accounts;
- **Secure passwords** - all users are required to use passwords securely;
- **IT Equipment checks** - rules and procedures covering the use of IT equipment. All IT equipment uniquely identified and listed on IT equipment list;
- **Management of Software** - controls over installation and updating of software;
- **Physical Security** - clear desk / clear screen policy, premises secured and monitored;
- **Disposal of IT equipment** - IT equipment can only be disposed of using approved contractor to ensure secure destruction;
- **Use of own IT equipment** - controls over the use of own IT equipment;
- **Staff training and checks** - all staff who have access to company information assets are given information security awareness training. Additional background checks on staff who process confidential information.

We shall review, measure and monitor our Information Security framework, documentation and implemented controls on an ongoing basis to ensure their relevance and effectiveness in protecting our information assets with the aim of continual improvement of our systems and performance.

**Approved by:**



Damian McLanachan

Managing Director

McLanachan Transport

Date: 01.08.2021