

## 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 Facility management identified.
  
- 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.
  
- 1.3 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.
  - 1.3.8 Failures of the security process are documented, and remedial action is taken.

- 1.4 Document Control
  - 1.4.1 Clear instructions are available for every document or form used in the business cycle.
  - 1.4.2 Examples or templates are available to indicate proper form and document usage. These examples should be protected from theft or tampering.
  - 1.4.3 Procedures for document use should include techniques to prevent unauthorized changes, additions or deletions.
  - 1.4.4 Procedures for each document or form should include instructions on completion and disposition of the form. Each form should also indicate the name of the person who filled it out.
  - 1.4.5 Adequate secure document storage capacity should be available.
  - 1.4.6 Procedures should be in place for approving changes in document format or procedure.
  - 1.4.7 Information system support for document preparation should require authentication, and should serve to help reduce errors.
  - 1.4.8 Document version control procedures are in place.
  
- 1.5 Financial Controls
  - 1.5.1 The primary financial officer or manager for the facility or organization is clearly identified.
  - 1.5.2 Operational functions which generate a financial transaction are identified and documented.
  - 1.5.3 Clear procedures are in place for the reporting of financial transactions.
  - 1.5.4 There is a procedure in place for regular financial audit.
  - 1.5.5 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 Management and/or security personnel control issuance and replacement of all locks, locking devices, keys, access tokens, codes, etc. according to written procedures.
- 2.1.7 Procedures are in place to identify, challenge and remove employees or visitors who are violating access control restrictions.
- 2.1.8 Maps/blueprints are available that show the perimeter, the building layout, identify secure perimeter areas, and identify all interior areas. All doors, windows, closets, and utility connection points should also be indicated.
- 2.1.9 Restricted, high security and hazardous material areas are clearly marked.
- 2.1.10 Security response personnel are available 24 hours a day.

### 2.2 Perimeter Control

- 2.2.1 Facility perimeter identified.
- 2.2.2 Secure perimeter areas identified.
  - 2.2.2.1 Cargo handling areas
  - 2.2.2.2 Cargo storage areas, including hazmat and high value.
  - 2.2.2.3 Utility service points (power, water, communications)
  - 2.2.2.4 Public parking.
  - 2.2.2.5 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 Vehicles and personnel entering or exiting the secure perimeter should be logged. Positive identification should be required of all persons.
- 2.2.6 There should be random inspection of vehicles and persons as they enter or exit the secure perimeter. All inspections should be documented.

- 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 with locking devices.
  - 2.3.9 Emergency exits are properly controlled.
  - 2.3.10 External supply or utility closets are secured and routinely checked.
  
- 2.4 Perimeter/External Access Control
  - 2.4.1 Access points into secure perimeter areas manned and/or monitored, or otherwise secured.
  - 2.4.2 Employee entrance(s) are manned and/or monitored, and are secured when not in use.
  - 2.4.3 Positive identification required for employee access to secure perimeter or facility interior.
  - 2.4.4 Access point for non-employees is manned and/or monitored and is secured when not in use.
  
- 2.5 Internal Boundaries and Security
  - 2.5.1 Internal access is controlled.
  - 2.5.2 Internal areas are clearly identified and access controlled.
  - 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 Waiting area for visitors, vendors and service providers should be separated from all other areas and monitored.
  - 2.5.7 Employee restrooms, locker-rooms, cafeterias and break areas should be separated from shipping, receiving, storage and production areas.
  - 2.5.8 Areas such as phone closets, server rooms and network relays should be 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.
  - 2.6.2 All visitors, vendors and service providers must sign in at the reception area. Picture ID must be provided, along with the reason for the visit and the name of the person they are to visit.
  - 2.6.3 All visitors, vendors and service providers must wear ID badges clearly indicating their visitor status.
  - 2.6.4 All visitors and vendors must be accompanied by a trained escort while on the premises.
  - 2.6.5 All visitors, vendors, and service providers must sign out at the completion of their visit. Their visitor credentials must be returned.
  - 2.6.6 Procedures must be in place for identifying, challenging and removing unescorted 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 for employees.
- 3.1.6 Review of personnel security practices to insure they comply with appropriate regulatory or contractual obligations.
- 3.1.7 Documentation of all steps and results in the employment cycle.
- 3.1.8 Procedures for safeguarding employee data.
- 3.1.8 Positions with a high impact on security are identified; security procedures applied to manage risk.
- 3.1.9 Documented procedure for use of identification badges to positively identify employees and provide access control. ID badges should include name, picture and job description.
- 3.1.10 Pictures, signatures and fingerprints are included in personnel records.
- 3.1.11 Access to ID badge materials, uniforms and personnel records is restricted and controlled. Logs are used to monitor distribution of ID badges and uniforms.

#### **3.2 Hiring Practices**

- 3.2.1 Prospective employees are informed of the personnel security procedures that will be used.
- 3.2.2 Use of standardized application for all applicants.
- 3.2.3 All personal information on the application verified with appropriate documentation.
- 3.2.4 Verification of all education, certification, previous employment and references.
- 3.2.5 Pre-employment criminal background investigation.
- 3.2.6 Pre-employment drug screening.
- 3.2.7 Pre-employment credit check to establish baseline.
- 3.2.8 Pre-employment interview by trained personnel.

- 3.3 Employee Provisioning
  - 3.3.1 Procedure for new employee orientation and training, including organization security policies and procedures.
  - 3.3.2 Procedure for issuance of identification.
  - 3.3.3 Procedure for issuance of computer and/or communications equipment, passwords, accounts, etc.
  
- 3.4 Ongoing personnel security
  - 3.4.1 Random drug testing.
  - 3.4.2 Periodic updates to credit check and criminal background investigation.
  - 3.4.3 Annual updates to employee data
  - 3.4.4 Comparison of update 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 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 recovery of identification card.
  - 3.5.3 Procedure for recovery/deactivation of computer or communications equipment.
  - 3.5.4 Procedure for de-provisioning/de-activation of access codes, email accounts, passwords, etc.
  - 3.5.5 Procedure for escort of terminated employee while on premises.
  - 3.5.6 Procedures to 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 High security seal procedures training
    - 4.1.5.3 Security risk identification and reporting training
    - 4.1.5.4 Training in the security aspects of each position.
  - 4.1.6 All shipments, receipts and storage activities are documented.
  - 4.1.7 Procedures 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 Raw material should be stored separately from finished goods.
  - 4.2.4 Access to each segregated area should be controlled and monitored.
  - 4.2.5 High value material storage segregated and access controlled.
  - 4.2.6 Hazardous materials identified, segregated, stored appropriately and access controlled.

#### 4.3 Receiving

- 4.3.1 Driver identification required before accepting shipment.
- 4.3.2 Cargo manifest must be present, complete and legible.
- 4.3.3 Container seal should be inspected, compared to seal number on manifest, and any discrepancy noted.
- 4.3.4 Procedures should exist for refusal of a shipment with improper documentation or seal discrepancies.
- 4.3.5 A shipment with a security seal discrepancy should be reported to appropriate law enforcement or customs officials.
- 4.3.6 Deviations from standard practices in container loading/stuffing should be noted.
- 4.3.7 Container contents should be verified against cargo manifest. Any discrepancies in content, weight, quantity, marking or packaging should be documented.
- 4.3.8 Procedures in place for reporting contraband or other illegal activities to appropriate law enforcement officials.
- 4.3.9 Procedures for documenting and reporting cargo shrinkage or theft.
- 4.3.10 Procedures for investigating any discrepancies found in the receiving process.
- 4.3.11 Procedures are in place for screening mail and small package deliveries prior to internal distribution.
- 4.3.12 Receiving documentation includes name(s) and signature(s) of all involved.

#### 4.4 Storage

- 4.4.1 Storage of materials should take place only after all receiving procedures are complete.
- 4.4.2 Priority should be given to correct storage of hazardous and high value materials.
- 4.4.3 Materials should be properly stored in an access controlled area until they ready for shipment.
- 4.4.4 If material is to be stored in a trailer or container, the contents must be documented, the container sealed, and the container must be stored in a secure area with access control and monitoring.
- 4.4.5 Empty trailers or containers must stored in a secure area with access control and monitoring. Procedures must be in place to prevent tampering or unauthorized entry into stored containers.

#### 4.5 Shipping

- 4.5.1 All shipping containers/trailers/trucks should undergo a 7 point inspection, including doors and locking mechanism, before they are loaded/stuffed. Inspection details should be documented.
- 4.5.2 Procedures should insure that shipping documentation is complete, legible and accurate.
- 4.5.3 Computer systems and data used to prepare shipping documents should be protected from unauthorized physical or electronic access.
- 4.5.4 Shipping data should be verified against the appropriate purchase order or delivery order where possible.
- 4.5.5 Shipping documents should be protected against loss and unauthorized disclosure or modification.
- 4.5.6 Physical counts, weights and labeling should be verified as the container is loaded/stuffed.
- 4.5.7 The trailer should be sealed in accordance with the security seal procedure, and the seal number noted on the shipping documentation and the seal log. For at-risk shipments a high security seal should be used.
- 4.5.8 Drivers should be properly identified before they are allowed to pickup the shipment.
- 4.5.9 Shipping documents should include name(s) and signature(s) of all involved.
- 4.5.10 Packing materials are inspected prior to use.

#### 4.6 Seal Management Program

- 4.6.1 Seals should be 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.
- 4.6.3 Documented procedures for recognizing a compromised seal and reporting it to the proper authorities.
- 4.6.4 Documented procedures reporting missing seals to the proper authorities.
- 4.6.4 Procedures for storing seals in a safe, accountable, access controlled manner.
- 4.6.5 Seals distributed and logged only by authorized personnel.
- 4.6.6 Procedures for handling sealed containers that are in transit. This should include reporting, refusal, and resealing procedures for 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 recognition and response.
    - 5.1.5.3 Preventive container and vehicle inspections for maintenance and regulatory compliance.
    - 5.1.5.4 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.
- 5.2 Inspection of Containers and Conveyance
  - 5.2.1 All inspections follow established procedure and are documented.
  - 5.2.2 Security inspection of containers using 7 point inspection method. Specified conditions requiring a container not be used.
  - 5.2.3 Security inspection of vehicles.
  - 5.2.4 Security inspection of passenger baggage.
  - 5.2.5 Container inspections to occur before filling/stuffing, after unloading, and when receiving an empty from storage or service provider.
  - 5.2.6 Net and gross weight of vehicles and containers should be recorded.
  - 5.2.7 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 Technological tracking systems (GPS).
  - 5.3.3 Check points, convoys, escorts, dog screening.
  - 5.3.4 Shipment risk assessments (dwell time analysis, lane segment history, etc)
  - 5.3.5 Each movement of a container or conveyance should be documented.
  
- 5.4 Regulatory Inspections
  - 5.4.1 Procedure for compliance inspection of containers and vehicles, including required equipment, equipment condition, licensing, permits, etc.
  - 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

- 6.1 Utilities, Systems and Communication Security Management
  - 6.1.1 Manager(s) responsible for utilities, systems and communication security identified.
  - 6.1.2 Published utilities, systems and communication security policies identifying program goals. Should include acceptable use policy and email retention policy.
  - 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 Maintenance personnel trained in utility shutoff conditions and procedures.
    - 6.1.5.2 Training for power failure procedures.
    - 6.1.5.3 Proper use training for communications systems.
    - 6.1.5.4 Basic security and proper use training for information systems.
  - 6.1.6 Procedures in place for routine backup and offsite storage of mission critical data.
  - 6.1.7 Procedures in place for emergency replacement of mission critical equipment.
  - 6.1.8 Procedures in place for restoration of data from backups.
  - 6.1.9 Recovery procedures include verification that critical systems are again functioning properly.
  
- 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 not left unescorted in the presence of active IS equipment.
  - 6.2.5 IS vendors and maintenance personal are positively identified and continuously escorted. If given access to information systems must have privacy agreement in place.
  - 6.2.6 Backup power to maintain critical systems for controlled shutdown.

- 6.3 Information access control
  - 6.3.1 User id's and passwords used to control access to information systems.
  - 6.3.2 Users should have least privileges necessary to adequately perform their jobs.
  - 6.3.3 Information systems should have audit procedures in place to identify user, date and time for any data entry or modification.
  - 6.3.4 Procedures should be in place to deactivate the user id and password of any terminated employee.
  - 6.3.5 Password policy and controls should include standards for password strength and expiration.
  - 6.3.6 Lost password procedure should include positive identification of the user before issuing a new password.
  
- 6.4 Communication Security
  - 6.4.1 Established procedure for use of communications facilities, including telephone systems, cellular phones, 2-way radios, instant messaging, and text messaging.
  - 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.
  
- 6.5 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 Established procedures to respond to utility outages.
  - 6.5.4 Emergency lighting in critical areas.
  - 6.5.5 Established procedures for utility service resumption.

## 7. 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. This should include a list of 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.
- 7.1.6 Secure partnership program applies to all customer, vendor, service providers, etc.

### 7.2 Supplier Screening

- 7.2.1 Security screening incorporated into the supplier selection process. This should include verification of references and inferred reliability based on quality of internal controls and security.
- 7.2.2 Procedure for regular supplier background/credit checks. Financial stability included in supplier risk assessment.
- 7.2.3 Suppliers are required to provide detail information on their internal security policies and procedures, including participation in any regulatory partnership programs.
- 7.2.4 Security requirements which apply to suppliers should be included in any request for quotes or pricing, and should be included in contracts and agreements.
- 7.2.5 Established procedure for notifying supplier of non-compliance with security requirements.
- 7.2.6 Verification of stated participation in regulatory partnership programs, or of compliance with established security parameters.
- 7.2.7 Procedure in place for regular supplier audits.
- 7.2.8 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 audit and corrective action.
- 8.1.7 Audit schedule(s) established based on risk assessments, with a one year maximum audit cycle.

### 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 employees, vendors and customers.
- 9.1.5 Ongoing emergency response and recovery training program for employees.
- 9.1.6 Established program and procedures for review and update of emergency plans.
- 9.1.7 Established emergency procedures that include planning for natural disaster and terrorist attack.
- 9.1.8 An emergency evacuation plan is posted for each facility.

### 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

- 9.3 Emergency Response Team
  - 9.3.1 The plan specifies an emergency response team whose job it is to manage the response and recovery operations.
  - 9.3.2 Each person on the emergency response team has a clearly defined role.
  
- 9.4 Emergencies and Regulatory/Law Enforcement Agencies
  - 9.4.1 Emergency plans should include a comprehensive list of contacts and phone number for regulatory and law enforcement agencies.
  - 9.4.2 Emergency plans should include policy and procedure for informing regulatory/law enforcement agencies, based on the nature of the emergency.
  - 9.4.3 Policy should indicate 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 should be 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

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

### 10.4 Policy and Procedure Management

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

10.5 Training and Education

- 10.5.1 An ongoing program of training and education is in place.
- 10.5.2 The training requirements of each job position is identified.
- 10.5.3 Training records are routinely reviewed to ensure employees are receiving the training indicated by their positions.
- 10.5.4 Training programs are reviewed to ensure they meet the current security and regulatory requirements.
- 10.5.5 Training programs should include:
  - 10.5.5.1 Threat awareness.
  - 10.5.5.2 Basic security procedures.
  - 10.5.5.3 Social engineering resistance.
  - 10.5.5.4 IT security training for information workers.
  - 10.5.5.5 Recognizing internal conspiracies.
  - 10.5.5.6 Maintaining perimeter and access control integrity.
  - 10.5.5.7 Workplace safety and violence prevention.
  - 10.5.5.8 Drug and alcohol awareness.