

Mandatory requirements for cross-border suppliers

IKEA Security Measures and Requirements for Suppliers and Factories

Before being approved and able to deliver to IKEA, all Suppliers will be expected to meet the standards as defined in the IKEA Security Measures and Requirements for Suppliers and Factories at each of its manufacturing units that delivers goods to IKEA.

Each manufacturing unit delivering products to IKEA will undergo Security reviews which will be completed on a risk basis or randomly.

These requirements cover the areas of

1. Physical Security
2. Access Controls
3. Procedural Security
4. Education and Training
5. Personnel Security

The initial review will be in the form of a questionnaire and will be subject to physical site visits and confirmation.

Government Recognized Security Programs

It is recommended that Suppliers and/or Factories be certified in a Recognized Government Security Program (Authorized Economic Operator Full or Security (AEO) Japan/Korea/Europe/Israel, United States Customs-Trade Partnership Against Terrorism (C-TPAT), New Zealand Customs Secure Export Scheme, Canada Partners in Protection (PIP), Mexico New Scheme of Certified Companies etc.), or if not certified in one of these programs have equivalent minimum security criteria and processes in place that meet the Ingka Procurement LLC Security Requirements for Suppliers and Factories as defined here in the Ingka Procurement LLC Security Measures and Requirements for Suppliers and Factories.

1. PHYSICAL SECURITY

1A PERIMETER SECURITY

Perimeter and Building Structure Standard:

Walls and Fences: Many factories are within a compound. Other factories consist of free-standing buildings. Where feasible a wall or fence is advisable around any compound or factory building in order to minimize the risk of unauthorized access. The wall or fence must be high enough to discourage entry and **MUST** be made of a material strong enough to withstand attempts to penetrate it. A deterrent such as barbed wire or broken glass on the top of the wall or fence may be used. Perimeter wall or fencing must be reviewed periodically for weaknesses or possible penetration. Inspection and report records should be maintained.

Mandatory requirements for cross-border suppliers

Access Points to the Wall or Fence: The wall or fence for the factory compound or the factory building may have one or multiple entrances and exits. There **MUST** be some type of security at all access points. This security may consist of a guarded checkpoint, locks, alarms, or other security measures. Outside business hours, entrances and exits **MUST** be kept locked and measures must be in place to prevent access by unauthorized persons. Guards at access points are recommended.

1B EXTERIOR/INTERIOR SECURITY

Lighting: Outside and inside lighting **MUST** be in place and should be adequate enough to assist in identifying unauthorized persons on the premises, persons in areas where they do not belong, and other inappropriate activities. There **MUST** be lighting in security or guard shack, parking areas, cargo receiving areas and cargo loading areas is required.

Parking: Parking areas should be evaluated from a security perspective. Where possible, parking areas for visitors should be separated from those parking areas used by employees but **MUST** be separate from those areas used for cargo-receiving. Cargo-loading/unloading areas must be separated from other parking areas.

Building Materials: All buildings **MUST** be constructed of materials that resist unlawful entry and protect against outside intrusion and penetration. It is recommended that the building be checked periodically to ensure that there has been no outside intrusion and penetration. Inspection and repair records should be retained.

Access Points/Entrances and Exits: The factory may have one or multiple entrances and exits. There **MUST** be some type of security at all access points. Doors **MUST** be made of strong and durable materials that cannot be easily broken or penetrated. Entrances and exits **MUST** be secured with locks and kept locked after working hours. Alarm systems are an ideal method of security, and if possible, all doors should be protected with an alarm. Guards at access points are recommended. If the factory has separate cargo-receiving and cargo-loading entrances and exits, these **MUST** be evaluated with the same security considerations in mind.

Windows: Windows, where present, **MUST** be set in secure frames made of strong and durable materials, preferably metal. Windows, where present, **MUST** be secured with locks, particularly windows on the lower floors. Alarm systems on the windows are ideal. Consideration may be given to installation of steel bars or mesh where windows are not present or to prevent breakage of glass, although this must be weighed against the risk that would exist if windows could not be used for egress in an emergency.

Exterior/Interior Storage Areas:

Exterior: The exterior storage areas should be well lit. Any exterior storage area outside the factory building should have physical barriers to deter and guard against unauthorized access. Fencing is recommended. It **MUST** have locks at a minimum, and/or alarms, or other security devices at all entrance and exit points. Guards may also be used to prevent unauthorized access to these areas.

Mandatory requirements for cross-border suppliers

Interior: It is advisable to maintain separate storage areas or space for raw materials, finished goods, dangerous goods (must be restricted access), and/or other specified items. If the separate storage area is within the factory, it should be separated by a door, gate, cage or other physical barrier. Measures **MUST** be taken to restrict access to such areas. Guards may also be used to prevent unauthorized access.

For both interior and exterior areas a written record of the movements of materials into and out of storage areas **MUST** be maintained. It is preferable to keep the finished goods of each customer separated within a secure area. If area is locked, access to keys must be limited to appropriate management/supervisory personnel.

1C SECURITY PERSONNEL

Security Personnel Standard:

Designated Personnel: The factory **MUST** have a designated managerial level employee in charge of security. Written security procedures **MUST** be maintained and should periodically be reviewed and updated.

Careful consideration must be given to determining which personnel will have keys and the codes to locks and alarms, and to the return of keys and the change of codes in the event of staff turnover.

Security Guards: Hiring of security guards is an excellent step in establishing appropriate security procedures. Consideration must be given to the number of guards; days and hours guards will be on duty, and areas that will be patrolled. The security guards should carry beepers, walkie-talkies or mobile phones in order to allow them to communicate promptly any security breach.

When security guards are employed either directly or through an agency, background /police record checks **MUST** be performed and periodically refreshed. Guards should be properly trained in security measures and undertake periodic training to remain relevant

Guards should regularly check all yard holding areas, internal and external enclosures, including doors, windows, perimeter fencing, gates and fences, to ensure that there has been no breach and that the enclosures are in good order.

1D COMMUNICATION SYSTEMS

The factory **MUST** have an internal communication system, whether in the form of an intercom, walkie-talkies, telephones, or other methods, in order to allow communication by security guards or employees if a problem arises. There should also be an external communication system to allow the factory to contact local authorities if necessary. Procedures should exist to notify the local police of any unusual or illegal activities.

Mandatory requirements for cross-border suppliers

2. ACCESS CONTROLS

Processes **MUST** be in place to prohibit unauthorized access to all points of ingress and egress, shipping, loading dock, cargo and storage areas, as well as associated electronic systems and data. Any restricted areas must be clearly marked as such.

2A Employee Access:

A process **MUST** be in place to identify all employees entering or exiting the facility. An effective means of monitoring employee movement is through the use of employee badges or other forms of identification that identify persons as factory employees. It is recommended that such badges be checked when employees enter and leave the factory, and that employees be required to display these badges while at work. Badges could be used to identify or restrict access to restricted areas.

Alternatively, a security guard may utilize an employee listing, which is updated regularly to reflect both new and former employees. Employees should not be permitted in areas of the factory not necessary to the performance of their jobs.

Unauthorized personnel **MUST** be challenged.

2B Deliveries / Dispatches

Factory **MUST** have measures in place to prevent the unauthorized access to the premises by services providers, including deliveries and dispatch equipment and representatives. The arrival of trucks/containers should be by appointment with procedures in place to secure matching of the truck/container to the appointment. Some form of photo identification should be required upon arrival at the facility.

It is a **MUST** that all trucks/containers and drivers delivering or picking up goods are logged upon arrival at the facility and inspected prior to entrance to premises in accordance with IKEA minimum 7- or 17-point inspection security requirements or departure from the facility for containers and/or tractor/trailers. The use of security guards is ideal for this function. Log records and inspection records performed at point of ingress and egress must be retained and periodically reviewed by designated security manager or general management. This applies to trucks owned by the factory and drivers employed by the factory.

Procedures must be in place for the refusal of entry to any driver/container/carrier or such that does not meet the minimum-security requirements or pass the 7- or 17- point inspection.

2C Visitors /Factory Access

All visitors and their vehicles entering and exiting the factory must be checked in and out, and a written log of visitors retained. Visitors **MUST** present some form of photo or positive identification upon arrival at facility. It is recommended to check with the factory employee who is scheduled to meet with the visitor before allowing the visitor access, and that the visitor be escorted at all times while within the factory. Visitor should be required to wear a visitor badge at all times while within the factory.

Mandatory requirements for cross-border suppliers

Through education and training employees and management should have a process in place to challenge unauthorized visitors. All co-workers should know the policy and process.

2D Documentation/Systems

Access to shipping information, systems and documentation **MUST** be restricted to only those employees needing access as a means of performing their job. The factory should transmit and store shipping information by secure means, such as computers with appropriate passwords and firewalls. When necessary to send hard copy documentation, the use of a courier for delivery of hard copies of shipping documents is recommended. Access to systems, software and programs is controlled and restricted through the use of individual assigned accounts to authorized persons. Systems access **MUST** require password protection and system **MUST** mandate periodic password changes. It is recommended that factory have written procedures in place to identify improper access, tampering or alteration of data by IT personnel or factory management.

The accuracy and integrity of the data and documentation is very important to guard against misuse. Procedures **MUST** be in place to ensure the accuracy and completeness of data and documentation.

3. PROCEDURAL SECURITY

Procedures and programs **MUST** be in place to protect against the introduction and/or exchange of illegal or un-manifested materials and/or the loss of legal and manifested materials. This **MUST** include but not be limited to; seal control procedures, conveyance inspection process and loading verification processes. Procedures **MUST** be in place and documented for verifying seals on containers/trailers and ensuring the conveyance hardware and fasteners are appropriate and secure to deter easy access after sealing. Procedures **MUST** be in place and documented for detecting and reporting shortages and overages. This should be done at a supervisor, management or a designated security representative. There should be procedures for notifying law enforcement in cases where anomalies or illegal activities are detected or suspected by the company.

Container/trailer integrity should be maintained to protect against the introduction of unauthorized persons, personnel and material. There **MUST** be a process that includes verification of the seal that meets or exceeds PAS ISO 17712, as well as any Tamper Evident Devices and their corresponding serial numbers when applied to conveyance. Conveyance security **MUST** include the physical search of all readily accessible areas, the securing of all internal/external compartments and panels and include a focused look at the locking mechanisms and door hardware to ensure there are no easily accessible bolts where rivets should be or defective fasteners or hinges. There should be a documented process for rejecting compromised conveyances back to the carrier. There should also be a documented process for reporting cases in which un-manifested materials, or signs of tampering, are discovered.

Mandatory requirements for cross-border suppliers

3A Goods

A supervisor should oversee incoming and outgoing goods. Written records of all goods should be maintained indicating the date of receipt, the date of shipment, a description and marking of the cartons/bales, etc., and the weight and quantity. The factory should also monitor shortages and overages in incoming and outgoing goods. Shortages or overages should be noted in writing and reported to a designated supervisor.

Production and packing records should accurately reflect the use of raw materials and packing materials. End of line, finishing and packing areas should be well supervised and monitored.

Prior to loading of container/trailers, a 7-point inspection **MUST** be conducted and needs to include a review of the inside walls, ceiling and floor for potential alterations. Inspections should be documented, and records retained.

Controls **MUST** be in place to detect if packages may have been tampered with between time of packing/staging and time of loading. Additionally, procedures **MUST** be in place to detect and resolve overages/shortages between time of packing/staging and the time of loading container.

3B Hazardous Material

All hazardous materials **MUST** be

- Properly labeled as such
- Stored separately from other production and raw material areas
- Have restricted access

3C Shipping Containers

Seals:

Standard procedures **MUST** be in place and documented to verify and control the use of security seals for shipping conveyances. Procedures **MUST** cover seal verification for Arrivals, Unloading and upon Dispatch. Records of seal inspections/verifications must be retained

Seals **MUST** meet or exceed the PAS ISO17712 standards. For Ingka Procurement LLC business only PAS ISO17712 can be used. Seals **MUST** be stored in a locked or secured area with limited access by those authorized to distribute and use seals and a limited number of designated employees should be authorized to use and distribute seals. A seal control procedure, record of use and inventory process must be in place.

Shipping Conveyances (containers, trailers, rail cars, etc.)

Only IKEA designated and approved logistics and transportation service providers can be used to pick up or transport IKEA cargo. Conveyances **MUST** be well-maintained and in good condition. Conveyances in poor condition or in need of repair should not be used and should be rejected back to service provider providing the equipment. There should be a documented process for rejecting compromised conveyances.

Mandatory requirements for cross-border suppliers

Incoming container content should be verified against manifests for overages/shortages and procedures should be in place to resolve un-manifested materials. While on premises, whether loaded or unloaded, shipping containers **MUST** be kept in a secure area or staged in a secure fashion so as to prevent unauthorized access (locked and/or sealed). Manifests and shipping documents should accurately reflect contents and seal information associated with a shipment. All documentation must be maintained.

Conveyance security **MUST** include a physical inspection of shipping conveyances in accordance with methods referenced in **Appendix A Container Inspection Methods** of this document and that includes inspection and search of all readily accessible areas, the securing of all internal/external compartments and panels and include a focused look at the locking mechanisms and door hardware to ensure there are no easily accessible bolts where rivets should be or defective fasteners or hinges. All inspections should be documented. There should also be a documented process for reporting cases in which un-manifested materials, or signs of tampering, are discovered.

4. EDUCATION AND TRAINING

Training programs **MUST** be provided to all employees to make them aware of the need to prevent unauthorized access to the factory and address the issues of theft prevention and product and/or shipment tampering. Such education and training should include all levels of employment, new hires as well as periodic updates. Records should be retained of training conducted.

Factory should have a procedure in place for reporting security breaches and employees should be instructed regarding the reporting procedures in the event of any security breach. Training should include visitor identification and challenges as well as IT security policies, procedures and standards. As part of the education and training programs appropriate and compliant disciplinary measures should be discussed.

5. PERSONNEL SECURITY

A record **MUST** be maintained of all personnel. Records **MUST** include who have keys or codes to locks, alarms and systems. Controls must be in place for maintaining accurate records.

Employment Screening

At a minimum, the factory **MUST** have prospective employees complete a basic job application. The factory **MUST** screen and interview prospective employees. Information concerning previous employment and references should be obtained during the screening process. If identification cards or records are available, copies should be retained as part of the personnel file. It is recommended that photographs of employees be retained as part of the personnel file. Where feasible and allowed, it is recommended that the factory attempt to verify information provided by job candidates by, among other things, contacting past employers and reviewing documentation establishing the identity of the applicant. Records

Mandatory requirements for cross-border suppliers

of these interviews and investigations should be maintained. Where available and feasible to do so, it is recommended that background or police record checks be performed for those employees in IT and security.

Termination Procedures

Factory **MUST** have in place procedures that address the termination of employment for all employees that leave the company. At a minimum, termination procedure **MUST** include retrieval of employment badges, access keys or cards, removal of all system access and notification to security personnel. For employees whose employment is terminated by the company, procedures should include an escort from premises. For employees who terminate their own employment, exit interviews are recommended to understand why they are leaving. Records of these interviews should be retained.

Mandatory requirements for cross-border suppliers



Factory Security Assessment Checklist

The following questionnaire has been developed based upon the IKEA Supplier Security Measurements and Requirements, which were created based upon the U.S. Customs CTPAT Foreign Manufacturer Recommendations and published best practices in this area.

Minimum requirements are identified below in **Highlighted Grey and bold**. If these minimum requirements are not met, then immediate corrective action is required. Other recommendations not met will be commented upon and may impact on the overall approval rating.

I: FACTORY INFORMATION

| | |
|---|--|
| Factory Name | |
| Address | |
| Contact Person | |
| Tel | |
| Fax | |
| E-mail | |
| Type of Facility | |
| Manufacturing Floors | |
| Warehouse/Storage Area | |
| Container Yard | |
| Weekdays of Operation | |
| Hours Operation | |
| Date of Response | |
| C-TPAT or mutually recognized security program assigned | |
| Certification Number | |
| Date of first certification | |
| Date of last recertification | |

Mandatory requirements for cross-border suppliers

SUMMARY OF AUDIT RESULTS

(A = Acceptable; CAPR = Corrective Action Plan Required; U = Unacceptable; immediate corrective action must be performed)

| | A | CAPR | U |
|-----------------------------------|----------|-------------|----------|
| 1. Physical Security | | | |
| A. Buildings/Perimeter | | | |
| B. Interior/Exterior Security | | | |
| C. Security Personnel | | | |
| D. Communication Systems | | | |
| 2. Access Controls | | | |
| A. Employee Access | | | |
| B. Deliveries/Dispatch Access | | | |
| C. Visitor/Factory Access | | | |
| D. Documentation/System Access | | | |
| 3. Procedural Security | | | |
| A. Goods | | | |
| B. Hazardous Materials | | | |
| C. Shipping/Receiving | | | |
| 4. Security Education / Awareness | | | |
| 5. Personnel Screening | | | |

Mandatory requirements for cross-border suppliers

Begin Questionnaire

1 – Physical Security

1A. Physical Security – Buildings/Perimeter

| Item # | Requirement | Yes/No | Comments |
|--------------|---|--------|---|
| 1.A.1 | Does the facility have a compound (area outside factory building for parking and/or receiving delivery vehicles)? | | (if no skip to 1.A.13) |
| 1.A.2 | Does facility have a gatehouse or guard shack? | | If yes who controls the gatehouse: |
| 1.A.3 | The outside entrances and exits of the factory compound/grounds have: a. Security Checkpoints b. Locks c. Alarms d. Gates/Guard Shack e. Other : _____ (Describe) | | (Indicate all that apply) |
| 1.A.4 | Is adequate lighting provided to external premises? | | |
| 1.A.5 | Are entrances and exits of factory compound kept locked after working hours? | | |
| 1.A.6 | If factory has a compound, is perimeter fencing present? a. Fencing material used: b. Height of fence: | | (If not, are there compensating controls?) |
| 1.A.7 | Fence has top-cover barrier? | | If so, provide type of top cover: |
| 1.A.8 | Fence surrounds entire compound? | | If not, what areas are not surrounded: |
| 1.A.9 | Is fencing coverage sufficient? | | |
| 1.A.10 | Are Guards present at the access points of fence during opening hours? | | Must be yes, if yes for 1.A.2. Must be yes if no to 1.A.4. |
| 1.A.11 | Periodic inspections are performed of fencing and buildings and records of inspections are maintained. | | |
| 1.A.12 | Records are maintained of repairs of perimeter fencing and building structure, the result of periodic inspections? | | |

Mandatory requirements for cross-border suppliers

| Item # | Requirement | Yes/No | Comments |
|---------------|---|--------|----------|
| 1.A.13 | Buildings are constructed of materials that resist unlawful entry? | | |

1B. Physical Security – Interior / Exterior Security

| Item# | Requirement | Yes/No | Comments |
|--------------|---|---|---|
| 1.B.1 | Is adequate lighting provided for: a. Internal cargo areas b. Cargo receiving areas c. Cargo loading docks d. Parking Areas e. Security or guard shacks f. Entrances and Exits | | (Adequate is defined as being able to support high quality CCTV images and/or allow security personnel to identify compromise from a distance.) |
| 1.B.2 | Private and employee parking areas are physically separated from: a. Unloading/loading docks b. Container storage areas | | |
| 1.B.3 | Are there working locking devices to protect external and internal doors, windows, gates and fences? | | (Ensure locks complete, functional and capable of deterring/preventing unauthorized intrusion. If not, answer No and describe) |
| 1.B.4 | Does facility have outside product or raw material storage areas? | | |
| 1.B.5 | Is the outside storage area secured with (check all that apply) | | |
| | <input type="checkbox"/> Perimeter Fencing | <input type="checkbox"/> Gates | |
| | <input type="checkbox"/> Guards | <input type="checkbox"/> Locks | |
| | <input type="checkbox"/> Security Patrols | <input type="checkbox"/> Restricted Access | |
| 1.B.6 | Does the facility have a security alarm system (Check all areas that apply) | | (System must be operational, monitored and properly maintained) |
| | <input type="checkbox"/> Restricted Areas | <input type="checkbox"/> Building Intrusion | |
| | <input type="checkbox"/> Perimeter | <input type="checkbox"/> Entrances/Exits | |
| | <input type="checkbox"/> Windows | <input type="checkbox"/> Guard Post Area | |
| | <input type="checkbox"/> Outside Storage | <input type="checkbox"/> Loading/Receiving Docks | |

Mandatory requirements for cross-border suppliers

| Item# | Requirement | Yes/No | Comments |
|---------------|--|--------|----------|
| | Container Storage Area | | |
| 1.B.7 | Are there separate storage areas for the different types of product and raw materials? | | |
| 1.B.8 | Are these Areas separated by door/Gate? | | |
| 1.B.9 | Is a written record kept of the movement of materials between these areas? | | |
| 1.B.10 | Do security personnel or supervisors patrol the "loading or dock" areas during working hours? | | |
| 1.B.11 | Are Closed Circuit TV's utilized to monitor the activity inside and outside the facility? | | |
| 1.B.12 | Is access to CCTV monitors and equipment restricted to management and security? | | |
| 1.B.13 | Is CCTV surveillance system used for non-business hours monitoring and are recordings retained and reviewed regularly by management and/or security regularly? | | |
| 1.B.14 | Are CCTV recordings maintained digitally for review for a minimum of 30 days? | | |
| 1.B.15 | Are CCTV recordings archived for a minimum of 6 months? | | |

1C. Physical Security – Security Personnel

| Item # | Requirement | Yes/No | Comments |
|--------------|---|--------|----------|
| 1.C.1 | Does the facility have a designated managerial level employee in charge of security? | | |
| 1.C.2 | Do written security procedures exist and are maintained? | | |

Mandatory requirements for cross-border suppliers

| Item # | Requirement | Yes/No | Comments |
|--------------|---|----------------------------------|---|
| 1.C.3 | Are security guards used either as employees or outsourced? | If no skip to section 1 D | a. How many are employed: _____ b. Days of the week guards are on duty: _____ c. Hours of the day guards on duty: _____ d. Maximum number of guards on duty per shift: _____ e. Minimum number of guards on duty per shift: _____ f. What position in organization do security guards report to: _____ |
| 1.C.4 | Are background/police record checks mandated for Security Personnel? If outsourced factory must request proof of background checks | | |
| 1.C.5 | Do the Security Guards regularly check all separate areas internal and external? | | a. How often: _____ b. What areas are patrolled: _____ |
| 1.C.6 | Are records of internal/external area patrols or security checks maintained? | | |
| 1.C.7 | Are security personnel equipped with communication devices? | | |
| 1.C.8 | Is security, not safety training provided for security personnel? If outsourced factory must request proof of trainings | | Describe Training programs |

1D. Physical Security – Communication Systems

| Item # | Requirement | Yes/No | Comments |
|--------------|--|--------|----------|
| 1.D.1 | Facility has phone systems in place for employees to contact internal security personnel or local law enforcement (police)? | | |
| 1.D.2 | Facility has phone systems in place for Guards to contact local law enforcement (police)? | | |

Mandatory requirements for cross-border suppliers

2. Access Controls

2A. Access Controls – Employee Access

| Item # | Requirement | Yes/No | Comments |
|--------|--|--------|--|
| 2.A.1 | Is there an employee identification system and who is responsible for controlling ID system? | | |
| 2.A.2 | Does the identification system include the issuance of photo ID and security badges to factory employees? | | If no, describe identification system: |
| 2.A.3 | If ID badges are used, are they used to control the access of employees to restricted areas? | | If badges are not used, describe how restrictions are enforced |
| 2.A.4 | Are unauthorized personnel challenged and removed from unauthorized area? | | |
| 2.A.5 | Are restricted areas such as inside and outside loading bays, product storage, shipping and receiving offices, clearly marked as such? | | |
| 2.A.6 | Are dock or loading areas/doors considered restricted areas? | | |
| 2.A.7 | Is access to restricted areas limited to only those workers working in the area or necessary to perform their job? | | Describe how limited access is enforced/monitored: |
| 2.A.9 | Is there a documented process to control who has access keys and/or codes to locks and alarms? Access to keys and codes is limited? | | |

2B. Access Controls – Deliveries/Dispatches

| Item # | Requirement | Yes/No | Comments |
|--------|--|--------|----------|
| 2.B.1 | Are all delivery vehicles and containers entering or exiting the factory recorded or logged? | | |
| 2.B.2 | Are controls in place to record those trucks/containers leaving the factory? | | |
| 2.B.3 | Are drivers delivering or receiving cargo positively identified via photo or vendor identification before cargo is received or released? | | |
| 2.B.4 | Are procedures in place for the refusal of entry should security standards not be met? | | |

Mandatory requirements for cross-border suppliers

| Item # | Requirement | Yes/No | Comments |
|--------------|---|--------|----------|
| 2.B.5 | Are recording/logging procedures in points 2.B.1 through 4 documented? | | |

2C. Access Controls - Visitor Factory Access

| Item # | Requirement | Yes / No | Comments |
|--------------|--|----------|---------------------------|
| 2.C.1 | Is visitor access managed upon arrival at facility? | | Describe control methods: |
| 2.C.2 | Are visitors and visitor vehicles recorded or logged? | | |
| 2.C.3 | Are visitors required to present photo identification at the time of arrival? | | |
| 2.C.4 | Are visitors escorted while on the premises? | | |
| 2.C.5 | Is there a visitor pass system? | | |
| 2.C.6 | Are unauthorized persons challenged and removed if necessary? | | |
| 2.C.7 | Are there documented procedures for removal of unauthorized personnel/visitors from restricted areas? | | |

2D. Access Controls – Documentation/System Access

| Item# | Requirement | Yes/No | Comments |
|--------------|---|--------|----------|
| 2.D.1 | Is shipping information accessible only to those employees who need access in order to perform their job? | | |
| 2.D.2 | Is access to systems and software/programs controlled and restricted (computers, password protections)? | | |
| 2.D.3 | Factory has written procedures in place to identify improper access, tampering or altering of business data by I.T. personnel or factory management? | | |
| 2.D.4 | Procedures are in place to ensure the accuracy and completeness of data and documentation? | | |

Mandatory requirements for cross-border suppliers

3. Procedural Security

3A. Procedural Security – Goods

| Item # | Requirement | Yes/ No | Comments |
|--------------|--|------------|----------|
| 3.A.1 | Does a supervisor oversee the incoming/ outgoing of goods at all times. | | |
| 3.A.2 | Does factory have controls in place during packing of product to prevent introduction of unauthorized materials? | | |
| 3.A.3 | Are controls in place to prevent tampering of Product/Unit Load between packing and staging of shipment loading? | | |
| 3.A.4 | Are procedures in place to research and resolve overages and shortages between the time of staging merchandise and the time of loading container for transport? | | |

3B. Procedural Security – Hazardous materials

| tem # | Requirement | Yes/No | Comments |
|--------------|--|---|---------------------------------------|
| 3.B.1 | Does factory keep hazardous materials (biological, chemical, radiological or physical) which has potential to cause harm to humans or animals such as chemicals, paints, combustibles, irritants, corrosives etc. | If no skip this section. | |
| 3B.2 | Is hazardous material labeled? | | |
| 3B.3 | Is hazardous material stored separately? | | |
| 3B.4 | Access to hazardous material areas is restricted? | | How is restricted access enforced: |

3C. Procedural Security – Shipping/Receiving

| Item # | Requirement | Yes/No | Comments |
|--------------|---|--------|----------|
| 3.C.1 | Does factory have written seal control procedures covering points 3.C.2 through 5? | | |

Mandatory requirements for cross-border suppliers

| | | | |
|--------|--|--|---|
| 3.C.2 | Written procedures designate those employees authorized to distribute seals and those who have access to seals? | | |
| 3.C.3 | Is there a seal control/use/inventory record in place? | | |
| 3.C.4 | Are high security bolt seals that meet or exceed PAS ISO17712 standards purchased and used by factory? | | |
| 3.C.5 | Are all deliveries for outgoing goods sealed by a designated factory employee, not the driver? | | If not, describe type of conveyance used to deliver goods |
| 3.C.6 | Are containers examined for physical integrity, damage and/or contamination upon: a. receipt in compound b. before loading | | |
| 3.C.7 | While on factory premises do full or partially loaded conveyances remain sealed if stored overnight? | | |
| 3.C.8 | While on factory premises are containers stored door to door to prevent access? a. empty b. full | | If no, is there sufficient room to store door to door |
| 3.C.9 | Prior to loading/stuffing, factory has a multi-point security inspection process that includes an inspection of (check all that apply): a. Reliability of locking mechanism b. Front Wall (inside/out) c. Left Side (inside/out) d. Right Side (inside/out) e. Floor f. Ceiling/Roof (inside ceiling/outside roof) g. Inside/Outside of doors h. Outside/Undercarriage i. Inspect inside and outside for dirt, pests, larvae etc. | | |
| 3.C.10 | If damaged rivets, bolts or any door hardware are found on the empty is there a process to reject the conveyance and return to the owner? | | |
| 3.C.11 | If damaged rivets, bolts or any door hardware are found is there a documentation process that includes taking photographs? | | |

Mandatory requirements for cross-border suppliers

| | | | |
|--------|---|--|--|
| 3.C.12 | Are records maintained of this process and able to be shared with IKEA upon request? | | |
| 3.C.13 | Is there a multi-point inspection process on full conveyances that focuses on the locking mechanisms and door hardware to look for faulty or compromised/damaged bolts or rivets? | | |
| 3.C.14 | Are loaded and sealed conveyances and holding yards part of security patrols | | |

4. Education and Training

| Item # | Requirement | Yes/No | Comments |
|--------|--|--------|----------|
| 4.1 | Is security program with training and awareness required for all employees, including newly hired employees? | | |
| 4.2 | Does awareness training include IT security policies, procedures and standards? | | |
| 4.3 | Is there a mechanism for personnel to report suspicious activities anonymously? | | |
| 4.4 | Are disciplinary measures advised for breach of security during education and training? | | |
| 4.5 | Are random, unannounced internal audits conducted of security and security procedures? | | |
| 4.6 | Do you make all vendors/business partners aware of IKEA security requirements? | | |
| 4.7 | Are vendors/business partners periodically audited to ensure security protocols are followed? | | |
| 4.8 | Are records maintained of audits performed at business partners' facilities? | | |
| 4.9 | Is there documentary evidence that violations have been corrected? | | |

5. Personnel Security

| Item # | Requirement | Yes/No | Comments |
|--------|--|--------|----------|
| 5.1 | How many employees work at the facility? | | |

Mandatory requirements for cross-border suppliers

| | | | | | | |
|-----|--|----------------------|--|---|--------------------------|----------------------|
| 5.2 | Are employment applications required of employees, (includes complete name, address, birth date, prior employment, education, emergency contacts, references, etc.)? | | | | | |
| 5.3 | Is information in the application verified? | | | | | |
| 5.4 | Are prospective applicants interviewed and records of interview maintained? | | | | | |
| 5.5 | Are any of the following checks/test done as a prerequisite for employment? (check all that apply) | | | | | |
| | <input type="checkbox"/> | Background Checks | | | <input type="checkbox"/> | Drug Tests |
| | <input type="checkbox"/> | Police Records | | | <input type="checkbox"/> | Photo ID provided |
| | <input type="checkbox"/> | Finger Prints Taken | | | <input type="checkbox"/> | |
| | <input type="checkbox"/> | | | | <input type="checkbox"/> | |
| 5.6 | The above listed checks/tests are required at all level of employment? | | | If No, describe those levels they are required for: | | |
| 5.7 | Applicable forms of identification are required at time of employment and copies are retained with employee records? | | | | | |
| 5.8 | Are periodic (every two (2) to five (5) years) background checks conducted of employees? | | | | | |
| 5.9 | Factory has termination procedures that include the following? (check all that apply) | | | | | |
| | <input type="checkbox"/> | Exit interview | | | <input type="checkbox"/> | Retrieve ID badge |
| | <input type="checkbox"/> | Notify security | | | <input type="checkbox"/> | Retrieve keys |
| | <input type="checkbox"/> | Remove system access | | | <input type="checkbox"/> | Escort from premises |
| | <input type="checkbox"/> | | | | <input type="checkbox"/> | |