TRANSPORTATION YOU CAN RELY ON

P35 – Information Security Awareness Policy

01.08.2024

McLANACHAN TRANSPORT LTD
UK & EUROPEAN DISTRIBUTION

P-35 Information Security Awareness Policy

This policy is intended to provide guidance to all our workers on good practice and company policy and procedures with regards to information security.

Information is a critical business asset and protecting the confidentiality, integrity and availability of information assets from all threats whether internal, external, deliberate or accidental is a business priority. It is essential that all workers who access or process information at work are aware of the risks and good practice with regards information security. As well as all company policies and procedures workers should keep up to date with current developments including details of threats from appropriate external sources such as;

- National Cyber Security Centre - ncsc.gov.uk
- Cyber Aware - cyberaware.gov.uk
- Get Safe Online - getsafeonline.org

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;
- **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 disposed of using approved contractor;
- **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.

McLanachan Transport Ltd
6 Condor Glen
Eurocentral
Motherwell
ML1 4UY
T +44 (0)1698 813248
Email info@mtltransport.com

IT Equipment

All company staff with access to information technology and communications facilities are required to use these facilities sensibly, professionally, lawfully and with respect for the company and interested parties and in accordance with this policy and other company rules and procedures

IT equipment supplied for the use of workers should be used carefully and any issues reported.

All company IT equipment is maintained and checked and a register of IT equipment is maintained. Any new IT equipment should be checked, approved and added to the register prior to use. Server and network infrastructure cabinets should be kept locked and where appropriate computer workstations should be secured and ports removed or deactivated. Laptops and handheld devices must be stored securely and encrypted where required. All staff are responsible for ensuring IT equipment they have been issued is kept securely to prevent any unauthorised access.

Handheld Devices

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 and if any personal or confidential company information is viewed or stored on the device it must be encrypted. 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.

Good practice with Handheld devices;

- Use the security features available such as fingerprint recognition and always use a secure password;
- Ensure appropriate security software for tracking or remotely wiping the device is installed;
- Keep the device and all installed applications up to date;
- Do not use unknown or public wi-fi if connecting to business networks;
- Do not leave unattended or in left in view in an unattended vehicle.

McLanachan Transport Ltd
6 Condor Glen
Eurocentral
Motherwell
ML1 4UY
T +44 (0)1698 813248
Email info@mtltransport.com

Use of Own IT Equipment

All IT Equipment used to access company files, network or to send communications must be checked and approved prior to use and be subject to ongoing checks to ensure up to date Anti-virus / malware / Firewall software is installed and operational and to ensure minimum level of security is maintained including operating system and software security updates. In the case of a personally owned device holding personal data the company may require access to your device to review or delete personal data and therefore your consent for the company to access or remotely wipe your device will be required before it can be used for this purpose. Any devices used to access or store personal data must be encrypted. Confidential data must never be stored or viewed on any personally owned device.

The following rules must be followed for the use of handheld and own devices:

- Prior to use on company networks all devices must be registered and approved;
- All devices must be protected by pin, password or biometric authentication;
- Devices should not have non-approved applications or software installed and should have appropriate security software installed and all applications should be kept up to date;
- Good physical security measures must be taken - devices never left unattended or in vehicles;
- Any incidents, i.e. suspected unauthorised use of a device, should be reported;
- If lost, stolen or compromised it must be reported to the company immediately;
- Personal data should only be stored on mobile devices approved for this purpose.

Internet and emails

The internet should only be used for business purposes although some occasional use for personal purposes is acceptable if it does not interfere with normal operational duties and is used in accordance with the following guidelines;

- Users should never share their account login details as all internet use is monitored and logs are retained of sites visited by each user account;
- Personal use must be in own time and must not interfere with network performance;
- Internet must be used in an acceptable way and in compliance with legal regulations;
- Any IT security incidents including accidental clicking of links in a spam / phishing emails or accidental accessing of inappropriate content should be logged and reported.

McLanachan Transport Ltd
6 Condor Glen
Eurocentral
Motherwell
ML1 4UY
T +44 (0)1698 813248
Email info@mtltransport.com

The following is not permitted:

- Visiting any web sites that contain offensive, obscene or inappropriate content;
- Posting any comments that are offensive, obscene or inappropriate;
- Posting any images, videos or comments about the company, customers, suppliers, other workers or any other interested party associated with the business;
- Disclosing any personal, confidential or business related information online;
- Using company equipment to access any social media accounts;
- Download, upload or sharing of any software or copyrighted materials;
- Using any IT equipment where another user is logged in;
- Removal or alteration of any software including firewalls and other internet security software installed on company equipment.

Avoiding Phishing and other attacks

All workers must remain vigilant at all times to ensure no malware is accidentally installed on company IT systems and to avoid any scam or phishing emails. The following guidance should be followed:

- Ensure antivirus software is installed, operational and up to date at all times;
- Do not download or install unknown software, applications or games without approval;
- Do not allow any external parties to plug any devices into the company network and be report any suspicious looking devices;
- Always connect to the internet using company network which is protected by a Firewall or ensure firewall in place if connecting directly to the internet;
- Do not click any links sent within emails even if they have been sent from a trusted source;
- Never respond to any emails requesting bank login details or payment card details and never send card details or other confidential information via email;
- Report anything suspicious and take action to scan systems and change all passwords in the event of an attack.

McLanachan Transport Ltd
6 Condor Glen
Eurocentral
Motherwell
ML1 4UY
T +44 (0)1698 813248
Email info@mtltransport.com

Use of emails

It is important that emails sent on behalf of the company are always polite, courteous and professional at all times. Emails should be sent using company email accounts and equipment and all users should be aware emails are not secure and no personal or confidential information should ever be sent via email without additional security. Extreme care should be taken when dealing with any attachments received with emails as they may contain viruses.

Personal use is permitted but staff must ensure personal email use:

- does not interfere with the performance of your duties;
- does not affect server performance by leading to large numbers of files or bulky files being sent / received;
- does not have a negative impact on the company in any way.

Under no circumstances may the company communication facilities be used in connection with the operation or management of any other business unless express permission has been obtained.

If you copy an email to others, it may breach data protection laws if it reveals all the recipients' email addresses to each recipient. Accordingly, it may be appropriate to use the 'Bcc' (blind carbon copy) field instead of the 'Cc' (carbon copy) field when addressing an email to more than one recipient.

Password Security

Use of passwords is an important way of ensuring protected files and resources are secure and correct use of passwords is critical in maintaining security.

The following must be followed to ensure password security:

- Passwords should not be shared with anyone else within or outside the organisation;
- Passwords should be changed regularly;
- Passwords should be secure and difficult to guess; i.e. at least 8 characters using a mix of lowercase, uppercase, numbers and special characters. Names or dictionary words should be avoided;
- Password should be unique; avoid using the same password for different logins and accounts;
- Default passwords or passwords reset and sent via email should be changed;
- Passwords shouldn't be written down and stored in locations where they can be discovered;
- Passwords should not be stored electronically, especially in a file called 'passwords';
- Password managers or other software should not be used for managing passwords without prior approval.

McLanachan Transport Ltd
6 Condor Glen
Eurocentral
Motherwell
ML1 4UY
T +44 (0)1698 813248
Email info@mtltransport.com

Office Security

As well as physical security of IT systems it is also important to consider physical security to protect information. Personal or commercially sensitive information should not be posted to notice boards or office wall and should not be visible from outside the premises or from any reception or entrance areas. Doors, windows server rooms and network cabinets should be locked as required and any visitors to site escorted at all times. Any workstations that are used for processing confidential information must be sited in a location to ensure they are not overlooked or near windows and site visitors should be advised that they cannot use mobile phones with cameras within the premises.

Clear Desks - When away from desk for any extended period confidential paperwork must be placed in a locked drawer or stored securely. At the end of the working day desks must be cleared of all confidential or sensitive data.

Public areas - If working in a public area confidential papers must be kept secure at all times

Clear Screen - when left unattended all devices should be locked. No confidential information should be viewed if working in a public place.

Protected Information

Care must be taken to ensure all staff comply with Data Protection rules. Whenever and wherever you are processing personal data you must keep it secret, confidential and secure, and you must take particular care not to disclose to any other person (whether inside or outside the company) unless authorised to do so. Further information relating to the protection of personal data is in the company **Privacy Policy**.

Information Transfer

When transferring information internally or externally consideration should be given to the security of the transfer to ensure adequate protection of the information is in place. Where required a formal data transfer and processing agreement will be prepared covering the secure transfer of information with approved 3rd parties. Confidential information should not be sent by email to an internal or external source or saved to removable media without additional security. Company information should never be stored to personal cloud storage or sent to a personal email account.

The confidentiality of information being transferred on portable media or across networks, must be protected by use of appropriate encryption techniques.

McLanachan Transport Ltd
6 Condor Glen
Eurocentral
Motherwell
ML1 4UY
T +44 (0)1698 813248
Email info@mtltransport.com

Remote Access

All company policies, procedures and controls in place within the office are also to be followed while working remotely and steps are taken to ensure any new or additional risks from remote working are addressed.

To achieve this the following must be followed;

- All remote access or teleworking must be approved prior to the remote access of any information;
- Risks assessments will be completed, where required, and remote access only permitted once adequate controls are in place to mitigate any risks identified;
- A list of remote access authorisations will be maintained and periodically reviewed;
- If remote access is no longer required any equipment issued should be returned and access accounts closed;
- Classified information shall only be taken for use away from the organisation in an encrypted form unless its confidentiality can otherwise be assured;

When remote working it is important that all the relevant security measures and procedures in place within the office are followed at the remote location.

User Account Management

All users are given unique login details to ensure each account can be identified. A register of user logins is maintained for all systems where authenticated access controls are in place. Procedures are in place to ensure access rights are reviewed and removed when access is no longer required.

Where required the system administrator shall retain confidential authentication information to validate the identity of users. All users are required to adhere to all company policies covering use of IT equipment, data protection and management of passwords. User accounts should not be shared with any other users.

System Access

Access to systems and secure areas will be controlled and reviewed on an ongoing basis with checks to ensure only authorised users are able to access secured systems. Systems are also in place to log and monitor access and any attempted or actual unauthorised access will be reported as a security incident.

Software Installation

No Software should be installed without approval. Software and other necessary updates or patches should be installed when requested. Any new software will be subject to review prior to installation to ensure the software is suitable and compatible with other systems. Antivirus or other security software must never be removed or deactivated. Any issued with software including accidental installation of suspected malware must be reported. Software installed on all devices will be subject to regular software auditing and all worker must assist with this process.

McLanachan Transport Ltd
6 Condor Glen
Eurocentral
Motherwell
ML1 4UY
T +44 (0)1698 813248
Email info@mtltransport.com

Disposal of IT Equipment

All IT equipment is disposed of using approved supplier for secure disposal of IT equipment. Any personal devices that have been used to access company data must firstly be checked and securely processed prior to disposal.

If company rules and procedures are not adhered to, then use of our facilities may be curtailed or withdrawn and disciplinary action may thereafter follow.

Approved by:

Damian McLanachan

Managing Director

McLanachan Transport

Date: 01.08.2024

McLanachan Transport Ltd
6 Condor Glen
Eurocentral
Motherwell
ML1 4UY
T +44 (0)1698 813248
Email info@mtltransport.com