Supply Chain Security Audit Tool - Warehousing/Distribution

This audit tool was developed to assist manufacturer clients with the application of the concepts in the *Rx-360 Supply Chain Security White Paper: Audits and Assessments of Third Party Warehousing and Distribution Facilities* . This audit tool was designed specifically for the warehousing and distribution segment and was built to closely match the requirements outlined in the *Rx-360 Supply Chain Security Template -- Requirements for Third Party Logistics Providers.* This helps an organization to utilize the requirements in their contracts and standards, and have an audit tool that closely matches their desired contract terms, providing a cohesive audit program.

Supply Chain Security Audit Tool - Warehousing/Distribution

Company		Audit	
Location		Number	
Contact Name		Number	
AUDITOR(s)		Email	

Supply Chain Security Audit Tool - Warehousing and Distribution

CATEGORY		Y	N	N/A	COMMENTS
I. General Requirements					
Statement of Confidentiality	Vendor has appropriate confidentiality agreements on file				
Restrictions for the Purchase, Sale and Shipment of Products	Duties are segregated to reduce the likelihood of product diversion or theft (for example, the person picking and packing is not also the person checking goods).				
Restrictions for the Purchase, Sale and Shipment of Products	All orders and receipts are tracked.				
Sourcing of Components Required for <Company Name> Products	Components required for <Company Name> products are only sourced from suppliers authorized by <Company Name>.				
National Cargo Security Program Requirements	Vendor is either a participant in the C-TPAT program or the applicable foreign equivalent National Cargo Security program, or at a minimum, satisfies <Company Name>'s minimum Supply Chain Security requirements.				
National Cargo Security Program Requirements	Vendor is already an approved member of the applicable National Cargo Security program or has signed a memorandum of understanding ("MOU") with <Company Name> guaranteeing vendor compliance with <Company Name>'s specified minimum security criteria.				
National Cargo Security Program Requirements	Vendor has completed <Company Name>'s Security Profile Questionnaire.				
Sub-contractor Approval	All sub-contractors used by vendors to handle <Company Name> Goods are approved by <Company Name>.				

External Security Firms	External firms retained to provide security at vendor or subcontractor facilities are licensed to the full extent required under applicable laws.				
External Security Firms	External firms retained to provide security at vendor or subcontractor facilities that house <Company Name> Goods or Confidential Information have no business connection with any firm providing temporary staff to the authorized supplier.				

Company		Audit	
Location		Number	
Contact Name		Number	
AUDITOR(s)		Email	

Supply Chain Security Audit Tool - Warehousing and Distribution

CATEGORY		Y	N	N/A	COMMENTS
II. Physical Security					
Site Security Personnel	There is one point of contact for site security.				
Site Security Personnel	A guard is present at all staffed points of entry during working hours.				
Construction	Material construction of the facility, including doors, windows, skylights and all potential points of entry, is suitable to withstand forced entry.				
Construction	Warehouse exit doors and dock doors are constructed to resist forced entry.				
Secured Points of Entry	All points of entry (including visitor access, shipping and receiving access, fire exits and roof hatches) are closed and locked except as necessary for normal operations.				
Secured Points of Entry	All unstaffed access points are locked, covered by security screens, and alarmed.				
Secured Points of Entry	All windows and skylights have security screens.				
Secured Points of Entry	Dock and warehouse door hinges are pinned or welded.				
Secured Points of Entry	Facility structures and fencing are regularly inspected.				
Monitoring Systems	The resolution of live and recorded surveillance images is good enough to clearly recognize individuals.				
Monitoring Systems	Video surveillance is maintained twenty-four (24) hours per day.				
Monitoring Systems	Video surveillance covers all sides of the facility.				
Monitoring Systems	Video is monitored in real time and is also recorded.				

Monitoring Systems	The video surveillance system includes continuous date and time stamping of recorded images.				
Monitoring Systems	The surveillance system is inspected and tested regularly.				
Monitoring Systems	Procedures are in place for manual testing of systems and equipment.				
Monitoring Systems	Video recording is on digital media, not analog tape.				
Monitoring Systems	Video surveillance equipment is kept in a secure location.				
Monitoring Systems	Video or audio surveillance media that does not document an event is stored for a minimum of 30 days following its recording.				
Monitoring Systems	Video or audio surveillance media that documents an event is retained indefinitely.				
Monitoring Systems	Video media is stored in a secure internal location separate from the recording equipment.				
Lighting	Lighting is sufficient to identify all persons entering and exiting the facility and parking areas using the video monitoring system.				
Lighting	Lighting is on twenty-four (24) hours per day.				
Communication	Facility has internal and external communications systems that connect to internal security and local police.				
Alarm System	The alarm system is physically wired.				
Alarm System	The alarm system includes motion-detection sensors.				
Alarm System	Glass-break detectors are used wherever necessary, particularly on ground floor windows or other windows that can be easily accessed.				
Alarm System	The alarm control system is placed in a secure location.				
Alarm System	Alarm systems and video surveillance equipment are connected to a back-up power system.				
Alarm System	The alarm system is inspected and tested regularly.				
Alarm System	Procedures are in place for manual testing of systems and equipment.				
Perimeter Fencing	The facility perimeter is fenced or walled.				
Perimeter Fencing	Perimeter fencing and fence topper are free of vegetation.				

Perimeter Fencing	Perimeter fencing and fence topper are in a good state of repair.				
Perimeter Fencing	Fencing is far enough from adjacent structures to prevent site access from them.				
Perimeter Fencing	Perimeter fencing is at least 8 feet high, not including the height of the fence topper.				
Perimeter Fencing	Perimeter fencing has a four-strand or five-strand barbed wire or razor wire fence topper.				
Perimeter Fencing	If the fence topper is barbed wire, it is angled at 45 degrees out of the facility.				
Perimeter Fencing	Perimeter fencing completely encloses the facility and is penetrated only at designated access points.				
Perimeter Fencing	The grounds are clear of vegetation for ten meters on both sides of the perimeter fencing.				
Perimeter Fencing	There are no view blocks (outbuildings, vehicles, etc.) along the perimeter fencing.				
Perimeter Fencing	Camera and guard views along the perimeter fencing and adjacent spaces are not obstructed.				
Perimeter Fencing	Perimeter fencing is patrolled by Security.				
Perimeter Fencing	Adequate CCTV coverage is installed along the perimeter fencing.				
Private Vehicle Control	Private vehicles are parked in a fenced parking area that is physically separate from facilities housing <Company Name> Goods or IP.				
Private Vehicle Control	The vendor uses a registration system for all vehicles permitted access to the private parking area.				
Private Vehicle Control	Private vehicles are not permitted in or next to cargo handling locations.				
Private Vehicle Control	The fenced private parking area is outside of the vendor’s facility.				
Private Vehicle Control	Private vehicles permitted to enter the facility are searched on entry and exit.				

Company		Audit	
Location		Number	
Contact Name		Number	
AUDITOR(s)		Email	

Supply Chain Security Audit Tool - Warehousing and Distribution

CATEGORY		Y	N	N/A	COMMENTS
III. Access Control					
Visitor Identity	The identity of every visitor is verified against their government-issue photographic identification before they are granted access to the facilities.				
Visitor Chaperoning	Visitors are accompanied by an authorized employee at all times when in facilities housing <Company Name> Goods or IP, or devices containing <Company Name> IP.				
Visitor Chaperoning	A visitor log is kept				
Visitor Chaperoning	All visitor logs are retained for at least 12 months.				
Identification Badges	Photo or serialized ID badges are provided to all personnel and visitors.				
Identification Badges	Access to the ID badge card issuance system is controlled.				
Verification of Identity	The identity of all personnel or visitors granted access to the facility is verified by electronic means or directly by staff security.				

Company		Audit	
Location		Number	
Contact Name		Number	
AUDITOR(s)		Email	

Supply Chain Security Audit Tool - Warehousing and Distribution

CATEGORY		Y	N	N/A	COMMENTS
IV. Records and Logs					
External Security Records	Security personnel records are kept indefinitely, unless instructed otherwise by <Company Name>.				
External Security Records	Personnel records are kept for external Security personnel.				
Employee Records	Employee termination records are kept for both vendor and sub-contractor employees.				
Employee Records	Records of employees ordering, receiving and shipping <Company Name> Goods are kept for both vendor and sub-contractor employees.				
Employee Records	Training records are kept for both vendor and sub-contractor employees.				
Video Surveillance Equipment	Maintenance and testing of all video surveillance equipment is recorded in a log.				
Video Surveillance Equipment	Each camera has an operational specification written for it.				
Video Surveillance Equipment	Security officers audit each camera against the matching operational specification at least once each month.				
Computer System Logs	All computer systems containing <Company Name> IP, and the critical computing resources on which they depend, are logged and tracked in accordance with applicable laws and regulations.				
Computer System Logs	Access Control Logs are reviewed every 60 days to verify that only users with valid business reasons and existing management approval have access to systems containing <Company Name> IP.				
Computer System Logs	Computer log files are retained for at least 60 days.				

Computer System Logs	Security Activity Reports are reviewed weekly.				
Computer System Logs	A Digital Access log is kept.				
Computer System Logs	Digital access logs are reviewed every 60 days.				
Site Access Records and Logs	A Site Visitor log, documenting all visitors and vendors, is kept.				
Site Access Records and Logs	All visitor logs are retained for at least 12 months.				
Site Access Records and Logs	All access codes are logged.				
Site Access Records and Logs	Access Code and Key Possession records are kept, as applicable.				
Site Access Records and Logs	Controlled Access logs are kept and updated for every change of access.				
Site Access Records and Logs	Controlled Access records are reviewed for irregularities every 12 months.				
Driver and Vehicle Information Required for Transport	Driver name and license records are kept for each shipment of <Company Name> Goods.				
Driver and Vehicle Information Required for Transport	A vehicle license record is kept for each shipment of <Company Name> Goods.				
Driver and Vehicle Information Required for Transport	Cargo seal serial number logs are kept for each shipment of <Company Name> Goods.				
Driver and Vehicle Information Required for Transport	Records of the date and time of cargo pick-up are kept for each shipment of <Company Name> Goods.				
Scrap and Destroy Records	Records of scrapped <Company Name> Goods and IP are kept, as applicable.				
Inventory and Use Records of Goods	Discrepancies between physical inventories and inventory records are reported to <Company Name> as security incidents.				
Inventory Records of Cargo Shipments	The name of the shipper or consignee is recorded for each cargo shipment.				
Inventory Records of Cargo Shipments	The description, weight and number of units contained are recorded for each cargo shipment.				
Inventory Records of Cargo Shipments	Shortages and overages for each cargo shipment, if any, are recorded.				
Inventory Records of Cargo Shipments	Shipment and receipt dates, Custom manifests, and other accompanying documentation are recorded for each cargo shipment.				
Inventory Records of Cargo Shipments	Shipment seals are tracked and verified.				
Inventory Records of Cargo Shipments	All shipments are reconciled against their shipment manifest .				

Company		Audit	
Location		Number	
Contact Name		Number	
AUDITOR(s)		Email	

Supply Chain Security Audit Tool - Warehousing and Distribution

CATEGORY		Y	N	N/A	COMMENTS
V. Procedural Security					
Data Access Policy and Procedures	The data access policy requires password protection of systems				
Data Access Policy and Procedures	Procedures ensure that user accounts and passwords used to access these systems are not posted, otherwise distributed, or shared by more than one person.				
Data Access Policy and Procedures	Procedures that establish and maintain the authorization mechanisms which control access exist.				
Business Continuity Plan	Disaster Recovery Plans include details of all physical systems, details of all information systems, details of all network security processes and requirements, and a contact list.				
Business Continuity Plan	Disaster Recovery Plans are printed out and stored in secure on- and off-site locations.				
Business Continuity Plan	The Business Continuity Plan meets the requirements specified in the SCS Contract.				
Security Incident Procedures	Security incident documentation includes provisions to escalate incidents and emergency contact information				
Security Incident Procedures	A Security Incident report template exists.				
Security Incident Procedures	Management reviews all completed Security Incident reports.				
User Account Procedures	Procedures to create, maintain and terminate user accounts are included in the vendor's Network Security document.				
Internal Access Procedures	Internal access control procedures address site access, visitor control, video surveillance and monitoring, and alarm and access control systems monitoring and response.				

Cargo Security Standards	Cargo security documentation includes procedures for the use and verification of high security seals.				
Cargo Security Standards	Cargo security documentation includes procedures for verifying the physical integrity of trucks, trailers, containers, rail cars, and aircraft.				
Cargo Security Standards	Cargo security documentation includes procedures for verifying the reliability of locking mechanisms on all transportation.				
Cargo Security Standards	Cargo security documentation includes procedures to ensure that all outbound shipments are destined to an authorized location.				
Cargo Security Standards	Cargo security documentation includes procedures to ensure that shipments are scheduled for delivery during normal business hours, unless a shipment has a specific receiving procedure in place prior to shipment.				

Company		Audit	
Location		Number	
Contact Name		Number	
AUDITOR(s)		Email	

Supply Chain Security Audit Tool - Warehousing and Distribution

CATEGORY		Y	N	N/A	COMMENTS
VI. Personnel Security					
Employees Handling <Company Name> Product or Intellectual Property	Only proprietary, full-time vendor and subcontractor employees are approved to access or handle <Company Name> Product or IP.				
Employees Handling <Company Name> Product or Intellectual Property	Vendor notifies <Company Name> and waits for approval before allowing sub-contracted individuals to access or handle <Company Name> Product or IP.				
Employees Handling <Company Name> Product or Intellectual Property	All vendor and subcontractor employees successfully complete a drug analysis test, as permitted by law, before being allowed access to Goods				
Background Investigations	Background investigations are conducted on all employees, if this is permitted by law, prior to hiring or assignment, and prior to granting them access to <Company Name> Goods or IP.				
Employee Terminations	All terminations of employees and sub-contractor employees must be documented.				
Employee Terminations	A ‘not eligible for re-hire’ list of terminated employees is kept.				
Employee Terminations	New applicants for employment are checked against the ‘not eligible for re-hire’ list prior to employment.				
Employee Terminations	The facts surrounding the termination of any employee who is determined not to be eligible for re-hire are documented to the extent permitted by law.				
Employee Terminations	Access control devices (keys or cards) are collected from every terminated employee and sub-contractor employee immediately upon termination.				

Employee Terminations	Systems access permissions for terminated employees are removed within 24 hours of their termination.				
Retention of Training Records	Detailed training records are kept of all personnel receiving training and training updates.				

Company		Audit	
Location		Number	
Contact Name		Number	
AUDITOR(s)		Email	

Supply Chain Security Audit Tool - Warehousing and Distribution

CATEGORY		Y	N	N/A	COMMENTS
VII. Cargo Security					
On-site Cargo Security	All trucks, trailers and containers are secured using high-security seals that comply with the standards of the country of origin, applicable trans-shipment countries, and the country of destination.				
On-site Cargo Security	Access to container seals is limited.				
On-site Cargo Security	Container seals cannot be removed without destroying them.				
On-site Cargo Security	Trucks are permitted to enter and leave the facility through secured access points only.				
On-site Cargo Security	Unattended containers, trucks, and trailers containing <Company Name> Goods are parked in secure holding areas.				
On-site Cargo Security	Unattended containers, trucks, and trailers containing <Company Name> Goods are locked and alarmed.				
On-site Cargo Security	Unattended containers, trucks, and trailers containing <Company Name> Goods are monitored through video surveillance or directly by security personnel.				
On-site Cargo Security	Cargo loading and unloading is supervised by <Company Name>-authorized personnel.				
On-site Cargo Security	Full pallets, partial pallets, and single shipped master cartons are weighed before shipment.				
On-site Cargo Security	Delivery, loading and unloading occur during applicable business hours only.				
On-site Cargo Security	<Company Name> Goods are not pre-loaded into cargo vehicles except under pre-approved conditions.				

On-site Cargo Security	Cargo weight and carton count of all received shipments of <Company Name> Goods are reconciled against the manifest documents while the cargo vehicle is still present.				
On-site Cargo Security	Cargo vehicles are inspected for unauthorized or unmanifested materials before <Company Name> Goods are loaded.				
On-site Cargo Security	Shipments are scheduled for delivery during normal receiving business hours, unless a shipment has an alternate receiving procedure in place prior to shipment. Each alternate receiving procedure can apply to one specific shipment only.				
On-site Cargo Security	Shipping and Receiving functions are segregated such that <Company Name> Goods cannot be simultaneously loaded on and unloaded from the same truck, trailer or container.				
On-site Cargo Security	Cargo Vehicle locking mechanisms are inspected upon each loading of <Company Name> Goods.				
On-site Cargo Security	Cargo Vehicle inspection logs list the names of the person(s) conducting the inspections and their findings.				
On-site Cargo Security	Information regarding incoming and outgoing shipments, including the routing of said shipments, is kept confidential and is securely guarded.				
On-site Cargo Security	Driver identification is verified before vehicles carrying <Company Name> Goods depart.				
Controlling Access to Cargo	Access to shipping and loading docks is recorded in a log.				
Controlling Access to Cargo	Access to cargo areas is recorded in a log.				
Controlling Access to Cargo	Access to trailers, containers, or any other vehicle involved in the transport of <Company Name> Goods is recorded in a log.				
Controlling Access to Cargo	Drivers are accompanied by authorized personnel when in a shipping/receiving area for <Company Name> Goods.				

Controlling Access to Cargo	Vendor keeps complete records of driver names, license number, vehicle license number and issuing governmental authority (tractor and trailer, if applicable), seal serial number, and the date and time of pick-up for every shipment of <Company Name> Goods .				

Company		Audit	
Location		Number	
Contact Name		Number	
AUDITOR(s)		Email	

Supply Chain Security Audit Tool - Warehousing and Distribution

CATEGORY		Y	N	N/A	COMMENTS
VIII. Control of <Company Name> Goods in the Facility					
Storage of <Company Name> Goods	<Company Name> storage areas are located within the confines of the facility.				
Storage of <Company Name> Goods	<Company Name> storage areas are kept closed and locked.				
Storage of <Company Name> Goods	<Company Name> Goods are transferred upon reception to secure, access controlled internal location(s) by authorized personnel.				
Storage of <Company Name> Goods	Access to <Company Name> Goods is provided for established business needs only.				
Storage of <Company Name> Goods	<Company Name> storage areas are accessible from specific monitored locations only.				
Storage of <Company Name> Goods	Access to <Company Name> storage areas is by assigned access code. If the facility cannot accommodate an access code system, keys or access cards may be used instead.				
Storage of <Company Name> Goods	Access codes are issued to authorized individuals only, and are not shared between individuals.				
Storage of <Company Name> Goods	Access codes are changed at least once every three (3) months.				
Storage of <Company Name> Goods	Access codes are controlled and logged by authorized individuals only.				
Storage of <Company Name> Goods	Extra, unused or returned access keys or cards are kept in a secure location.				
Storage of <Company Name> Goods	The identity of each person seeking access to <Company Name> Goods is verified in real time.				

Storage of <Company Name> Goods	Electronic access logs that include the name of the accessing individual and the date and time of access are kept and retained indefinitely.				
Storage of <Company Name> Goods	Photo or serialized identification badges are visibly displayed by all personnel provided access to <Company Name> Goods or IP.				
Storage of <Company Name> Goods	Temporary staff (for example, maintenance or cleaning crews) are supervised at all times by authorized personnel.				
Storage of <Company Name> Goods	Personal belongings are searched when personnel enter and exit the storage areas.				

Company		Audit	
Location		Number	
Contact Name		Number	
AUDITOR(s)		Email	

Supply Chain Security Audit Tool - Warehousing and Distribution

CATEGORY		Y	N	N/A	COMMENTS
IX. Returned and Rejected Product					
Mandatory Scrap and Destruction	<Company Name> Goods in vendor's possession that are no longer required to fulfill a contract or agreement are scrapped and destroyed within a specified time frame.				
Mandatory Scrap and Destruction	Unusable <Company Name> Goods are scrapped and destroyed within a specified time frame.				
Mandatory Scrap and Destruction	<Company Name> Goods at end of life are scrapped and destroyed within a specified time frame.				
Mandatory Scrap and Destruction	<Company Name> Goods in vendor's possession are scrapped and destroyed within a specified time frame if vendor's agreement is terminated or no further production, supply and/or distribution of <Company Name> Goods is authorized.				
Destruction of Scrapped or Returned <Company Name> Goods and IP	Vendors store scrapped or returned product, packaging labels, and product inserts in a dedicated secure area on the premises.				
Destruction of Scrapped or Returned <Company Name> Goods and IP	Destruction of <Company Name> Goods is performed in the presence of an authorized <Company Name> representative and is certified.				
Destruction of Scrapped or Returned <Company Name> Goods and IP	Certificates of destruction are retained indefinitely.				
Destruction of Scrapped Electronic Files	Vendors remove <Company Name> electronic files from their inventory when these are no longer required to fulfill a contract or agreement.				
Destruction of Scrapped Electronic Files	Electronic files scheduled for destruction are securely deleted using procedures specified by <Company Name> .				
Destruction of Scrapped Electronic Files	Electronic file destruction is documented.				

Company		Audit	
Location		Number	
Contact Name		Number	
AUDITOR(s)		Email	

Supply Chain Security Audit Tool - Warehousing and Distribution

CATEGORY		Y	N	N/A	COMMENTS
X. Reporting and Notification					
Firewall Access Violations	Firewall access violations are logged and periodically reviewed to identify potential network intrusions.				
After-hours Alarm Notification	Vendor keeps an after-hours alarm notification list that has multiple layers of redundancy to guarantee that a responder is always available.				
After-hours Alarm Notification	The after-hours alarm notification list is updated and tested at least once every six months.				
Employee Background Issues	Written approval from <Company Name> 's account manager is obtained prior to allowing access to <Company Name> Goods by individuals or entities whose names appear on lists of known terrorist organizations, government debarred lists or previous criminal activity				
Security Incidents	A local management contact to be telephoned in the event of a security incident is identified by the vendor.				

Company		Audit	
Location		Number	
Contact Name		Number	
AUDITOR(s)		Email	

Supply Chain Security Audit Tool - Warehousing and Distribution

CATEGORY		Y	N	N/A	COMMENTS
XI. Information Protection					
Information Security Managment	An Information Security Management function establishes information security management policies; monitors compliance to established controls; assesses information risks and manages risk mitigation.				
Protected Access to Confidential Information	<Company Name> Confidential Information are stored only on secure computers that are protected from general purpose computer networks by a dedicated firewall.				
Protected Access to Confidential Information	<Company Name> Confidential Information is not stored on internal drives to which external portable media recordable devices can be attached for the extraction of data .				
Environmental Controls	Critical computer resources are housed in accordance with equipment manufacturer's operating specifications for temperature ranges, humidity levels and particulate count.				
Fire Suppression	Data centers and computer rooms housing critical computer resources are equipped with fire suppression systems.				