

PEI, Inc.
598 Red Oak Rd
Stockbridge, Ga. 30281

LOSS PREVENTION AND SECURITY PLAN

Effective Date: June 1st, 2004

Revision 1: January 3, 2005

Revision 2: June 24, 2006

Approval Date: June 26, 2006

Approval Authority: Executive Director

Approved By: Jay Patterson

1. PURPOSE:

- 1.1. To protect PEI, Inc. assets to include employees, property, processes, information, and information systems through security processes including security against theft, loss, or natural disaster.
- 1.2. To protect shipments in our transportation network.
- 1.3. To provide processes and train our staff in order to keep PEI, Inc. free from loss and mishap.
- 1.4. To provide a plan of response to varying levels of National security.
- 1.5. To make every effort for continuous improvement in our security performance by identifying, assessing, addressing vulnerabilities, preventing or mitigating incidents, enhancing training, developing response capabilities, maintaining and improving relationships with customers.

2. SCOPE:

- 2.1. All employees will receive training in this plan to provide:
 - 2.1.1. Awareness in ways to prevent theft and vandalism.
 - 2.1.2. An awareness in security issues associated with the transportation industry, and in particular, our unique transportation processes.
 - 2.1.3. Recognizing and responding to possible security threats as well as possible methods to enhance security.

3. REFERENCES:

- 3.1. Customs Trade Partnership Against Terrorism (C-TPAT)
- 3.2. PEI, Inc. Employee Handbook
- 3.3. PEI, Inc. Emergency Procedures Plan
- 3.4. PEI, Inc. Safety Policies

4. DEFINITIONS

- 4.1. Loss- The theft, destruction, and misuse of any property and employees, care, or ownership of PEI, Inc. that renders it unusable or missing.
- 4.2. Mishap- Any loss caused by human error or an act of God.

- 4.3. Theft- The willful misuse, pilfering, or stealing of any PEI's owned property. This includes all property under the control of PEI, Inc.
- 4.4. Transit- Any freight that is in between its origin and destination. Or any shipment in the care of PEI.
- 4.5. Computer Network/System- Any part of the Information Technology (IT) department. This includes, Personal Computers or PC Servers, Laptops, Intranet, and e-mail.
- 4.6. MIS Department - Management Information System Department.

5. RESPONSIBILITIES:

- 5.1. Safety Department - Responsible for assisting in Loss Prevention Investigations, documenting theft/loss incidents and security recommendations. Sets PEI's Corporate policy on safety and security, as well as implementing procedures under the direction of Senior Management.
- 5.2. General Manager - Responsible for ensuring implementation for this process.
- 5.3. Operations/Warehouse Manager - Responsible for taking corrective action and ensuring that the proper or necessary training is carried out.
- 5.4. Training Manager - Responsible for ensuring training is conducted and retraining is implemented and documented.
- 5.5. Driver/Warehouse/Employees - Responsible for adhering to security measures as outlined.

6. PROCEDURE:

6.1. Theft Response Plan

- 6.1.1. All incidents involving losses are to be reported to the Safety Department and the appropriate law governing enforcement agency. When a loss does occur all efforts will be made for recovery and cessation of the factors that lead to the loss.
- 6.1.2. In the case of any criminal act (e.g. theft, hijacking) the safety department must be notified immediately after the proper law enforcement officials have been notified. The Safety Department will represent PEI's interests, and will be the point of contact for the company.
- 6.1.3. Operations will take the following actions:
 - 6.1.3.1. Report the theft to local, state, and federal agencies when appropriate. Ensure the vehicle(s) and freight are entered into the National Crime Information Center (NCIC) via the above agencies. A good description of the item(s) stolen and serial numbers will be required.
 - 6.1.3.2. Report the theft to the Safety Department by calling 888-590-9255. A Safety Department Supervisor will then contact the Safety Manager.
 - 6.1.3.3. Alert Company drivers via cell phone.
 - 6.1.3.4. Contact all facilities advising them of the situation and require the information to be relayed to their local drivers.
 - 6.1.3.5. In the event a reward is authorized, all notifications will include this information and the amount of reward offered.
- 6.1.4. The Safety Department shall coordinate all efforts of recovery and apprehension with appropriate law enforcement officers.
 - 6.1.4.1. Make certain all-available information on the theft has been gathered for a comprehensive investigation and prosecution.

- 6.1.4.2. Monitor and coordinate with Operations personnel involved in the theft response.
- 6.1.4.3. Determine the feasibility of rewards, its amount will be determined by Senior Management, and initiate the printing and distribution of the reward posters.

6.2. Employee/Driver Responsibilities

- 6.2.1. Maintain situational awareness of world events and ongoing threats, via the news media (newspapers, TV, radio, etc.).
- 6.2.2. Keep their family members and supervisors aware of their whereabouts while in transit.
- 6.2.3. Determine the location of all emergency exits and stairwells in buildings they enter.
- 6.2.4. Take any threatening or malicious communications (Telephonic, facsimile, written, oral, or E-Mail) or bomb threat seriously. If such a call is received, obtain and record as much information as possible to assist in identification of the caller. Record the time of the call, the exact words, any distinguishing features of the caller, and any background noise. Report the information to your immediate supervisor/dispatcher so that local law enforcement can be notified.
- 6.2.5. Take notice and report suspicious devices, unattended briefcases, or other unusual materials immediately to your immediate supervisor. Do not attempt to handle or remove the object.
- 6.2.6. Be alert and immediately report any situation that may constitute a threat or suspicious activity to your immediate supervisor/dispatcher.
- 6.2.7. During the course of employment/contract, access may be granted to confidential information regarding phases of PEI, Inc. business. This information is not to be revealed to unauthorized personnel.
- 6.2.8. PEI, Inc. requires that no public statement or commentary representing PEI be made in any way without first obtaining consent from the Corporate Office. All events and situations that pertain to the Company and are observed while in performance of their duties will remain confidential.
- 6.2.9. The use or possession of firearms or other illegal weapons is strictly prohibited on company property or in the performance of your duties.
- 6.2.10. No employee/driver is to solicit or accept any gift or gratuity from outside parties for any reason relating to employment/contract with PEI including performance of services, special treatment, or dissemination of company information. Especially prohibited is the acceptance of any gift or gratuity for the performance of services or for special treatment.

6.3. Employee Security Standard Operating Procedures

The driver provides a major point of vulnerability to risk exposure. In recognition of this vulnerability, we must expect higher standards of acceptable performance for all PEI drivers. Employee Drivers/Contract Lease Operator hiring shall focus on the selection of the proper individual that meets PEI standards.

- 6.3.1. Driver Screening and Hiring.

- 6.3.1.1. Any person who drives for PEI and has the primary responsibility of transporting customer product or shipments shall be qualified as specified in PEI Safety Policies.
- 6.3.1.2. All qualified drivers will be subject to a background check, Motor Vehicles Record (MVR) check and periodic Drug and Alcohol testing.
- 6.3.1.3. Driver training program.
 - 6.3.1.3.1. All over the road drivers will attend an orientation at the Corporate Office – Stockbridge, Ga prior to being assigned a shipment.
 - 6.3.1.3.2. Orientation on company rules and procedures will be conducted and the driver shall participate in on-going in-service training.
- 6.3.2. Dock / Warehouse Employees
 - 6.3.2.1. All Warehouse Employees will successfully pass a pre-employment criminal background check and a drug and alcohol test.

6.4. En Route Procedures Cargo Security

- 6.4.1. Every reasonable effort will be made to safeguard company property, equipment, and shipments, but not at the expense or the safety of the driver. As the visible representative of PEI, Inc., all drivers shall perform in a manner as to clearly demonstrate to the customer a concern for their cargo entrusted to our care.
- 6.4.2. Cargo Seals
 - 6.4.2.1. When required by the customer on Full Truck Loads only, seals will be utilized to ensure that the vans/trailers moving between branches and/or shipper and consignee are not subject to cargo theft without detection. The seal will be affixed to the van/trailer by the shipper.
 - 6.4.2.2. Sealed truckload shipments should never be delivered without the original shippers seal. It is the responsibility of the driver to review all bills of lading (BOL) before leaving the shippers loading dock. If the BOL calls for a seal on the van/trailer and a seal has not been installed, the driver must contact Operations. Operations will complete an inquiry as to the status of the seal and advise the driver. If it is determined that no seal is to be placed on the van/trailer then the BOL must be corrected by the shipper. If it is determined that a seal is to be placed on the van/trailer then the shipper must affix a seal before the van/trailer leaves the dock area.
 - 6.4.2.3. When a truckload shipment is picked up by a PEI driver, and the shipper has placed a seal on the trailer, the seal can only be broken by the consignee or the driver with prior written authorization from the consignee. The consignee must sign the BOL with the seal intact upon delivery. If the BOL indicate that a seal must be on the trailer, and it is discovered on delivery that there is no seal, then the branch General Manager must be notified immediately for further instructions.
- 6.4.3. Locks And Keys
 - 6.4.3.1. Locks and keys provide physical security measures for protection against unauthorized entry into PEI trailers, against theft of company property, and for safeguarding freight documentation and cargo entrusted to our care.

- 6.4.3.2. Locks used to secure trailers are provided on each trailer by the Maintenance Department. Drivers will be issued their key at orientation.
- 6.4.3.3. The driver from the point of origin to final destination shall padlock all trailers containing freight. All drivers will utilize a PEI padlock on all loaded trailers as a condition of employment/contract. Padlocks shall be left on the trailers at all times.
- 6.4.3.4. Trailer doors on all loaded and/or equipped trailers must be kept locked when parked at a PEI facility or dropped at an authorized location.
- 6.4.3.5. If a driver parks a trailer at an authorized site for his/her convenience, an approved kingpin must be placed on the trailer, or be secured in a fenced in area that can be locked. Should a lock need to be cut off, authorization must be obtained from Management, preferably the Operations Manager.
- 6.4.4. En Route Driver Responsibilities
 - 6.4.4.1. Drivers are not to discuss the cargo being hauled, or past cargo that was hauled with anyone outside the Company while in transit. Destination, origin, or intermediate points are for the information of authorized personnel only.
 - 6.4.4.2. Under no circumstances will a loaded trailer be dropped or left unattended at an unauthorized site or relay point. All efforts will be made to deliver this loaded trailer to the consignee, a relay driver, or a branch location. There are no exceptions unless specifically approved by the branch General Manager or the Senior Vice President of Operations. In those specific instances where a trailer is dropped at a location other than a PEI facility, the trailer padlocks and kingpin lock will remain in place. Violation of this policy will be grounds for termination.
 - 6.4.4.3. No hitchhikers or any other unauthorized personnel are allowed in tractors or trailers. Violation of this policy will be grounds for severe disciplinary action including possible termination.
 - 6.4.4.4. If, after a driver accepts the load, the driver discovers the doors or locks to the trailer are opened or tampered with, by someone else, the driver must report it to Operations immediately.
 - 6.4.4.5. Power units and loads are to be parked in well-lighted areas during the hours of darkness. Isolated areas of truck stops, terminals, and customer lots are to be avoided whenever possible. When the National "Threat Level Security" color code is at Orange, power units and loads must be parked in well-lighted areas ONLY where truck is visible at all times, and when the level is at RED, drivers must park in secure areas only (i.e.: fenced in secure lot).
 - 6.4.4.6. Escalating diesel fuel prices dictate that drivers be encouraged to take action to avoid potential fuel thefts.
 - 6.4.4.6.1. Where possible the driver shall remain in eye contact of his vehicle. When patronizing motels and restaurants, the unit should be visible from the lobby and/or seating areas, and in a well-lighted area.
 - 6.4.4.6.2. When tractors are to be left unattended the keys shall be removed and the cab locked.

- 6.4.4.7. A driver must report overages or damaged freight on an exception sheet. Any such occurrence must be reported to the Claims Department.
- 6.4.4.8. In the event of a hijacking or potential hijacking, the driver will surrender the vehicle. The safety of our drivers is the foremost concern.

6.5. Facility Security Standard Operating Procedures

Proactive security and loss prevention programs for PEI facilities are important elements in the total system of providing safe, uninterrupted, and efficient service to our customers. These programs result in reduced risk exposure, reduced losses, improved response time, better communication between corporate management, and field operations. When a loss occurs, all efforts will be made for recovery and prosecution will be made to the fullest extent of the law.

6.5.1. All Branch Locations - General

- 6.5.1.1. The General Manager of each branch is responsible for the physical aspects of security as it relates to his/her individual branch location and for directing the activities of employees under their control.
- 6.5.1.2. Access to the facility yard and dock areas will be limited to authorized personnel only. All employees, vendors, salesmen, and other visitors will park only in designated areas as defined by the General Manager and conduct their business in a controlled environment. All visitors/vendors must be escorted while on Company property.
- 6.5.1.3. Approaching unauthorized vehicles on company property should be conducted by at least two employees, question drivers and direct them to move immediately, if the vehicle is parked and the owner cannot be identified, notify the Facilities Manager and have the vehicle towed from the company property. Consult your local law enforcement officials for laws governing the removal of unauthorized vehicles.
- 6.5.1.4. At least once a week, preferably first thing Monday morning, a yard check will be conducted. Tractors and trailers are to be examined for damage as well as unauthorized entry. The Safety Department must be notified immediately upon discovery of any type of damage or related security concerns. In the event cargo is discovered to be missing, the General Manager must be notified immediately. Documentation of the day and time when the yard check was conducted must be kept and retained for a period of six (6) months, if no abnormalities are discovered. Damage, theft and unauthorized entry reports will be kept on file for a period of no less than seven years.
- 6.5.1.5. It is the responsibility of the General Manager or his designee to notify the Corporate Safety and Claims Departments of theft or pilferage. The General Manager or his designee will also take the following action in the event of such unlawful acts:
 - 6.5.1.5.1. Review and maintain all pertinent records available at the facility for relay to the Corporate Safety and Claims Department. All originals must be safeguarded to prevent any tampering or destruction.
 - 6.5.1.5.2. Notify proper law enforcement authorities if required, and the

Corporate Safety and/or Claims Department, who will then advise the Senior Vice President of Operations and the Administrative Vice President.

- 6.5.1.6. Branch locations are not authorized to employ outside security services of any type without prior approval of Senior Vice President of Operations. Any anticipated need for such service is to be directed to the Senior Vice President of Operations accompanied with the following information:
 - 6.5.1.6.1. Reason for service.
 - 6.5.1.6.2. Length of time required.
 - 6.5.1.6.3. Number of guards and hours of employment.
 - 6.5.1.6.4. Projected costs.
 - 6.5.1.6.5. Certificates of Insurance - Necessary documents (Certificate of Insurance, etc.) should be requested from the designated security source.
 - 6.5.1.7. Bills of lading, shipping order, delivery receipts, and all other such documentation will be controlled and secured in such a manner as to prevent access by unauthorized persons.
 - 6.5.1.8. Tires, tools, and parts shall be kept in a secure and locked location subject to annual inventory.
 - 6.5.1.9. All areas are to be secured when the facility is not in operation.
- 6.5.2. Warehouse and Building Security
 - 6.5.2.1. Physical Security: All buildings should be constructed of materials, which resist unlawful entry and protect against outside intrusion.
 - 6.5.2.1.1. Physical security should include:
 - 6.5.2.1.1.1. Building Alarm Systems:
 - 6.5.2.1.1.1.1. Fire Suppression: This system is fully monitored 24 hours a day with an off-site vendor who reports any alarm activity directly to the police or fire department as well as an emergency contact list. The actual reporting process is explained in section 6.5.2.1.1.2 below.
 - 6.5.2.1.1.1.2. Intrusion and Motion Detectors: This system is monitored during non-working hours. All doors and windows are alarmed for intrusions where deemed necessary. A motion detector system is strategically placed through out the building. The notification process is detailed in section B below.
 - 6.5.2.1.1.1.3. Individual alarm access codes will be issued to supervisors and above. Upon the individual leaving the company, the alarm code will be canceled and keys returned.
 - 6.5.2.1.1.1.4. Emergency back up system (Battery) will be capable of functioning for a minimum of 15 minutes in case of activation during a power failure. Alarm systems will function for that time period.
 - 6.5.2.1.1.2. Notification Process:
 - 6.5.2.1.1.2.1. In conjunction with the systems above, it is necessary to

have a process in place to notify the proper people in the event of an incident.

- 6.5.2.1.1.2.1.1. Fire Alarm
 - 6.5.2.1.1.2.1.1.1. Notify Fire Department
 - 6.5.2.1.1.2.1.1.2. Notify emergency contact list
- 6.5.2.1.1.2.1.2. Intrusion / Motion Detector
 - 6.5.2.1.1.2.1.2.1. Notify Police Department
 - 6.5.2.1.1.2.1.2.2. Notify emergency contact list
- 6.5.2.1.1.3. Security Hardware Issues
 - 6.5.2.1.1.3.1. All doors and windows must be checked periodically for defects. Any missing or broken hardware will be fixed or replaced.
 - 6.5.2.1.1.3.2. A complete process covering the issue and return of all keys for the facility will be in place. This will be addressed in the employee education section of training.
- 6.5.2.1.1.4. Adequate locking devices for external and internal doors, windows, gates and fences.
- 6.5.2.1.1.5. Points of entry to the dock should display "Restricted Area-Authorized Personnel Only" signs. Normal points of entry and exit from the dock area should be limited. Persons entering or exiting the dock area should ideally do so through one main access point. Emergency exit doors should be marked as such, and configured to facilitate exiting from the building interior and prevent entrance into the building from the outside.
- 6.5.2.1.1.6. Segregation and marking of international, domestic, and high-value cargo within the warehouse by a safe, caged, or otherwise fenced-in area. The caged/fenced in area should include the overhead or top cover on the caged/fenced in area.
- 6.5.2.1.1.7. Adequate lighting provided inside and outside the facility to include parking areas.
- 6.5.2.1.1.8. Separate parking area for private vehicles separate from the shipping, loading dock, and cargo areas.
- 6.5.2.1.1.9. Having internal/external communications systems in place to contact internal security personnel or local law enforcement police.
- 6.5.2.1.1.10. Customer Goods: Damaged, un-wanted freight or goods may be given to employees by the customer/owner PROVIDED:
 - 6.5.2.1.1.10.1. The customer/owner gives WRITTEN approval to the employees stating that the customer/owner no longer wants the item(s) and that the employees can take custody of it.
 - 6.5.2.1.1.10.2. The employees or obtains written approval from Company Management. A copy of the written approval from the customer/owner and Company Management must be filed with the order documentation in the event the

customer/owner later files a claim that the item(s) were lost or stolen. The Claims Department will have access to the written approvals from the customer/owner and Company Management.

- 6.5.2.1.1.11. Gym bags, duffle bags, backpacks, lunch coolers and the like are not allowed in the dock area. Employees must secure and store any bags in a designated area before the start of their shift.
- 6.5.2.1.1.12. Forklifts are only permitted out of the dock area to perform specific tasks assigned by Branch Management.
- 6.5.2.2. ACCESS CONTROLS: Unauthorized access to facilities should be prohibited.
- 6.5.2.3. PROCEDURAL SECURITY: Procedures should be in place to protect against un-manifested material being introduced into the warehouse.
 - 6.5.2.3.1. Security controls should include:
 - 6.5.2.3.1.1. Having a designated supervisor to oversee the introduction/removal of cargo.
 - 6.5.2.3.1.2. Properly marked, weighed, counted, and documented cargo/cargo equipment verified against manifest documents.
 - 6.5.2.3.1.3. Procedures for verifying seal on containers and trailers.
 - 6.5.2.3.1.4. Procedures for detecting and reporting shortages and overages.
 - 6.5.2.3.1.5. Procedures to notify Customs and other law enforcement agencies in cases where anomalies or illegal activities are detected or suspected by the company.
 - 6.5.2.3.1.6. Proper storage of empty and full containers to prevent unauthorized access.
 - 6.5.2.3.1.7. Personnel Security: Branch locations will conduct employment screening and interviewing of prospective employees to include background checks and application verifications.
 - 6.5.2.3.1.8. Education and Training Awareness: A security awareness program must be provided to employees including recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized access. These programs should encourage active employee participation in security controls.

6.6. Cyber & Information Systems - Standard Operating Procedures

This section sets forth the policies of PEI with regard to its computer network, including access to and review or disclosure of electronic files and electronic mail (e-mail) transmitted through or stored on any part of the Company's computer system. This policy also addresses proper use of e-mail and the Internet.

6.6.1. Ownership

- 6.6.1.1. PEI's computer system includes individual desktop computers (PC's), laptop computers, floppy disks, compact disks (CD's), magnetic tapes, modems, file servers, printers, and all other components of the Company's computer network. All hardware and software are the property of PEI.

Records, files, and electronic communications contained in these systems likewise are the property of PEI.

6.6.2. No Modifications

6.6.2.1. Employees are prohibited from making any-hardware modifications to PEI's equipment or to use hardware brought in from outside the Company without prior express approval of the MIS Department. Likewise, employees are prohibited from installing any software whatsoever onto the network. Often the installation of a new software program can alter or replace critical "system" files needed by other applications. Employees may install software to the local hard drive of a PC only with express prior permission of the MIS Department. Be sure the Company's approved virus checking software is installed with the latest data file and always running on your computer. Never disable this software. Never insert any floppy disks into your PC or download any files from any, outside source without first checking them for viruses.

6.6.3. Use for Business Purposes

6.6.3.1. Use of the PEI computer network is provided to employees at the Company's expense to assist them in carrying out the Company's business. Unauthorized review of files, dissemination of passwords or confidential information, damage to systems, removal of files or programs, or improper use of information contained in the computer system is strictly prohibited. Access through the Company to the computer system (and to the extent the Company elects to make it available to the Internet) is intended solely for business related purposes. Use of the computer network or the Internet to engage in commercial activities for your own benefit, or for the benefit of anyone other than PEI, is strictly prohibited

6.6.4. Inspection and Monitoring

6.6.4.1. PEI's computer system and its contents are subject to inspection, examining and/or monitoring by authorized Company employees. There are many reasons why the Company may need to access employee-mail, computer files, the computer network or other company property, including but not limited to the need to conduct business at times when an employee is unavailable: to respond to requests by outside auditors of counsel: to maintain control to conduct training activities; and to monitor job performance and investigate employee conduct. The Company has the capability to access, review, copy, modify and delete any information transmitted through or stored on the network, including e-mail messages. The Company reserves the right to access, review, modify or delete all such information and to disclose it to any party (inside or outside the Company) that PEI, in its sole discretion, deems appropriate.

6.6.5. Security and Passwords

6.6.5.1. Security on the computer system is a high priority. Employees must use passwords as made available by the MIS Department to protect against unauthorized access to files on which they are working. Note however, that individual passwords do not prevent authorized Company representatives from accessing those files. Never disclose personal or system passwords to anyone other than authorized Company representatives. Keep your password in your head, on your person (wallet or purse), or locked up. If

you believe that someone else knows one of your passwords, you should contact the MIS Department to have your password changed.

- 6.6.5.2. All computer systems [main frame and personal/laptop computers] must be secure from unauthorized access by way of secured/locked access to rooms and/or buildings, in addition to password protection.
- 6.6.5.3. A secure gateway or firewall must be established to limit only authorized access via the Internet or LAN/WAN.
- 6.6.5.4. All systems will be protected from the introduction of computer viruses/worms.
- 6.6.5.5. Schedule for system and data backups
 - 6.6.5.5.1. Backup of system files are to be done daily. System, data backups and Initial Program Loads (IPL's) will be processed at or around 2:00 AM each morning. The system will not be available during this time.
 - 6.6.5.5.2. Should the system crash it should be restored with no data failure. Downtime should be at a minimum provided there are no system issues for a complete system recovery. If data integrity is compromised, recovery should be from the previous nights backups. No data is saved during the day. Data throughout that day will be lost.
 - 6.6.5.5.3. Should there be a system failure/crash, all information shall be processed manual and back loaded once the system is restored.
 - 6.6.5.5.4. Copies of system data and any non-vital records backed up shall be stored off site daily. If any backup files are needed they should be within one hour from the main office.
- 6.6.6. Notebook Computers
 - 6.6.6.1. Extra precautions must be exercised when taking confidential information out of the office in a notebook computer. Never leave notebook computers that contain certain confidential information unattended while traveling. Confidential information should never be stored on the hard drive of laptops. Never put a notebook computer or external hard drives through an airport or other security metal detector. While resulting damage to the computer is uncommon, when it does occur it usually results in complete, permanent loss of all information stored on the computer.
- 6.6.7. Copyrighted Information
 - 6.6.7.1. Use of the PEI computer system to copy and/or transmit software programs, documents or other information protected by the copyright laws is prohibited by federal law and may subject you and the Company to civil and criminal penalties. Never copy software programs of any kind, including programs on the network, without express authorization from the MIS Department. Never accept copies of any software from other employees or persons outside the Company without approval of the MIS Department. Never download information from the Internet without approval from the MIS Department. This includes, without limitation, screen savers, games, personal finance software, and income tax software, as well as any type of software used in your daily work.
- 6.6.8. E-Mail Guidelines and Etiquette
 - 6.6.8.1. Use of computer software to engage in any communications that are in violation of the Company's policies including, but not limited to,

transmission of comments or jokes that are discriminatory, defamatory, obscene, indecent, offensive, or harassing, or transmissions of messages that disclose personal information about others without authorization, is strictly prohibited. NOTE: Someone other than the person(s) to whom you send them may read your e-mail messages. All messages should be courteous, professional and business like; "Flaming" (posting an e-mail message intending to insult and provoke) is prohibited. Be polite, act in a professional and courteous manner, using appropriate language at all times. Use caution when sending "joking" or humorous messages since intended sarcasm can be lost without facial expressions or voice intonations. Use discretion and common sense at all times. If you have any reservation whatsoever concerning the appropriateness of a message, you should refrain from sending it.

6.7. Natural Disaster Preparations

- 6.7.1. Every General Manager will survey their location for the potential of mishaps caused by human error or an act of God. Once all reasonable potential problems have been reviewed, the General Manager will cause an action plan to be written on how to deal with the problem(s) and notify employees of what actions to take.
- 6.7.2. Location specific will include, but not limited to the following:
 - 6.7.2.1. Hurricanes
 - 6.7.2.2. Floods
 - 6.7.2.3. Nuclear Power Plants
 - 6.7.2.4. Cyclones/Tornados
 - 6.7.2.5. Earthquakes
 - 6.7.2.6. Brush Fires
 - 6.7.2.7. Adverse Weather Conditions (Heavy Snow Fall, Extreme Heat, etc.)
- 6.7.3. These procedures will supplement the branch locations overall safety and security plan. All plans must be on file and approved by the Corporate Safety Department.

6.8. Threat Level Operating Procedures

- 6.8.1. Threat Level Security - Loss Prevention and Security Plan Summary
 - 6.8.1.1. The various Threat Level Procedures are cumulative and based on general awareness training for groups of employees that are job specific and detailed in the Plan itself.
 - 6.8.1.2. All employees undergo general security and awareness training for recognition and reporting of suspicious activity, proper employee identification requirements, and understanding changes in customer freight shipping and receiving procedures based on different National Threat Levels.
 - 6.8.1.3. Additional driver awareness training includes en route cargo security procedures including hijacking recognition, use of safe havens, trailer securement (locking) procedures, and theft reporting procedures for the quickest possible asset recovery.
 - 6.8.1.4. Additional Facility personal awareness training includes site security measures for the building and all equipment in the yard, customer contact monitoring for changes in customer shipment and receiving procedures

that are based on different Threat Levels, and the establishment of a Control Center of Senior Management to coordinate emergency procedures.

- 6.8.1.5. The following “Threat Level Security” color codes shall correspond to the National color code scheme and will activate as the National threat security level color changes for the United States.
- 6.8.1.6. In the event of an emergency, drivers may find cellular communications inoperable. If this is the case, drivers will landline their dispatchers ASAP, or head to the nearest PEI agent and **SEEK** further instructions from their dispatcher.

Threat Level Security

Status	Drivers & Employees	En route Freight	Branch Locations	Cyber/Information Systems
GREEN (Low)	NORMAL	NORMAL	NORMAL	NORMAL
BLUE (Guarded)	NORMAL	NORMAL	NORMAL	NORMAL
YELLOW (Elevated)	NORMAL	NORMAL	NORMAL	NORMAL
ORANGE (High)	<ol style="list-style-type: none"> 1. Safety to contact all drivers and e-mail all Branches with advisory with Threat Level Status change to ORANGE-HIGH or higher. 2. Branch Management to e-mail all branch employees and notify local branch drivers with the Threat Level Status change. 3. Review Emergency Response Communications with Drivers 4. Remind all drivers to exercise patience and expect delays in picking up or delivering freight due to heightened security. 5. Heighten awareness - immediately report any suspicious activity. 6. Drivers <u>MUST</u> be parked in well-lighted areas <u>ONLY</u> where truck is visible at all times. 	<ol style="list-style-type: none"> 1. Heighten awareness to report any suspicious activity. 2. Operations check for local changes in shipper's inbound security procedures. 3. Operations check for local changes in consignee freight acceptance procedures. 4. Operations will notify all facilities of any changes in customer's freight pick-up or acceptance procedures. 5. Reinforce and post Company policy to keep trailers locked at all times 6. Immediately contact Operations for missing equipment or critical freight issues. Fleet & Safety Dept will notify branches nationwide and see that the appropriate Law Enforcement agency is notified. 	<ol style="list-style-type: none"> 1. Post the Threat Level Status in operations, maintenance, dock, customer service, and cafeteria. 2. Heighten awareness to report any suspicious activity. 3. Review Emergency Response Communications with branch personnel. 4. Reinforce and post Company policy to keep trailers locked upon departure. 5. Visually verify that all trailers locked upon departure. 6. Verify positive identification of all guest and visitors. 7. Immediately report suspicious activities to your supervisor for assessment and notification to the proper authorities. 	<ol style="list-style-type: none"> 1. Heighten awareness to report any suspicious activity. 2. Monitor for attempted cyber security breach attempts.
RED (High) Complete actions at lower level	<ol style="list-style-type: none"> 1. Verify positive ID of all employees entering company property. 2. Comply with all route restrictions per regional and local authorities. 3. Keep equipment in site at all times. 4. Drivers must park in secure areas <u>ONLY</u>. 	<ol style="list-style-type: none"> 1. Operations will notify all facilities of any additional changes received regarding customers freight pick-up acceptance procedures. 	<ol style="list-style-type: none"> 1. Reserve the right to refuse new loads until the new customer has been verified. 2 Close all dock doors not in use. 3. Prohibit any visitors without an escort. 4. Establish a Control Center for Senior Management to coordinate and emergency procedure. 5. Inspect and verify that all incoming and departing trailers are locked. 	<ol style="list-style-type: none"> 1. Post Members Only updates for customers specific needs on the Company Intranet / WEB Site. Post updates on restricted driver, freight pick-up or delivery issues.

Threat Level Security

Risk of Attack	Recommended Actions
LOW (Green)	<ul style="list-style-type: none"> ❑ Obtain a copy of Terrorism: Preparing for the Unexpected brochure from you local Red Cross Chapter. ❑ Develop a personal disaster plan and disaster supplies kit using Red Cross brochures Your Family Disaster Supplies Kit. ❑ Examine volunteer opportunities in your community; choose an agency to volunteer with and receive training. ❑ Take a Red Cross CPR/AED and first aid course.
BLUE (Guarded)	<p>Complete actions at lower level</p> <ul style="list-style-type: none"> ❑ Be alert to suspicious activity and report it to the proper authorities. ❑ Review stored disaster supplies and replace items that are outdated. ❑ Develop emergency communications plan with family/neighbors/friends. ❑ Provide volunteer services and take advantage of additional volunteer training opportunities.
YELLOW (Elevated)	<p>Complete actions at lower level</p> <ul style="list-style-type: none"> ❑ Be alert to suspicious activity and report it to the proper authorities. ❑ Ensure disaster supplies kit is stocked and ready. ❑ Check telephone numbers and e-mail addresses in your personal communications plan and update as necessary. ❑ Develop alternate routes to/from work/school and practice them. ❑ Continue to provide volunteer services.
ORANGE (High)	<p>Complete actions at lower level</p> <ul style="list-style-type: none"> ❑ Be alert to suspicious activity and report it to the proper authorities. ❑ Review your personal disaster plan. ❑ Exercise caution when traveling. ❑ Have shelter in place, materials on hand, and review a copy of Terrorism: Preparing for the Unexpected brochure. ❑ If a need is announced, donate blood at designated blood collections centers. ❑ Prior to volunteering, contact agency to determine their needs.
RED (High)	<p>Complete actions at lower level</p> <ul style="list-style-type: none"> ❑ Listen to radio/TV for current information/instructions. ❑ Be alert to suspicious activity and report it to the proper authorities. ❑ Contact business to determine status of workday. ❑ Adhere to any travel restrictions announced by local governmental authorities. ❑ Be prepared to shelter in place or evacuate if instructed to do so by local government authorities. ❑ Provide volunteer services only as requested.