

1. Administration and Management

- 1.1 Secure Business Foundation
 - 1.1.1 Organization properly formed.
 - 1.1.2 Organization properly licensed and permitted.
 - 1.1.3 Organization officers/owners identified.
 - 1.1.4 Organization management structure identified.
 - 1.1.4.1 Primary and secondary persons with responsibility for operations.
 - 1.1.4.2 Primary and secondary persons with responsibility for financial processes.
 - 1.1.4.3 Primary and secondary persons with responsibility for security.
 - 1.1.4.4 Primary and secondary persons with responsibility for regulatory compliance.

- 1.2 Secure Business Policy
 - 1.2.1 Published throughout the organization.
 - 1.2.2 Clearly states top level management commitment.
 - 1.2.3 Clearly states opposition to terrorism, drug trafficking and other criminal activity.
 - 1.2.4 Clearly states commitment to regulatory compliance.
 - 1.2.5 The business uses a documented Risk Assessment/Hazard Analysis approach to develop policies and procedures.
 - 1.2.6 The business documents a process approach to secure commerce, considering the operation of each process, the process inputs and outputs and the interrelation with other processes.

- 1.3 Secure Business Procedures
 - 1.3.1 All procedures are documented and available to the process owner.
 - 1.3.2 Procedures are supported by training.
 - 1.3.3 Security procedures are integrated into standard procedures structure (ISO manual, operating guide, etc)
 - 1.3.4 Procedural change processes are documented, and include version management/verification.
 - 1.3.5 The results of the security process are integrated into existing documents as much as possible.
 - 1.3.6 Exceptions or discrepancies uncovered by the security process are documented and investigated, and are reported as necessary.
 - 1.3.7 Plans and procedures are in place to respond to failures in the security process.

International Organization for Secure Commerce

Secure Commerce Protocols™

- 1.3.8 Failures of the security process are documented, and remedial action is taken.
- 1.4 Management Review
 - 1.4.1 The management of the business reviews the adequacy of the secure commerce processes annually at a minimum. Inputs to management review will include the results of internal and external audits, non-conformances encountered, adequacy of the current policies and procedures, training status, loss of security devices (ID badges, keys, e-entry cards, etc.), regulatory changes that impact the secure commerce processes and other applicable inputs.]
 - 1.4.2 Reported security incidents will be reviewed on a regular basis. The timing of the review should be consistent with the severity of the incident.
- 1.5 Document Control
 - 1.5.1 Clear instructions are available for every document or form used in the business cycle.
 - 1.5.2 Examples or templates are available to indicate proper form and document usage.
 - 1.5.3 Examples and template are protected from theft or tampering.
 - 1.5.4 Procedures for document use include techniques to prevent unauthorized changes, additions or deletions.
 - 1.5.5 Procedures for each document or form include instructions on completion and disposition of the form.
 - 1.5.6 Each form indicates the name of the person who filled it out.
 - 1.5.7 Adequate secure document storage capacity available.
 - 1.5.8 Procedures in place for approving changes in document format or procedure.
 - 1.5.9 Information system support for document preparation requires authentication.
 - 1.5.10 Information system support for document preparation serves to help reduce errors.
 - 1.5.11 Document version control procedures are in place.
- 1.6 Financial Controls
 - 1.6.1 The primary financial officer or manager for the facility or organization is clearly identified.
 - 1.6.2 Operational functions which generate a financial transaction are identified and documented.
 - 1.6.3 Clear procedures are in place for the reporting of financial transactions.

International Organization for Secure Commerce
Secure Commerce Protocols™

- 1.6.4 There is a procedure in place for regular financial audit.
- 1.6.5 There is a procedure in place for employees to report financial irregularities or misconduct.

2. Facilities Security

- 2.1 Secure Facilities Management
 - 2.1.1 Manager responsible for facility security identified.
 - 2.1.2 Published facilities security policy identifying program goals.
 - 2.1.3 Established process for ongoing risk assessment and procedure development.
 - 2.1.4 Security procedures published and available to process owners.
 - 2.1.5 Ongoing facility security training program for employees.
 - 2.1.6 Procedures are in place to identify, challenge and remove employees or visitors who are violating access control restrictions.
 - 2.1.7 Maps/blueprints are available for the facility.
 - 2.1.7.1 Property perimeter and fence lines identified.
 - 2.1.7.2 Perimeter and fencing access/entry points identified.
 - 2.1.7.3 Secure perimeter areas identified.
 - 2.1.7.4 Building layout with all interior areas identified
 - 2.1.7.5 High value, high security and hazardous material areas identified.
 - 2.1.7.6 All doors, windows, closets, and utility connection points indicated.
 - 2.1.7.7 Easements or common/shared areas.
 - 2.1.7.8 The confidentiality of map/blueprint documents is maintained.
 - 2.1.8 Restricted areas are identified and controlled appropriately as necessary to carry out the business policies and procedures.
 - 2.1.8.1 High value materials
 - 2.1.8.2 Restricted processes or property
 - 2.1.8.3 No Foreign Nationals restricted
 - 2.1.8.4 Hazardous materials or processes
 - 2.1.8.5 In-bond or other restricted storage
 - 2.1.9 Procedures are in place for ordering, maintaining and tracking the locks, keys or other materials necessary for operating the facility's access controls.
 - 2.1.9.1 Positive control by management and/or security personnel.
 - 2.1.9.2 Ability to identify all persons with access to any specific area.
 - 2.1.9.3 'Lost key' reporting and response procedures.
 - 2.1.10 Security response personnel are identified and available 24 hours a day.
- 2.2 Perimeter Control

International Organization for Secure Commerce

Secure Commerce Protocols™

- 2.2.1 Facility perimeter identified.
 - 2.2.2 Secure perimeter areas identified.
 - 2.2.2.1 Access points for entry and exit.
 - 2.2.2.2 Cargo handling areas
 - 2.2.2.3 Cargo storage areas, including hazmat and high value.
 - 2.2.2.4 Utility service points (power, water, communications)
 - 2.2.2.5 Public parking.
 - 2.2.2.6 Employee parking.
 - 2.2.3 Secure perimeter areas segregated, access controlled and monitored.
 - 2.2.4 Number of perimeter gates kept to the minimum required for access and safety.
 - 2.2.5 Perimeter entrance control.
 - 2.2.5.1 Procedure for identifying and logging persons entering the secure perimeter.
 - 2.2.5.2 Procedure for access control and logging of ALL vehicles entering the secure perimeter.
 - 2.2.5.3 Procedure for inspecting vehicles or persons entering the secure perimeter.
 - 2.2.6 Perimeter exit control.
 - 2.2.6.1 Procedure for identifying and logging persons exiting the secure perimeter
 - 2.2.6.2 Procedure for logging ALL vehicles exiting the secure perimeter.
 - 2.2.6.3 Procedure for inspecting vehicles or persons exiting the secure perimeter.
 - 2.2.7 Procedure for proper collection, storage and review of entry and exit logs, inspection reports, and other secure perimeter control documents.
- 2.3 External Security
- 2.3.1 Facility construction resists unauthorized entry.
 - 2.3.2 Facility walls and roof routinely inspected and maintained.
 - 2.3.3 Security cameras and alarm systems used for perimeter control are monitored and maintained.
 - 2.3.4 Fencing and gates are routinely inspected and maintained.
 - 2.3.5 Perimeter and exterior lighting sufficient to identify unauthorized access.
 - 2.3.6 Perimeter and exterior visibility sufficient to identify unauthorized access.
 - 2.3.7 External windows are closed and secured.
 - 2.3.8 Auxiliary/emergency entrances/exits are secured and controlled with appropriate locking devices or alarms.
 - 2.3.9 Emergency exits are properly controlled.

International Organization for Secure Commerce

Secure Commerce Protocols™

- 2.3.10 External supply or utility closets are secured.
- 2.3.11 Procedure exists for regular verification of external security items.
- 2.3.12 All checks and verification are documented.

- 2.4 Facility Access Control
 - 2.4.1 All facility access points are access controlled.
 - 2.4.2 Employee entrance(s) are access controlled and are secured when not in use.
 - 2.4.3 Positive identification is required for employee access to secure perimeter or facility interior.
 - 2.4.4 Access point for non-employees is access controlled and is secured when not in use.
 - 2.4.5 Access controls, alarms and monitoring devices are regularly tested and maintained.

- 2.5 Internal Boundaries and Security
 - 2.5.1 Internal access is controlled.
 - 2.5.2 Internal areas are controlled appropriately and are identified as necessary to carry out the business policies and procedures.
 - 2.5.3 Employees are authorized access to only those areas needed for the performance of their duties.
 - 2.5.4 Authorized access indicated by color coded ID badges or garments, by job description, or by other appropriate means.
 - 2.5.5 Emergency lighting is installed in hallways and at exits.
 - 2.5.6 All public areas such as reception areas, waiting rooms and public restrooms are separated from all other areas and monitored.
 - 2.5.7 Employee restrooms, locker-rooms, cafeterias and break areas are separated from shipping, receiving, storage and production areas.
 - 2.5.8 Areas such as phone closets, server rooms and network relays are protected by access controls.

- 2.6 Visitors, Vendors and Service Providers
 - 2.6.1 Security policy for visitors, vendors and service providers is posted at all entrances or communicated to the visitor prior to their arrival.
 - 2.6.2 A visitors procedures must be in place which includes:
 - 2.6.2.1 Mandatory sign in at the reception area or other designated location.
 - 2.6.2.2 Positive identification via picture ID.

- 2.6.2.3 Logging of employer, reason for the visit and the name of the person they are to visit.
- 2.6.2.4 Mandatory use of ID badges clearly indicating their visitor status.
- 2.6.2.5 Identification and control of individuals that may be restricted from certain areas based on nationality, employer or other additional risk factors.
- 2.6.2.6 Mandatory escort by trained personnel while on premises
- 2.6.2.7 Mandatory sign out and recovery of visitor credentials at end of visit.
- 2.6.2.8 Secure storage and regular review of visitor log.
- 2.6.3 Visitor procedures may include different categories of visitor with differing security procedures based on risk and training.
- 2.6.4 Procedures must be in place for safely identifying, challenging and removing unescorted and/or unidentified visitors.

3. Personnel Security

- 3.1 Personnel Security Management
 - 3.1.1 Manager responsible for personnel security identified.
 - 3.1.2 Published personnel security policy identifying program goals.
 - 3.1.3 Established process for ongoing risk assessment and procedure development.
 - 3.1.4 Personnel security procedures published and available to process owners.
 - 3.1.5 Ongoing personnel security training program.
 - 3.1.6 Personnel security procedures and practices are reviewed for compliance with appropriate regulatory and contractual obligations.
 - 3.1.7 Procedures include documentation of all steps and results in the employment cycle.
 - 3.1.8 Procedures exist for safeguarding employee data from disclosure.
 - 3.1.9 Positions with a high impact on security are identified.
 - 3.1.10 Personnel records contain complete information including:
 - 3.1.10.1 Name, address, phone
 - 3.1.10.2 Emergency contact information
 - 3.1.10.3 Physical description
 - 3.1.10.4 Picture
 - 3.1.10.5 Signature
 - 3.1.10.6 Fingerprints
 - 3.1.10.7 Optional emergency health information provided by employee.
 - 3.1.11 Documented procedure for use of identification badges
 - 3.1.11.1 Used to positively identify employees and provide access control.
 - 3.1.11.2 Include name, picture and job description.
 - 3.1.11.3 Includes documentation of any applicable color coding or formatting restrictions.
 - 3.1.11.4 Complete logging of ID badge issuance, revocation or loss report.
 - 3.1.11.5 Restricted access to ID badge materials, equipment and records.
 - 3.1.12 Procedures to restrict and log access to uniforms and other company issued employee materials.
- 3.2 Hiring Practices
 - 3.2.1 Prospective employees are informed of the personnel security procedures that will be used.
 - 3.2.2 Established procedure for application processing.

- 3.2.2.1 Use of standardized application for all applicants.
- 3.2.2.2 Application completed on-site.
- 3.2.2.3 Blank applications are not distributed.
- 3.2.2.4 Completed applications safeguarded to preserve integrity and confidentiality.
- 3.2.3 Procedures for application review that include, on a risk assessment basis, the following:
 - 3.2.3.1 All personal information on the application verified with appropriate documentation.
 - 3.2.3.2 Verification of all education, certification, previous employment and references.
 - 3.2.3.3 Pre-employment criminal background investigation.
 - 3.2.3.4 Pre-employment drug screening.
 - 3.2.3.5 Pre-employment credit check to establish baseline.
 - 3.2.3.6 Pre-employment interview by trained personnel.
- 3.2.4 Procedures for applicant interviews
 - 3.2.4.1 Interviews performed by trained personnel.
 - 3.2.4.2 Interview procedures comply with applicable laws and regulations.
 - 3.2.4.3 Interview procedures protect the safety of the interviewer.
- 3.3 Employee Provisioning
 - 3.3.1 Procedure for new employee orientation and training including:
 - 3.3.1.1 Organization security policies and procedures.
 - 3.3.1.2 Position specific security policies and procedures.
 - 3.3.1.3 Threat awareness briefing
 - 3.3.1.4 Security issue reporting procedures
 - 3.3.1.5 Emergency procedures
 - 3.3.2 Procedure for issuance of identification.
 - 3.3.3 Procedure for issuance of computer and/or communications equipment, passwords, accounts, etc.
 - 3.3.4 Provisioning procedures document performance of and employee acceptance of provisioning process.
- 3.4 Ongoing personnel security
 - 3.4.1 Random drug testing.
 - 3.4.2 Periodic updates to credit check and criminal background investigation consistent with risk assessment.
 - 3.4.3 Annual updates to employee data
 - 3.4.4 Comparison of updated employee data to baseline.
 - 3.4.5 Procedure for post-incident/post-accident drug testing and investigation.

- 3.4.6 Procedures for collecting and investigating information on employee misconduct.
- 3.4.7 Periodic replacement of all security badges, with format change.
- 3.4.8 Incentives for employees who actively participate in security and compliance programs.
- 3.4.9 Ongoing security training
 - 3.4.9.1 Threat awareness
 - 3.4.9.2 Policy and procedures
 - 3.4.9.3 Recognition of behavior changes and anomalies.
- 3.5 Termination and De-Provisioning Practices
 - 3.5.1 Use of standardized form to record details of termination.
 - 3.5.2 Procedure for exit interview which includes:
 - 3.5.2.1 Explanation of termination process.
 - 3.5.2.2 Recovery of identification card.
 - 3.5.2.3 Recovery of computer or communications equipment.
 - 3.5.2.4 Recovery of keys, credit cards or other company materials.
 - 3.5.2.5 Identification of all un-recovered materials.
 - 3.5.2.6 Documentation of entire exit interview process.
 - 3.5.3 Termination procedure includes:
 - 3.5.3.1 Steps to insure de-provisioning/de-activation of access codes, email accounts, passwords, etc.
 - 3.5.3.2 Escort of terminated employee while on premises.
 - 3.5.3.3 Notification of proper internal or external personnel.
 - 3.5.4 Procedures protect HR personnel during termination and de-provisioning process.

4. Warehouse Operations

- 4.1 Secure Warehouse Operations Management
 - 4.1.1 Manager responsible for warehouse security identified.
 - 4.1.2 Published warehouse security policy identifying program goals.
 - 4.1.3 Established process for ongoing risk assessment and procedure development.
 - 4.1.4 Security procedures published and available to process owners.
 - 4.1.5 Ongoing warehouse security training program for employees.
 - 4.1.5.1 Container inspection training
 - 4.1.5.2 Security seal procedures training
 - 4.1.5.3 Threat awareness training
 - 4.1.5.4 Security risk identification and reporting training
 - 4.1.5.5 Training in the security aspects of each position.
 - 4.1.6 All shipments, receipts and storage activities are documented.
 - 4.1.7 Procedures are in place to ensure information on inbound and outbound international shipments is reported in an accurate and timely manner.
 - 4.1.8 Participation of drivers and other third parties in the shipping, receiving or storage process is controlled and documented.
- 4.2 Material Segregation and Identification
 - 4.2.1 All materials are clearly identified.
 - 4.2.2 Shipping, receiving, production, and storage areas are segregated.
 - 4.2.3 Material segregation is enforced consistent with risk assessment, and considering:
 - 4.2.3.1 Raw material segregated from finished goods.
 - 4.2.3.2 Segregation of high value materials
 - 4.2.3.3 Segregation of hazardous materials
 - 4.2.3.4 Segregation of unidentified materials
 - 4.2.3.5 Segregation of materials pending disposition
 - 4.2.4 Access to each segregated area is controlled and monitored.

- 4.3 Receiving Procedures
 - 4.3.1 Driver identification required before accepting shipment.
 - 4.3.2 Cargo manifest must be present, complete and legible.
 - 4.3.3 Shipments from unknown locations or parties, or with unknown contents, are refused or isolated pending resolution.
 - 4.3.4 Container seal is inspected and compared to seal number on manifest, and any discrepancy noted.
 - 4.3.5 Shipments with improper documentation or seal discrepancies are refused or isolated until resolved.
 - 4.3.6 Security seal discrepancies are reported to appropriate law enforcement or customs officials.
 - 4.3.7 Deviations from standard practices in container loading/stuffing are noted.
 - 4.3.8 Container contents are verified against cargo manifest.
 - 4.3.9 Discrepancies in content, weight, quantity, marking or packaging are documented.
 - 4.3.10 Contraband or other illegal activities are documented and reported to appropriate law enforcement officials.
 - 4.3.11 Cargo shrinkage or theft is reported as appropriate.
 - 4.3.12 Discrepancies found in the receiving process are investigated until resolved.
 - 4.3.13 Mail and small package deliveries are screened prior to internal distribution.
 - 4.3.14 Unidentified receipts, packages or mail are isolated until an appropriate disposition is made.
 - 4.3.15 Hazardous materials are handled as appropriate.
 - 4.3.16 Receiving documentation includes name(s) and signature(s) of all involved.

- 4.4 Storage Procedures
 - 4.4.1 Storage of materials takes place only after all receiving procedures are complete.
 - 4.4.2 Priority is given to correct storage of hazardous and high value materials.
 - 4.4.3 Materials are properly stored in an access controlled area until they are ready for shipment.
 - 4.4.4 Material stored in a trailer or container:
 - 4.4.4.1 The contents are fully documented
 - 4.4.4.2 The container is sealed
 - 4.4.4.3 The container is stored in a secure area with access control and monitoring.
 - 4.4.5 Empty trailer and container storage

- 4.4.5.1 Stored in a secure area with access control and monitoring.
 - 4.4.5.2 Isolated from casual access.
 - 4.4.5.3 Inspected regularly.
- 4.5 Shipping Procedures
- 4.5.1 All shipping containers/trailers/trucks inspected before use.
 - 4.5.1.1 7-point: front wall, left side, right side, roof/ceiling, doors inside/outside, exterior/undercarriage
 - 4.5.1.2 Locking/latching mechanism.
 - 4.5.1.3 Signs of recent repair or modification.
 - 4.5.2 Shipping documentation is complete, legible and accurate.
 - 4.5.3 Computer systems and data used to prepare shipping documents is protected from unauthorized physical or electronic access.
 - 4.5.4 Shipping data is verified against the appropriate purchase order or delivery order where possible.
 - 4.5.5 Shipping documents are protected against loss and unauthorized disclosure or modification.
 - 4.5.6 Physical counts, weights and labeling are verified as the container is loaded/stuffed.
 - 4.5.7 The trailer is sealed in accordance with the seal procedure.
 - 4.5.8 Seal number noted on the shipping documentation and the seal log.
 - 4.5.9 High security seals used for at-risk shipments.
 - 4.5.10 Drivers are properly identified before they are allowed to pickup the shipment.
 - 4.5.11 Shipping documents should include name(s) and signature(s) of all involved.
 - 4.5.12 Packing materials are inspected prior to use.
- 4.6 Seal Management Program
- 4.6.1 Tamper evident seals are used to secure every container.
 - 4.6.2 High security seals (ISO PAS 17712) should be used for every international or high risk shipment.
 - 4.6.3 Documented procedures in place for controlling and applying seals to containers.
 - 4.6.4 Documented procedures for recognizing a compromised seal and reporting it to the proper authorities.
 - 4.6.5 Documented procedures reporting missing seals to the proper authorities.
 - 4.6.6 Procedures for storing seals in a safe, accountable, access controlled manner.

- 4.6.7 Seals distributed and logged only by authorized personnel.
- 4.6.8 Procedures for handling sealed containers that are in transit.
- 4.6.9 Procedures for reporting, refusal, and resealing of containers with missing or compromised seals.

5. Secure Transportation Operations

- 5.1 Secure Transportation Operations Management
 - 5.1.1 Manager responsible for transportation security identified.
 - 5.1.2 Published transportation security policy identifying program goals.
 - 5.1.3 Established process for ongoing risk assessment and procedure development.
 - 5.1.4 Security procedures published and available to process owners.
 - 5.1.5 Ongoing transportation security training program for employees.
 - 5.1.5.1 Container and vehicle security inspection.
 - 5.1.5.2 Threat awareness
 - 5.1.5.3 Threat recognition and response.
 - 5.1.5.4 Preventive container and vehicle inspections for maintenance and regulatory compliance.
 - 5.1.5.5 Seal management program
 - 5.1.6 Procedure for recording and documenting condition of and repairs to containers and conveyance.
 - 5.1.7 Procedures for reporting and responding to accidents or incidents during transportation activities.
 - 5.1.8 Transportation involving passengers should include security screening of all passengers and crew.
 - 5.1.9 Transportation involving passengers should include procedures controlling access to cargo during transit.
 - 5.1.10 Ongoing communications between transportation user and provider with regard to security issues.
- 5.2 Inspection of Containers and Conveyance
 - 5.2.1 All inspections follow established procedure and are documented.
 - 5.2.2 Inspection procedures include basic safety and compliance items.
 - 5.2.3 Security inspection of containers/trailers uses procedure which meets or exceeds 7 point inspection standard.
 - 5.2.4 Specified conditions are defined for requiring a container not be used.

International Organization for Secure Commerce
Secure Commerce Protocols™

- 5.2.5 Established procedure for the security inspection of vehicles.
- 5.2.6 Security inspection procedure for passenger baggage.
- 5.2.7 Container inspections occur before filling/stuffing, after unloading, and when receiving an empty from storage or service provider.
- 5.2.8 Net and gross weight of vehicles and containers are recorded.
- 5.2.9 Receipt of containers and trailers is accepted only from approved parties.

- 5.3 Tracking and security methods
 - 5.3.1 All vehicles and containers checked and logged as they enter and exit the secure perimeter.
 - 5.3.2 Each movement of a container or conveyance is documented.
 - 5.3.2.1 Documented by facility personnel
 - 5.3.2.2 Documented by driver
 - 5.3.3 Use of 'known location' methodology
 - 5.3.3.1 Customers provide transport vendors with list of locations valid for pickup or delivery.
 - 5.3.3.2 Procedure established for adding or removing locations.
 - 5.3.3.3 Loads are not picked up from or delivered to locations not on the list.
 - 5.3.3.4 Deviations from customers known shipping or receiving procedures are recorded by driver.
 - 5.3.4 Technological, physical and statistical tracking systems are used via established procedures.
 - 5.3.4.1 GPS
 - 5.3.4.2 Check points
 - 5.3.4.3 Convoys/escorts
 - 5.3.4.4 Dog screening
 - 5.3.4.5 Route timing
 - 5.3.4.6 Call in schedule
 - 5.3.4.7 Other methods
 - 5.3.5 Ongoing process of shipment risk assessments (dwell time analysis, lane segment history, transit times, etc)
- 5.4 Regulatory Inspections
 - 5.4.1 Procedure for compliance inspection of containers and vehicles, including:
 - 5.4.1.1 Required equipment
 - 5.4.1.2 Equipment condition
 - 5.4.1.3 Licensing
 - 5.4.1.4 Permits
 - 5.4.1.5 Program participation/registration
 - 5.4.2 Training for maintenance personnel on required equipment maintenance and standards.
 - 5.4.3 Procedures to report and respond to delays or detention due to compliance problems.
- 5.5 Seal Management
 - 5.5.1 Refer to Section 4.6

6. Utilities, Systems and Communications (USC)

- 6.1 Utilities, Systems and Communication Security Management
 - 6.1.1 Manager(s) identified with responsibility for:
 - 6.1.1.1 Utilities security
 - 6.1.1.2 Information systems security
 - 6.1.1.3 Communications security.
 - 6.1.2 Published USC security policies identifying program goals, including:
 - 6.1.2.1 Acceptable use policy for information systems.
 - 6.1.2.2 Acceptable use policy for communications.
 - 6.1.2.3 Email ownership and retention policy.
 - 6.1.2.4 Security policy for remote system access.
 - 6.1.3 Established process for ongoing risk assessment and procedure development.
 - 6.1.4 Security procedures published and available to process owners.
 - 6.1.5 Ongoing utilities, systems and communication security training program for employees.
 - 6.1.5.1 Threat awareness.
 - 6.1.5.2 Acceptable use.
 - 6.1.5.3 Basic security practices.
 - 6.1.5.4 Position specific security practices.
 - 6.1.6 Up-to-date inventory of equipment for utilities, information systems, communications and other systems
 - 6.1.7 Recovery procedures include verification that critical systems are again functioning properly.
 - 6.1.8 Procedures are in place for operations during a failure of any utility and/or communication systems that maintain the integrity of the security processes.
 - 6.1.9 Procedures for re-securing any areas which may have had a security breach due to loss of utilities or other systems.
 - 6.1.10 Procedures for regular testing of backup, emergency, offsite or failover systems.
- 6.2 Protecting Information Systems
 - 6.2.1 Servers, data lines, routers and other IS equipment physically protected from unauthorized access.
 - 6.2.2 Unused network or modem ports deactivated.
 - 6.2.3 Monitoring for unauthorized equipment (wireless, personal, etc.)
 - 6.2.4 Visitors are not left unescorted in the presence of active IS equipment.
 - 6.2.5 IS vendors and third party maintenance personnel are

- 6.2.5.1 Positively identified.
 - 6.2.5.2 Continuously escorted.
 - 6.2.6 Third parties with systems or data access have a privacy agreement in place.
 - 6.2.7 Hardware and software security measures in place consistent with risk of unauthorized access:
 - 6.2.7.1 Firewalls
 - 6.2.7.2 VPNs
 - 6.2.7.3 IPS/IDS systems
 - 6.2.7.4 Penetration testing
 - 6.2.7.5 System security audits
 - 6.2.8 Backup power to maintain critical systems for controlled shutdown.
 - 6.2.9 Procedures in place for routine backup and offsite storage of mission critical data.
 - 6.2.10 Procedures in place for emergency replacement of mission critical equipment.
 - 6.2.11 Procedures in place for restoration of data from backups.
 - 6.2.12 Procedures for erasure of data from equipment being retired, repurposed, replaced or donated.
 - 6.2.13 Procedures in place to insure systems are updated, patched and virus protected.
- 6.3 Information access control
- 6.3.1 User id's and passwords used to control access to information systems.
 - 6.3.2 Users have least privileges necessary to adequately perform their jobs.
 - 6.3.3 Information systems have audit procedures in place to identify user, date and time for any data entry or modification.
 - 6.3.4 Procedures in place to deactivate the user id and password of any terminated employee.
 - 6.3.5 Password policy and controls include standards for password strength and expiration.
 - 6.3.6 Lost password procedure includes positive identification of the user before issuing a new password.
 - 6.3.7 Logging of production or transmission of sensitive reports, data or forms.
- 6.4 Communication Security
- 6.4.1 Established procedure for use of communications facilities, including:

- 6.4.1.1 Telephone systems
- 6.4.1.2 Paging/announcing system
- 6.4.1.3 Cellular phones
- 6.4.1.4 2-way radios
- 6.4.1.5 Instant messaging/text messaging.
- 6.4.1.6 Satellite communications
- 6.4.2 Emergency communications procedures in case of phone system outage.
- 6.4.3 Procedures for taking and handling information requests over the phone.
 - 6.4.3.1 Identification of public vs. private information
 - 6.4.3.2 Resistance to social engineering
- 6.5 Utility Security
 - 6.5.1 Identification of all on premises utility connection points.
 - 6.5.2 Established conditions and procedures for emergency shutdown of utilities.
 - 6.5.3 Procedures and contact information for contacting utility providers to shutdown, service or restart utilities.
 - 6.5.4 Established procedures to respond to utility outages.
 - 6.5.5 Emergency lighting in critical areas.
 - 6.5.6 Established procedures for utility service resumption including:
 - 6.5.6.1 Safe restart of machinery or other devices
 - 6.5.6.2 Verification that critical systems are functioning
 - 6.5.6.3 Identification of failed backup or failover systems.
- 6.6 Other Systems
 - 6.6.1 Identification of other systems used on premises:
 - 6.6.1.1 Alarm system
 - 6.6.1.2 Video surveillance
 - 6.6.1.3 Time and attendance
 - 6.6.1.4 Fire alarm and suppression
 - 6.6.1.5 Access control
 - 6.6.1.6 TV/digital satellite
 - 6.6.1.7 Music
 - 6.6.2 Security risk assessment for each system.
 - 6.6.3 Procedures for operating during outages of each system.
 - 6.6.4 Procedures for verifying function upon restoration of each system.

7. Secure Partnerships

7.1 Managing Secure Partnerships

- 7.1.1 Manager(s) responsible for security partnerships identified.
- 7.1.2 Published security partnership policies identifying program goals, including committed regulatory partnerships.
- 7.1.3 Established process for ongoing risk assessment and procedure development.
- 7.1.4 Security procedures published and available to process owners.
- 7.1.5 Ongoing security partnership training program for employees, including
 - 7.1.5.1 Threat awareness
 - 7.1.5.2 Threat identification and reporting
- 7.1.6 Secure partnership program is applied to all business partners.

7.2 Supplier Screening

- 7.2.1 Publication of security requirements to current and potential suppliers.
- 7.2.2 Security screening & risk assessment incorporated into the supplier selection process:
 - 7.2.2.1 Verification of references
 - 7.2.2.2 Evaluation of internal controls.
 - 7.2.2.3 Evaluation of security program.
 - 7.2.2.4 Evaluation of credit & financial stability.
- 7.2.3 Procedure for regular supplier background/credit checks.
- 7.2.4 Suppliers are required to provide detail information on their internal security policies and procedures, including participation in any regulatory partnership programs.
- 7.2.5 Security requirements which apply to suppliers are included in any request for quotes or pricing.
- 7.2.6 Security requirements are included in contracts and agreements.
- 7.2.7 Established procedure for notifying supplier of non-compliance with security requirements.
- 7.2.8 Procedure to verify participation in regulatory partnership programs.
- 7.2.9 Procedure in place for regular supplier audits.
- 7.2.10 Procedure in place for regular supplier risk assessments.

- 7.3 Customer Screening
 - 7.3.1 Use of standardized form for collecting customer information.
 - 7.3.2 Verification of all information on customer form, including entity formation, officers/owner, physical location, and licenses or permits.
 - 7.3.3 Verification of potential customers against terrorist or export control watch lists.
 - 7.3.4 Regular update and verification of all client data.
 - 7.3.5 Procedure for providing customers with relevant details of security policies and procedures.
 - 7.3.6 All customer agreements include the security requirements of both parties.
 - 7.3.7 Procedure for notifying customer of changes to or violations of security policy or procedures.

- 7.4 Regulatory Partnerships
 - 7.4.1 Commitment to regulatory partnerships made at the policy level, backed by top-level management.
 - 7.4.2 Procedures for compliance with regulatory partnerships integrated into business process.
 - 7.4.3 Regular review and audit of partnership compliance.
 - 7.4.4 Regular evaluation of new partnership opportunities.

- 7.5 Partnership Development and Maintenance
 - 7.5.1 Procedure for regular contact with security partners.
 - 7.5.2 Bilateral partnership evaluation program.
 - 7.5.3 Cost effectiveness reviews of partnership programs.
 - 7.5.4 Commitment to fostering new partnerships with outside organizations for the purposes of increasing security.

8. Internal Audit

8.1 Managing Internal Security Audits

- 8.1.1 Independent manager responsible for security audits identified.
- 8.1.2 Published security audit policies identifying program goals.
- 8.1.3 Documented list of compliance items included in security items.
- 8.1.4 Security audit procedures published and available to process owners.
- 8.1.5 Ongoing security audit training program for employees.
- 8.1.6 Established program and procedures for security audits and corrective action.
 - 8.1.6.1 The audits will focus on the secure commerce processes as opposed to evaluating the elements of the security system.
- 8.1.7 Audit schedule(s) established based on risk assessments, with a one year maximum audit cycle.
 - 8.1.7.1 The scheduled audits are spread through the year
 - 8.1.7.2 One or more area/process covered on each audit.
 - 8.1.7.3 Changes or failure to comply with the schedule are documented and reported.

8.2 Auditor Roles and Responsibilities

- 8.2.1 The roles and responsibilities of internal security auditors are clearly defined.
- 8.2.2 Guidelines for handling of audit related data are published.
- 8.2.3 Established guidelines for determining the scope of each audit activity.
- 8.2.4 Published code of conduct for audit personnel.

8.3 Report Preparation

- 8.3.1 Established templates for reporting audit results.
- 8.3.2 Audit results are distributed only to stakeholders.
- 8.3.3 Report clearly states findings of fact without subjective opinions.

8.4 Follow-up and Review

- 8.4.1 Established procedure for follow-up audit scheduling and reporting.
- 8.4.2 Documented procedure for reviewing audit results.
- 8.4.3 Documented procedure for developing a corrective action/preventive action plan.

9. Emergency Response and Recovery

- 9.1 Managing Emergency Response and Recovery
 - 9.1.1 Manager responsible for emergency operations identified.
 - 9.1.2 Published policies for emergency and recovery situations.
 - 9.1.3 Emergency response procedures published and available to appropriate stakeholders.
 - 9.1.4 Ongoing emergency response and recovery training program for employees.
 - 9.1.5 Established program and procedures for review and update of emergency plans.
 - 9.1.6 Established emergency procedures based on business impact analysis for events including:
 - 9.1.6.1 Natural disaster
 - 9.1.6.2 Terrorist attack
 - 9.1.6.3 Prolonged utility outage
 - 9.1.6.4 Pandemic
 - 9.1.6.5 Loss of prime vendor
 - 9.1.6.6 Response to customer emergency
 - 9.1.7 An emergency evacuation plan is posted for each facility.
 - 9.1.8 An emergency communications plan is in place.
- 9.2 Emergency Plan
 - 9.2.1 A plan is in place for responding to emergency situations.
 - 9.2.2 The plan identifies the conditions that constitute an emergency.
 - 9.2.3 The plan identifies the chain of command for the duration of the emergency.
 - 9.2.4 The plan specifies and emergency notification procedure for management and employees.
 - 9.2.5 The plan identifies each individual's role for the duration of the emergency.
 - 9.2.6 Plans include contingencies for:
 - 9.2.6.1 Emergency facilities
 - 9.2.6.2 Emergency financing
 - 9.2.6.3 Emergency material replacement
 - 9.2.6.4 Emergency equipment replacement
 - 9.2.6.5 Emergency communications
 - 9.2.6.6 Restoration of IS data and services
 - 9.2.6.7 Safety of employees and visitors
 - 9.2.6.8 Security of organization assets during the emergency
 - 9.2.7 The plan identifies the conditions which indicate the end of the emergency.

- 9.3 Emergency Response Team
 - 9.3.1 Team(s) are formed to meet critical organization needs during an emergency:
 - 9.3.1.1 Relocation
 - 9.3.1.2 Replacement of equipment or materials
 - 9.3.1.3 Response to cyber attack or data loss
 - 9.3.1.4 Support of customers or vendors
 - 9.3.1.5 Financial support and operations
 - 9.3.1.6 General continuity of operations
 - 9.3.2 Team composition specified based on type of emergency and team goal.
 - 9.3.3 Each person on the emergency response team has a clearly defined role.
 - 9.3.4 Communications plan indicates how the team is activated.
 - 9.3.5 All stakeholders are notified of ERT's role and authority.
- 9.4 Emergencies and Regulatory/Law Enforcement Agencies
 - 9.4.1 Emergency plans include a comprehensive list of contacts and phone number for regulatory and law enforcement agencies.
 - 9.4.2 Emergency plans include policy and procedure for informing regulatory/law enforcement agencies based on the nature of the emergency.
 - 9.4.3 Policy indicates required cooperation with law enforcement during an emergency situation.

10. Secure Commerce Program

10.1 Managing the Secure Commerce Program

- 10.1.1 Manager responsible for the secure commerce program identified.
- 10.1.2 Published unified security policies identifying program goals.
- 10.1.3 Documented list of compliance items included in security program.
- 10.1.4 Security procedures published and available to process owners.
- 10.1.5 Ongoing secure commerce training program for employees.
- 10.1.6 Established program and procedures for ongoing risk assessments, including testing and evaluating security systems, emergency response and discrepancy procedures.
- 10.1.7 Policy and procedures are in place for collection and sharing of security related intelligence information.

10.2 Secure Business Process

- 10.2.1 Security processes and procedures are integrated into the business cycle.

10.3 Regulatory Footprint and Compliance

- 10.2.2 All regulatory compliance requirements for the organization have been identified.
- 10.2.3 Process owners have been identified for each compliance item.
- 10.2.4 An audit and review process is in place to verify compliance.
- 10.2.5 A procedure exists to report and correct incidents of non-compliance.

10.4 Policy and Procedure Management

- 10.2.6 A procedure is in place for recording, maintaining and disseminating the various company policies.
- 10.2.7 Security and compliance procedures are based on approved and support policy.
- 10.2.8 Security and compliance procedures are integrated with other business process procedures.
- 10.2.9 Procedures in place to allow employees to request a policy or procedure to be changed. This process includes risk analysis and change procedures.

10.5 Training and Education

10.2.10 An ongoing program of training and education is in place.

10.2.11 The training requirements of each job position are identified.

10.2.12 Training records are routinely reviewed to ensure employees are receiving the training indicated by their positions.

10.2.13 Training programs are reviewed to ensure they meet the current security and regulatory requirements.

10.2.14 Training programs should include:

10.2.14.1 Threat awareness.

10.2.14.2 Basic security procedures.

10.2.14.3 Social engineering resistance.

10.2.14.4 IT security training for information workers.

10.2.14.5 Recognizing internal conspiracies.

10.2.14.6 Maintaining perimeter and access control integrity.

10.2.14.7 Workplace safety and violence prevention.

10.2.14.8 Drug and alcohol awareness.