PLANES
MOVING & STORAGE

Information Security Policy

The Company strives to operate in a safe and secure environment for the purpose of protecting confidential information against loss, theft or unauthorized alterations. In addition to providing excellent service to our customers through an employee-oriented, quality conscious approach, we commit to protect the personal information that our customers provide to us and will only use it in the course of providing our services.

Our Responsibility

Every employee of the Company has a responsibility to protect the confidential information collected during the delivery of our services and to protect the confidential relationship between the Company, its employees, its customers, and partners. As an employee of the Company, you are an essential part of this process and must exercise good judgment and use the company's existing security policies and standards as a foundation for proper information handling.

Policy Compliance

This policy applies to all the Company employees. Failure to observe this policy may result in disciplinary action, up to and including immediate termination.

- Exceptions to this policy must be approved by the Information Technology department.
- Audits and monitoring may be performed to ensure policy compliance.
- Protection of customer information including Personally Identifiable Information (PII) is of utmost importance to the Company and is every employee's responsibility.

Policy Updates

This policy shall be reviewed annually. Changes to the policy will be approved, and relevant changes announced to employees

Help and Support

If you require assistance interpreting this policy, please:

- Contact your supervisor or manager.
- Contact the Human Resources Department

Security Awareness

<u>Security Training</u>

The Company provides information security awareness training and policies to guide employees in their duties and responsibilities.

- Employees are required to complete annual security awareness training.
- Employees are required to read, sign and comply with a non-disclosure agreement (NDA) providing for protection of confidential and/or customer information. Third parties may be required to sign an NDA.

<u>Social Engineering</u>

Social engineering is an intrusion method, which relies on human interaction to circumvent security processes and procedures. Examples of social engineering methods include:

- Phone calls involving the impersonation of a company representative or authority figure (known as "pretexting").
- Phishing emails and suspicious links.

PLANES
MOVING & STORAGE

Technology

Acceptable Use

Refer to the "Electronic Communications" Policy in the Company Employee Handbook for terms of acceptable use.

Approved Devices and Applications

Only approved devices, systems, software platforms and applications that are tracked and/or managed by the Information Technology department are permitted for company use.

• Systems and applications must be acquired and decommissioned using approved processes and procedures.
• Purchases must be made through approved channels.
• Only approved communications and data transfers are permitted for company use.
• Exceptions to this policy must be approved by the Information Technology department.

Software Updates

Updates to your computer's operating system and applications are managed by the IT dept. Updates include patches necessary to maintain the security and stability of the system. Do not disable or change these settings. When you receive updates, reboot your computer if prompted to do so.

Email

The Company email should only be used for business purposes (see Electronic Communications policy). There are security risks associated with sending messages via email.

Risks include but may not be limited to:

• Messages may be intercepted, read, and modified by unauthorized parties.
• Email may be used in delivering phishing attacks or malicious file attachments.
• Remote access to email accounts from non-corporate devices increases security risk.

External Sharing or Storing of Data

Use of Internet-based storage and apps is prohibited unless provided and managed by the Information Technology department. Exceptions to this agreement must be approved by the Information Technology department.

The company's most sensitive information (i.e. customer data, employee data) may not be:

• Emailed to non-Planes e-mail addresses or a third parties without appropriate protections,
• Printed and left unprotected or exposed longer than is business necessary,
• Downloaded to any external device (e.g. external hard drive, DVD or CD, USB drive),
• Transmitted to any personal device (e.g. home PC, smartphone, tablet), or
• Uploaded to external cloud-based services (e.g. Dropbox, OneDrive, Google) without approval from the Information Technology Department.

Mobile Devices

The Senior Manager for an employee's business or operating unit must approve the employee's access to company data through a mobile device. Use of a mobile device to access company data is subject to the "Electronic Communications" Policy.

• Only mobile devices that have been registered and approved will be permitted to access company data to perform work-related tasks.
• Employees must ensure their mobile devices are protected at all times.
• The Company may terminate access to company data by a mobile device.

Access

Account Management

Only authorized Company personnel will create user accounts.

• User accounts are restricted to authorized users.
• Access permissions incorporate the principles of least privilege and separation of duties.
• Privileged access should align with job responsibilities.
• User accounts are reviewed to ensure compliance with this policy.

Passwords

Establishing strong passwords and resetting them at regular intervals protects company information. The Company requires a password length of at least 8 characters and the use of three of the four character types (lower case alphabet, upper case alphabet, number, special character).
• Do not share a password with anyone including over the phone or in an email.
• Do not hint at the format of a password (e.g. my family name).
• Do not record passwords on paper.

Visitor Access

All visitors must sign in at the Security desk for a visitor badge. Visitor badges must be displayed at all times. Visitors must be escorted by an employee while they are in the building.

Remote Access

Remote access to information systems is restricted to approved use cases.
• Approved connections must be made securely.
• Contact the Help Desk for more information.

Vendor Access

Vendor access to information systems is restricted to approved use cases.
• Approved connections must be made securely.
• Senior management of the department or business unit must approve vendor access.
• Contact the Help Desk for more information.

Data Protection

Data Classification

The Company uses a single classification (Confidential) for all data that is received, processed, stored and generated on its network or hosted by a third party provider on the Company's behalf. Confidential data is protected at the highest level necessary to ensure the privacy of our customer information as well as to meet or exceed all regulatory and legal requirements.

Data Encryption

The Company provides solutions to protect data with encryption where appropriate. This includes using:
• Secure email for sending sensitive messages and attachments outside our network,
• Secure websites connections and applications,
• Encrypted file transfers and computer media.
Exceptions to this policy must be approved by the Information Technology department.

Privacy

The Company has an affirmative and continuing obligation to respect the privacy of customers and to protect the security and confidentiality of customer information. The handling of privacy information is subject to the "Privacy" policy." In conjunction with this policy:
• Each employee who has access to customer information shall be required to sign a confidentiality agreement.
• The company shall train their respective employees on privacy procedures, and each employee shall complete any company-wide privacy training.

PLANES
MOVING & STORAGE

Incident Management

Incident Reporting

While the Company takes precautions to protect our network, applications and data from malicious attacks, there is still a risk that they may be compromised. Incidents and suspicious activities such as those listed below should be reported immediately to the Help Desk or the Information Technology department.

- Loss of sensitive data,
- Denial or loss of service,
- Targeted online and social engineering attacks,
- Unauthorized modifications to data,
- Non-compliance with policies or guidelines,
- Employee abuse of privileges or policies,
- Loss or failure of encryption protections,
- Unauthorized changes to a system, and
- Access violations.

Audits and Reviews of Information Security Controls

Information security controls are periodically monitored, reviewed, and improved to ensure that the specific security and business objectives of the Company are met. Thus, information security conditions and policies of the Company are subject to annual internal and independent audits or reviews. Security audits or reviews are:

*Performed by individuals who have sufficient technical skills and knowledge of information security disciplines.

*Focused on ensuring that information security controls function as intended and are effective enough to reduce risk to an acceptable level.

*Provided to management so that risks can be remediated, or controls can be modified.

Revision History

Date of Change	Responsible	Summary of Change
11/09/2018	Jeff McGrath	Initial publication
01/08/2019	Jeff McGrath	Added Audit and Review sect.