Cybersecurity

(WAL Security Procedure 7.1)

In accordance with CTPAT cybersecurity, WAL reviews its IT policy annually or as risk or circumstances may dictate. If the IT policy is substantively changed following a review, you will be notified of such a change.

Data Breach

- ❑ If you detect data breach, data corruption, or data loss, notify the management immediately so that the management may contact the relevant IT companies to recover the data.

Social Engineering

- ❑ If you become a victim of social engineering (e.g., phishing), you must notify the management immediately.
- ❑ The victim is required to cooperate with the management to retrieve data or for investigative purposes.

Counterfeit Products

- ❑ You must use only authentic IT products and components.
- ❑ If employees discover the use of counterfeit products on any of the company's IT systems, they are responsible for notifying the management immediately.

IT Abuse and Disciplinary Action

- ❑ WAL does not allow improper access (i.e., unauthorized access) to our internal IT systems or external websites and tampering with or altering of business data.
- ❑ All system violators are subject to appropriate disciplinary actions for abuse, which may range from a warning to an involuntary termination.
- ❑ All disciplinary actions related to such violations will be documented for investigative purposes.

Cybersecurity

(WAL Security Procedure 7.1)

Cybersecurity and Cyber Threat Protection

- WAL has installed both an anti-malware and firewall to protect the company's IT systems.
- Removing, attempting to remove, or otherwise circumventing these protections in lace will be deemed to be IT abuse and is subject to disciplinary actions.
- Periodically, WAL's security software will be updated to maintain its security integrity.
- If updates fail to install on your device, or fail to install properly, the management must be notified immediately.

IT Network Health Check

- WAL's network health must be checked monthly for security and infrastructure integrity.
- If anyone suspects any irregularities in company network, the management must be notified immediately.

IT Inventory

- It is WAL's policy to conduct IT inventory regularly.
- During the process all employees' laptops and computers are subject to random check.
- The company checks the systems to ensure that the integrity of sensitive information related to the import/export processes is maintained.

IT Equipment Disposal

- WAL uses data destruction services, i.e., Iron Mountain, that follow NIST 800-88 Guidelines for Media Sanitization.
- Disposing IT equipment using any other method is strictly prohibited.

Cybersecurity
(WAL Security Procedure 7.1)

Limitation of Access

- Passwords and IDs are the entry point to our IT resources. Protecting access to our computer resources is pivotal in ensuring that our systems and the confidential information they contain remain secure.
- To this end, individual accounts are issued to all employees and access is limited based on the employee's assigned duties.
- The limitations will be reviewed periodically and based on the employee's duties, will be expanded, or narrowed.

Password Change Requirement

- To mitigate security risks and enhance cybersecurity, all employees of WAL must change their passwords to the company IT systems on a 90-day basis.
- The company IT systems that require periodical password changes are import/export operation systems and email system.

Password Handling

- Passwords for all systems are subject to the following rules:
  - No passwords are to be spoken, written, emailed, hinted at, shared, or in any way known to anyone other than the user involved. This includes supervisors and personal assistants.
  - No passwords are to be shared to "cover" for someone outside of the office.
  - Contact IT personnel to create a temporary account if there are needed resources to access.

Cybersecurity

(WAL Security Procedure 7.1)

Computer Log-off

- The user must “Log-off” the computer if the user will not have the computer under direct observation for a period time.
- The user must “lock” the computer using screensavers or sleep mode if the user will only be gone for a few minutes.
- The computer must be logged off or turned off at the end of the workday or work session.

Personal Devices

- All employees of WAL that use personal devices must adhere to the company IT policy contained herein.