WAREHOUSING WHITE PAPER CHECKLIST

ICHCA INTERNATIONAL

IVODGA INTERNATIONAL VESSEL OPERATORS DANGEROUS GOODS ASSOCIATION

NATIONAL CARGO BUREAU

World Shipping Council

This warehouse checklist should be used by warehouses storing and handling Dangerous Goods in preparation for, or after, sea transport. It can also be used in warehouse audits and inspections. It is intended that this checklist will make facilities safer and assist duty holders to be better prepared to react effectively if an incident occurs. Please answer all of the questions and keep a copy of this document in a safe place for future reference.

SECTION: 1	GENERAL	YES	NO	N/A
1.1	Certifications			
1.1.1	Does the warehouse[1] hold certifications demonstrating compliance with relevant industry / government standards[2]?	◯	◯	◯
1.2	Investigation Program			
1.2.1	Has the warehouse implemented a comprehensive investigation program for accidents, losses, or near-misses?	◯	◯	◯
1.3	Business Continuity			
1.3.1	Does the warehouse have a business continuity plan in place to keep operations going in case of fire, flood, loss of power, loss of communication, etc.?	◯	◯	◯

GUIDANCE NOTES:

[1] The term warehouse in this document may apply to operators or facilities including warehouses, waterfront facilities at ports or terminals, distribution centers, fulfillment houses, etc. where goods may be stored before their export, in the due course of transit, or before distribution for sale.

[2] Examples of relevant industry or government standards may include US Customs and Border Protection Customs Trade Partnership Against Terrorism (CTPAT) security program, International Organization for Standardization 9001 Quality Management Standard, Transported Assets Protection Association (TAPA) Facility Security Requirements Standard (for high value theft targeted goods), etc. as applicable.

SECTION: 2	WORKFORCE	YES	NO	N/A
2.1	Screening[1]			
2.1.1	Are written procedures in place for screening prospective employees[2] and to periodically check current employees[2]?	◯	◯	◯
2.1.2	Do screening procedures include verification of application information such as identity, past employment, references, and criminal history?	◯	◯	◯
2.1.3	Do screening procedures extend to temporary workforce and contractors[2]?	◯	◯	◯
2.2	Formal Induction			
2.2.1	Do new warehouse employees have a formal induction when joining?	◯	◯	◯
2.3	Identification			
2.3.1	Do warehouse employees wear uniforms?	◯	◯	◯
2.3.2	Are warehouse employees required to display company ID badges?	◯	◯	◯

2.4	Termination or Re-hiring Process			
2.4.1	Is the termination or re-hiring process for warehouse employees or contractors documented (including a checklist)?	◯	◯	◯
2.4.2	Does this process include collection of physical assets[3]?	◯	◯	◯
2.4.3	Does this process include termination of access to physical or electronic company systems?	◯	◯	◯
2.5	Training			
2.5.1	Do warehouse employees and contractors receive relevant awareness and function specific training as appropriate?	◯	◯	◯
2.5.2	Is required training documented and records maintained?	◯	◯	◯

GUIDANCE NOTES:

[1] Screening should be conducted in accordance with applicable legal limitations, and the availability of city, state, provincial, and country criminal record databases and other relevant information.

[2] Degree of screening should be based on the nature and sensitivity of the employee's position or contractor's function.

[3] Physical assets may include items such as access badges, keys, computers, etc.

SECTION: 3	CONSTRUCTION	YES	NO	N/A
3.1	Building Code Requirments[1]			
3.1.1	Does construction of the warehouse meet applicable building code requirements?	◯	◯	◯
3.2	Utilities and Appliances			
3.2.1	Are warehouse utilities including systems and associated wiring and piping protected from physical damage?	◯	◯	◯
3.2.2	Is sufficient clearance maintained between heat-producing appliances in the warehouse and any stored flammable or combustible materials or cargo?	◯	◯	◯
3.3	Internal Lighting and Ventilation			
3.3.1	Is warehouse internal lighting satisfactory for working conditions?	◯	◯	◯
3.3.2	Is warehouse ventilation / exhaust capability adequate for operations and / or emergencies?	◯	◯	◯
3.4	Emergency Power			
3.4.1	Is the warehouse fitted with a back-up generator or other source of emergency power?	◯	◯	◯

3.5	Facility Maintenance			
3.5.1	Is a preventative maintenance program established for the warehouse?	◯	◯	◯
3.5.2	Are maintenance and repair records maintained?	◯	◯	◯

GUIDANCE NOTES:

[1] Depending on applicable jurisdiction, the warehouse will need to conform to specific building code requirements. These may be in the form of national building codes and / or model building codes adopted by local authorities. Building codes generally include specific standards for building structure, occupancy, fire prevention, earthquake, windstorm, flood and tsunami resistance, energy provisions and consumption, etc.

SECTION: 4	OPERATIONS	YES	NO	N/A
4.1	Applicable Code Requirements			
4.1.1	Does storage of goods in the warehouse meet applicable building code requirements[1]?	◯	◯	◯
4.2	Rack Systems			
4.2.1	Is storage on rack systems maintained within rated load capacity?	◯	◯	◯
4.2.2	Is rated load capacity clearly marked on racks?	◯	◯	◯
4.2.3	Are periodic inspections of rack systems carried out?	◯	◯	◯
4.2.4	Are rack systems protected from allisions with forklifts or other vehicles[2]?	◯	◯	◯
4.2.5	Is adequate width of aisles between racks maintained?	◯	◯	◯
4.2.6	Are aisles between racks kept clear of obstructions?	◯	◯	◯
4.3	Cargo Securing			
4.3.1	Are stored goods adequately secured against falling, tipping over, etc.?	◯	◯	◯
4.4	Cargo Handling Equipment			
4.4.1	Is there a minimum clearance of 2m between re-charging or fueling area and stored goods?	◯	◯	◯
4.4.2	If propane is utilized, is it properly stored outdoors?	◯	◯	◯
4.4.3	Is a preventative maintenance program in place for cargo handling equipment?	◯	◯	◯
4.4.4	Is maintenance and repair of cargo handling equipment documented?	◯	◯	◯
4.4.5	Are equipment operators trained and certified?	◯	◯	◯

4.5	Idle Pallet Storage			
4.5.1	Does idle pallet storage location, configuration and maximum height conform with applicable code requirements including sprinkler protection?	◯	◯	◯
4.5.2	Are idle pallets stored flat (not on edge)?	◯	◯	◯
4.5.3	If allowed to be stored on racks, are idle pallets stored on highest level above other goods in storage?	◯	◯	◯
4.5.4	Are regular checks carried out for damaged pallets?	◯	◯	◯
4.5.5	Are accumulations of pallets and other combustible materials minimized in storage areas?	◯	◯	◯
4.6	Housekeeping Practices			
4.6.1	Are good housekeeping practices maintained[3]?	◯	◯	◯
4.6.2	Are housekeeping self-audits carried out on a regular basis?	◯	◯	◯
4.7	Smoking Requirements			
4.7.1	Are “No-Smoking” signs posted in prohibited areas?	◯	◯	◯
4.7.2	Are dedicated smoking areas established?	◯	◯	◯
4.7.3	Is there disciplinary action for non-compliance with smoking requirements?	◯	◯	◯

GUIDANCE NOTES:

[1] Building code requirements as they relate to storage may include types of storage allowed (rack, solid-pile, bulk, bin box, etc.), height of storage allowed, applicable floor loadings, minimum distance maintained from ceiling / roof structure, storage configuration (including idle pallets), proper elevation of floor stored goods to avoid water damage, etc.

[2] This may be achieved through use of end caps, bollards, posts, etc.

[3] Good housekeeping practices may include a high level of cleanliness and maintenance of the warehouse, prevention of visible pest contamination, clear aisles between racks, minimum clutter, etc.

SECTION 5	DANGEROUS GOODS STORAGE	YES	NO	N/A
5.1	Dangerous Goods Acceptance			
5.1.1	Does the warehouse store Dangerous Goods that are regulated under one or more of the nine UN Dangerous Goods classes[1] including Dangerous Goods transported under special provisions?	◯	◯	◯
5.1.2	Are Dangerous Goods packages and / or cargo transport units (CTU)[2], and their required documentation reviewed prior to accepting for storage?	◯	◯	◯

5.2	Storage Restrictions and Permitting Requirements			
5.2.1	Is there a documented process to ensure the warehouse complies with any Dangerous Goods storage restrictions or permitting requirements[3]?	◯	◯	◯
5.3	Personnel			
5.3.1	Is there a designated person accountable for Dangerous Goods compliance and safety?	◯	◯	◯
5.3.2	Is Dangerous Goods training[4] provided to warehouse employees?	◯	◯	◯
5.4	Segregation of Incompatible Goods			
5.4.1	Does the warehouse have documented protocols to ensure Dangerous Goods are properly segregated/separated from other Dangerous Goods/non-Dangerous Goods as appropriate?	◯	◯	◯
5.4.2	Does the warehouse have designated storage areas for Dangerous Goods to ensure proper segregation from incompatible materials?	◯	◯	◯
5.4.3	Are designated storage areas clearly identifiable with adequate, legible signposting?	◯	◯	◯
5.5	Inventory Statement and Management Plan			
5.5.1	Has an inventory statement[5] been developed for all Dangerous Goods stored at the warehouse?	◯	◯	◯
5.5.2	Is the inventory statement updated on an on-going basis[6] and maintained at the warehouse?	◯	◯	◯
5.5.3	Does the warehouse have a Dangerous Goods management plan[7]?	◯	◯	◯
5.5.4	Is the Dangerous Goods management plan updated on an on-going basis and maintained at the warehouse?	◯	◯	◯
5.6	Marks, Labels and Placards			
5.6.1	Are all Dangerous Goods packages and / or CTUs properly marked, labeled and / or placarded in accordance with the appropriate national and international Dangerous Goods transport regulations?	◯	◯	◯
5.6.2	Is there a documented process to ensure that required Dangerous Goods package and / or CTU marks, labels and / or placards, as well as piece count are consistent with Dangerous Goods documentation requirements?	◯	◯	◯

5.7	Packaging			
5.7.1	Is there a documented process to ensure that the packaging is approved for the Dangerous Goods offered?	◯	◯	◯
5.7.2	Does the warehouse have an inspection program for the integrity of all packages holding Dangerous Goods?	◯	◯	◯
5.8	Emergency Response Procedures			
5.8.1	In the event a package and / or CTU is leaking is there a documented spill procedure, readily accessible Personal Protection Equipment, and appropriate equipment in place to properly isolate the package and / or CTU and contain the contents?	◯	◯	◯
5.8.2	Are up to date safety data sheets[8], appropriate guidebooks[9] and emergency response procedures, as applicable, readily available to warehouse employees for all Dangerous Goods managed at the warehouse?	◯	◯	◯

GUIDANCE NOTES:

[1] United Nations Model Regulations commonly known as the "Orange Book" and as amplified in the International Maritime Dangerous Goods (IMDG) Code.

[2] Dangerous goods packages may include non-bulk or bulk packaging such as drums, barrels, boxes, bags, pressure receptacles, or intermediate bulk container. CTU's may include road transport tank or freight vehicle, a railway transport tank or freight wagon, a multimodal freight container or portable tank, multiple element gas containers (MEGC).

[3] Based on international or national regulation, local ordinance, relevant fire protection standards and / or lease agreement as applicable

[4] Training should include internal procedures and processes applicable to Dangerous Goods handling specific to the employee's job functions.

[5] A Dangerous Goods inventory statement should be developed for each building or compartment where Dangerous Goods are stored. This statement should include the hazard class, common or trade name, chemical name, Chemical Abstracts Service (CAS) number, composition (pure or mixture / solid, liquid or gas), maximum aggregate quantity stored, and required storage conditions for each dangerous good listed.

[6] Relevant inventories, plans and procedures should be updated on an on-going basis. An "on-going" basis could be defined as what is required to keep the subject material relevant and up to date at all times. It may also be based on specific requirements imposed by the authority having jurisdiction. For example, where adopted, the NFPA 400 Hazardous Materials Code requires an amended Dangerous Goods Inventory Statement (or HMIS) to "be provided within 30 days of the storage of any hazardous materials that changes or adds a hazard class or that is sufficient in quantity which exceeds 5 percent for any hazard class".

[7] A Dangerous Goods management plan should include relevant general information concerning operations at the warehouse, a general site plan, a building floor plan which shows designated Dangerous Goods storage areas within the warehouse, segregation, and compatibility controls, monitoring program, inspection and record keeping, employee training, and emergency response procedures.

[8] Safety data sheets are a component of the Global Harmonized System (GHS) of Classification and Labeling of Chemicals. They should be produced when chemical substances and mixtures meet the harmonized criteria for physical, health or environmental hazards under the GHS.

[9] Appropriate guidebooks may include the "Emergency Response Guidebook: A Guidebook for First Responders During the Initial Phase of a Dangerous Goods / hazardous materials Transportation Incident (ERG)", "Dangerous Goods – Initial Emergency response Guide", "Emergency Response Intervention Cards (ERIC)", etc.

SECTION 6	FIRE PROTECTION	YES	NO	N/A
6.1	Programs and Procedures			
6.1.1	Are fire protection risk assessments[1] carried out for the warehouse and updated on an on-going basis?	◯	◯	◯
6.1.2	Is there a documented fire protection impairment program[2] established for the warehouse?	◯	◯	◯

6.1.3	Is there an established employee fire brigade at the warehouse?	◯	◯	◯
6.1.4	Is fire extinguisher training provided for all employees at the warehouse?	◯	◯	◯
6.1.5	Are there written hot work procedures in place for the warehouse?	◯	◯	◯
6.2	**Sensors and Alarms**			
6.2.1	Are manual pull fire alarms installed at the warehouse?	◯	◯	◯
6.2.2	Do manual pull fire alarms connect to an offsite central monitoring station?	◯	◯	◯
6.2.3	Are smoke / fire detection sensors installed at the warehouse?	◯	◯	◯
6.2.4	Do smoke / fire detection sensors connect to an offsite central monitoring station?	◯	◯	◯
6.2.5	Are alarms and related equipment inspected on a regular basis and maintained by a qualified third party?	◯	◯	◯
6.3	**Fire Compartments**			
6.3.1	Are designated fire compartments properly separated with fire rated walls?	◯	◯	◯
6.3.2	Are openings between fire compartments fitted with fire rated doors?	◯	◯	◯
6.3.3	Are automatic fire rated doors inspected on a regular basis and maintained by a qualified third party?	◯	◯	◯
6.4	**Automatic Sprinkler Systems**			
6.4.1	If public water supply, is minimum flow rate and pressure maintained?	◯	◯	◯
6.4.2	If public water supply, is flow rate and pressure checked on a periodic basis?	◯	◯	◯
6.4.3	If on-site tank water supply, is adequate quantity of water maintained?	◯	◯	◯
6.4.4	If on-site tank water supply, is tank inspected on a periodic basis?	◯	◯	◯
6.4.5	If fire pump installed, is the pump tested and run on a periodic basis?	◯	◯	◯
6.4.6	If fire pump installed, is the flow rate and pressure checked on a periodic basis?	◯	◯	◯
6.4.7	Are water supply control valves locked open or provided with valve tamper indicators?	◯	◯	◯

6.4.8	Are hydraulic design parameters of the system adequate for the goods in storage[3]?	◯	◯	◯
6.4.9	Is storage of goods (commodity types, configuration, etc.) reviewed on a regular basis to ensure conformity with the hydraulic design parameters of the system?	◯	◯	◯
6.4.10	Is the automatic sprinkler system adequately maintained?	◯	◯	◯
6.4.11	Is the automatic sprinkler system periodically inspected and tested?	◯	◯	◯
6.4.12	Are all areas of the warehouse (where goods are stored) adequately protected by the sprinkler system?	◯	◯	◯
6.4.13	If located in an Earthquake Zone, is system fitted with seismic restraints and bracing?	◯	◯	◯
6.4.14	Is the sprinkler system linked to an alarm system monitored by a central alarm station 24/7?	◯	◯	◯
6.4.15	Is the alarm system tested on a periodic basis?	◯	◯	◯
6.5	**Other Fire Protection Equipment**			
6.5.1	Is the facility located within close proximity to an adequate number of fire hydrants (or other adequate source of water)?	◯	◯	◯
6.5.2	Are number, type and location of fire extinguishers adequate for the warehouse (based on type of goods and configuration of storage)?	◯	◯	◯
6.5.3	Are fire extinguishers inspected on a periodic basis?	◯	◯	◯
6.5.4	If the warehouse is fitted with standpipes and / or hose stations, are they adequately maintained?	◯	◯	◯
6.6	**Firewater Retention**			
6.6.1	Has a risk assessment[4] been carried out to determine if the warehouse requires a firewater retention facility and / or risk management plan?	◯	◯	◯
6.6.2	If required, has a risk management plan for retention and control of firewater been implemented?	◯	◯	◯
6.6.3	Is the firewater risk assessment and / or risk management plan reviewed and updated as applicable in the event of significant site changes[5]?	◯	◯	◯

GUIDANCE NOTES:

[1] Risk Assessments referred to here would include those carried out by the warehouse to ensure fire protection is adequate for the goods in storage. Other risk assessments may be carried out by the local fire department or for insurance purposes.

[2] A fire protection impairment program is used to supervise the safe shutdown of fire protection systems, control potential fire hazards during impairments and restore the fire protection system to service as soon as possible.

(CONT.):

[3] This can be determined by reviewing Hydraulic design information found on the hydraulic data plate for each system installed. These plates are attached in various locations on the system and include information such as location of the design area(s), discharge densities over the design area(s), required flow and residual pressure demand at the base of the riser, occupancy and commodity classifications, maximum permitted storage height and configuration, sprinkler demand, etc.

[4] Firewater risk assessments should evaluate the risk of firewater run-off to the environment based on the significance of a fire event and the quantities of firewater, and subsequent run-off that may be generated, leading to a potential environmental hazard.

[5] Significant site changes may include relevant changes in inventory, drainage or containment systems, fire compartments or risk assessment areas.

SECTION 7	SECURITY[1]	YES	NO	N/A
7.1	Perimeter / Warehouse Exterior			
7.1.1	Is cargo handling, shipping, and receiving yard adequately illuminated (particularly in loading and unloading areas)?	◯	◯	◯
7.1.2	Is cargo handling, shipping, and receiving yard adequately controlled[2] to prevent unauthorized access?	◯	◯	◯
7.1.3	Are external dock areas including doors fully illuminated?	◯	◯	◯
7.1.4	Are external dock areas including doors covered via CCTV[3] cameras that can view all operations and movement at all times?	◯	◯	◯
7.1.5	Is personal parking restricted to designated areas[4]?	◯	◯	◯
7.1.6	Are exterior walls and roof designed and maintained to resist penetration?	◯	◯	◯
7.1.7	Is external access to roof physically locked?	◯	◯	◯
7.1.8	Are all warehouse external doors alarmed to detect unauthorized opening and linked to main alarm system?	◯	◯	◯
7.1.9	Are dock doors constructed of sufficient strength to deter and / or delay forced entry with small hand tools?	◯	◯	◯
7.1.10	Are warehouse pedestrian doors constructed to resist penetration?	◯	◯	◯
7.2	Warehouse Access Control			
7.2.1	Is access at visitor entry points controlled by an employee, guard or receptionist[5]?	◯	◯	◯
7.2.2	Is there a process in place to receive visitors outside of operational hours?	◯	◯	◯
7.2.3	Are visitors required to show a government issued photo ID?	◯	◯	◯
7.2.4	Are visitors registered when they check in?	◯	◯	◯
7.2.5	Is a visitor log maintained[6]?	◯	◯	◯

7.2.6	Is workforce entry point(s) access controlled 24 hours per day / 7 days per week?	◯	◯	◯
7.2.7	Is access to internal dock / warehouse areas or sections restricted to authorized workforce and escorted visitors based on business need?	◯	◯	◯
7.2.8	Are all drivers identified using government issued ID?	◯	◯	◯
7.2.9	Is a driver log maintained?	◯	◯	◯
7.2.10	Are all internal dock areas including doors covered by CCTV?	◯	◯	◯
7.2.11	Are views of freight being loaded / unloaded clear at all times?	◯	◯	◯
7.3	**Cargo Integrity**			
7.3.1	Are CTUs pre-loaded or staged in loaded condition at the warehouse dock or in the storage yard during non-operational hours[7]?	◯	◯	◯
7.3.2	Is a seven-point physical inspection[8] performed on all outbound dedicated CTUs?	◯	◯	◯
7.3.3	Is the seven-point inspection process documented?	◯	◯	◯
7.3.4	Are seals that meet or exceed the most current ISO 17712 standard for high security seals[9] utilized for all applicable shipments?	◯	◯	◯
7.3.5	Are there documented procedures in place for management and control of seals, CTU door locks, and other security equipment?	◯	◯	◯
7.3.6	Are seals affixed or removed by authorized personnel only?	◯	◯	◯
7.3.7	Are procedures in place to ensure cargos shipped and received are validated at point of handover by conducting a manual and / or electric piece count?	◯	◯	◯
7.3.8	Is the handover / validation process documented?	◯	◯	◯
7.3.9	Are abnormalities found during the handover / validation process consistently recognized, documented, and reported?	◯	◯	◯
7.3.10	Are truck driver ID, cargo pick-up documentation or other specified pre-alert details[10] validated prior to loading?	◯	◯	◯
7.4	**Security Systems[11]**			
7.4.1	Are all intruder alarm systems activated during non-operational hours and linked to the main alarm system?	◯	◯	◯
7.4.2	Are alarm events monitored 24 hours per day / 7 days per week / 365 days per year via an internal or 3rd party external monitoring post?	◯	◯	◯
7.4.3	Is the monitoring post protected from unauthorized access[12]?	◯	◯	◯

7.4.4	Are all security system alarms responded to in real-time 24 hours per day / 7 days per week / 365 days per year?	◯	◯	◯
7.4.5	Are alarms acknowledged by monitoring post and escalated promptly[13]?	◯	◯	◯
7.4.6	Is there a documented procedure to ensure alarm system access (including servers, consoles, panels, networks, and data) is restricted to authorized individuals or system administrators?	◯	◯	◯
7.4.7	Are access privileges promptly updated when individuals depart the organization, change roles, or no longer require access?	◯	◯	◯
7.4.8	Does the alarm system transmit an alert on power failure or loss?	◯	◯	◯
7.4.9	Is access tightly controlled to CCTV system (including hardware, software, and data / video storage)?	◯	◯	◯
7.4.10	Is CCTV system[14] only viewed by authorized personnel?	◯	◯	◯
7.4.11	Does the warehouse have documented maintenance programs in place for all physical security installations / systems to ensure functionality at all times?	◯	◯	◯
7.4.12	Is security system functionality verified on a regular basis?	◯	◯	◯
7.5	**Policy and Procedures**			
7.5.1	Does the warehouse maintain an emergency contact list for security incidents?	◯	◯	◯
7.5.2	Is the emergency contact list updated regularly?	◯	◯	◯
7.5.3	Does the warehouse have a formally appointed person responsible for security on site?	◯	◯	◯
7.5.4	Does the warehouse maintain (and communicate) a documented security policy, including cybersecurity, that ensures all relevant persons (i.e., employees and contractors) are clearly aware of security expectations?	◯	◯	◯
7.5.5	Does the warehouse conduct vulnerability risk assessments that are documented and recognize the likelihood and impact of security related events[15]?	◯	◯	◯
7.5.6	Is access to shipping documents and commercially sensitive information on stored goods controlled[16]?	◯	◯	◯
7.5.7	Are documents safeguarded until destruction according to applicable regulation or customer requirement?	◯	◯	◯
7.5.8	Does the warehouse maintain records of all collections and proof of deliveries[17]?	◯	◯	◯

7.5.9	Is there a documented procedure, log and / or key plan to track how keys are managed and controlled?	◯	◯	◯
7.6	**Information Technology (IT)**			
7.6.1	Has there been a screening conducted for (new) employees by HR?	◯	◯	◯
7.6.2	Has the warehouse installed appropriate software and hardware protection for its computer systems to protect against common cybersecurity threats such as malware or internal or external intrusions?	◯	◯	◯
7.6.3	Are measures in place to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities?	◯	◯	◯
7.6.4	Does the warehouse have a system in place to identify unauthorized access of IT systems or data or abuse of policies and procedures?	◯	◯	◯
7.6.5	Is employee or other authorized user access to IT systems restricted based on job description or assigned duties?	◯	◯	◯
7.6.6	Is user access to IT systems safeguarded against infiltration[18]?	◯	◯	◯
7.6.7	Do all devices, including personal devices used for work purposes, adhere to warehouse cybersecurity policies and procedures including regular updates and means of secure access to warehouse IT systems?	◯	◯	◯
7.6.8	Does the warehouse employ measures to prevent the use of counterfeit or improperly licensed IT products?	◯	◯	◯
7.6.9	Is warehouse data backed up on a regular basis as appropriate?	◯	◯	◯
7.6.10	Is all sensitive and confidential data stored in an encrypted format?	◯	◯	◯
7.6.11	Does the warehouse account for IT equipment or media that contains sensitive information through regular inventories?	◯	◯	◯

GUIDANCE NOTES:

[1] The level of security should be based on on-going risk assessments considering the goods in storage and location of the warehouse. Level of risk will depend on parameters such as over-all value, consumer demand, ease of sale on black market, degree of danger represented by the goods (such as highly toxic commodities) and / or significant impacts created by the loss of the goods. Location of the warehouse also plays a role as those facilities located in higher crime areas or areas of civil unrest may elevate the risk of theft, tampering or loss. The recommendations included in this checklist should be considered as a minimum for warehouse storage.

[2] Controls to prevent unauthorized access may include: a physical barrier enclosing the yard area; gates that are manned or electronically controlled; visible perimeter signs indicating no unauthorized access or parking; visible signs on external doors or walls instructing drivers, visitors, etc. to proceed to appropriate entry location; or periodic sweeps or patrols by CCTV, guards, or responsible member of workforce.

[3] CCTV systems with color or day / night capability are recommended.

[4] It is recommended that designated parking areas be at least 25m walking distance from dock areas.

[5] Persons controlling visitor access points should be trained on entry / exit procedures including required information, badge issuance, escort requirements, etc. as applicable.

[6] It is recommended that visitor logs be maintained for at least 30 days.

[7] This practice is not recommended.

(CONT.):

[8] A seven-point physical inspection includes inspection of the CTU undercarriage, right and left sides, front wall, ceiling / roof, inside / outside doors and floor and any locking mechanism as applicable.

[9] Qualifying cable and bolt seals are acceptable.

[10] Pre-alert details are provided prior to pick-up and validated at time of pick-up. Details may include driver name, carrier name, truck license tag number, time of pick-up, order number, etc.

[11] Security systems may include lighting, CCTV, access control and / or intruder detection systems as applicable based on the level of risk presented by the goods in storage and location of the warehouse.

[12] Unauthorized access may be controlled by means of an electronic access control system, physical locks, biometric scanners, etc.

[13] To ensure timely response to potential intruders, it is recommended that any alarm activations are escalated in less than 3 minutes.

[14] It is recommended that CCTV systems include digital recording capability with recordings stored for a minimum of 30 days where allowed by local law.

[15] It is recommended that security vulnerability risk assessments be conducted at least annually (or more frequently as risk factors dictate or in the event of a security breach). These assessments should include the testing of IT infrastructure security.

[16] Access to shipping documents and commercially sensitive information should be controlled on a "need to know" basis with all access monitored and recorded.

[17] It is recommended that applicable records be maintained for a period of not less than two years to ensure their availability for investigations as required.

[18] Access may be protected through the use of strong passwords, passphrases or other forms of authentication that are changed on a regular basis or as soon as possible in the event of system compromise.

SECTION 8	EMERGENCY RESPONSE	YES	NO	N/A
8.1	Emergency Response Plan			
8.1.1	Is there an emergency response plan for the warehouse?	◯	◯	◯
8.1.2	Does the plan consider fully the hazard and nature and extent of the possible emergency[1]?	◯	◯	◯
8.1.3	Does the plan consider the consequences and the possible effect on people and the environment?	◯	◯	◯
8.1.4	Does the plan include provisions for escape and / or rescue of affected warehouse personnel[2]?	◯	◯	◯
8.1.5	Does the plan consider all the activities, urbanization etc. that are adjacent to the facility?	◯	◯	◯
8.1.6	Does the plan complement the plan that the Port or Local Authority have developed and is there effective liaison with the Authorities in place and ongoing?	◯	◯	◯
8.1.7	Does the Plan consider escalation of the incident due to deteriorating conditions (including weather) and/or through cumulative effects?	◯	◯	◯
8.1.8	Has the Plan been tested, and practice drills carried out with the third-party services and response teams (especially the Incident Controller[3])?	◯	◯	◯
8.1.9	Has the Plan been adapted and kept under review to respond to changing circumstances, new facilities, new cargoes and equipment, changes to the surrounding infrastructure and activities?	◯	◯	◯

8.2	Emergency Response Personnel			
8.2.1	Are there selected and trained essential personnel who will have a role to play in emergency response, especially the Incident Controller?	◯	◯	◯
8.2.2	Have all the relevant authorities and third-party services been informed about the roles in the warehouse organization including contact numbers?	◯	◯	◯
8.2.3	Has an Emergency Control Center[4] been established?	◯	◯	◯
8.3	Emergency Response Information			
8.3.1	Has a Dangerous Goods Inventory Statement been developed for the warehouse?	◯	◯	◯
8.3.2	Is the Dangerous Goods Inventory Statement updated on a periodic basis and provided to the local fire department?	◯	◯	◯
8.3.3	Are up to date emergency response procedures, including safety data sheets where provided, readily available to local fire department and other relevant third parties for all Dangerous Goods managed at the warehouse?	◯	◯	◯
8.4	First Aid			
8.4.1	Has an adequate number of employees been trained in first-aid techniques?	◯	◯	◯
8.4.2	Are the means for first-aid[5] available to warehouse employees in adequate numbers?	◯	◯	◯
8.4.3	Are the means for first aid easily accessible in the warehouse?	◯	◯	◯

GUIDANCE NOTES:

[1] Examples where an emergency response plan may be required include explosion, fire, loss of power, severe weather, active shooter, riot, strike, etc.

[2] This would include the development of escape and emergency routes; and ensuring these routes (and exits) are freely accessible with appropriate signage, not blocked, obstructed by parking or locked.

[3] The incident controller is responsible for overall management of an incident. This will include coordination of emergency response resources, staff, and third-party services.

[4] An emergency control center can be an installation or activity from which a series of operations related to emergency response is directed.

[5] The means for first aid will vary according to the activity carried out at a particular warehouse. Some examples of items that may be included are information pertaining to relevant first aid treatments, sterile dressings of various sizes and shapes, bandages, safety pins, adhesive dressings, sterile wipes, gloves, face shields, foil blankets, burn dressings, clothing shears, antiseptic creams, scissors, tweezers, automatic external defibrillators (AED), etc.

ICHCA

E: secretariat@ichca.com

W: www.ichca.com

IVODGA

T: 1-518-761-0263

E: mail@ivodga.com

W: www.ivodga.com

www.linkedin.com/company/the-international-vessel-operators-dangerous-goods-association-ivodga

NCB

E: ncbnyc@natcargo.org

W: www.natcargo.org

WSC

Anna Larsson, Communications Director, World Shipping Council

E: alarsson@worldshipping.org

W: www.worldshipping.org