

GLOBAL CYBERWORKS

Supplier Code of Conduct

January 2023

This information is privileged and confidential to Global Cyberworks
Any disclosure, copying or distribution is prohibited without written consent from Global Cyberworks

Table of Contents

3	Introduction
5	Supplier code of conduct
7	Supplier code of conduct standards
40	Supplier security standards
52	Rating policy and remediation

Introduction

This manual provides specific requirements and recommended guidelines for Suppliers on how to maintain safe workplaces, respect fundamental rights,

enable environmental resilience and operate with a high standard of business transparency and ethics.

The Global Cyberworks (LF) Supplier Code of Conduct ("Supplier Code") and its related standards and guidance are based on local, national laws/regulations, the International Labor Organization's Core Conventions, and other relevant international standards.

Although Suppliers' employees in different departments have varied natures of work, the Standards contained in the Supplier Code and associated guidance are applicable to all workers, in every worksite and residential facility. All workers must be informed about their rights and entitlements under both local law and the Supplier Code. Suppliers must also do their utmost to ensure LF Standards are communicated to and respected by next-tier Suppliers that produce parts or materials for Global Cyberworks and its customers.

The LF Security Standards are the basic security measures required for the Suppliers producing LF products based on the Customs-Trade Partnership Against Terrorism (C-TPAT), Security Guidelines issued by the US Customs and Border Protection Agency and the Authorized Economic Operators (AEO) Guidelines issued by the European Commission.

At the sole discretion of Global Cyberworks and at a time of Global Cyberworks's own choosing, Suppliers may be audited according to these Standards and guidelines. During audits, Suppliers must provide full access to their facilities. During our audits we may engage with workers and their elected representatives.

Failure to comply with the required Standards and associated guidance laid out in the Supplier Code will have different consequences depending on the severity of the issue. Zero-tolerance issues must be remediated immediately and may result in Suppliers being permanently prohibited from producing merchandise for Global Cyberworks and its customers. For all other issues, the Supplier will be expected to remediate within the expected time-frame and improve future performance.

Suppliers are responsible for ensuring next-tier suppliers comply with the required

Standards and associated guidance by performing periodic assessments and training.
Assessments and training shall be performed at a minimum on an annual basis.

Supplier Code of Conduct

Global Cyberworks is committed to driving responsible business practices in our company and supply chain. We expect our suppliers to continuously improve their performance to provide **safe workplaces, respect fundamental rights, enable environmental resilience** and operate with a high standard of **business transparency and ethics**.

The Standards contained in the Global Cyberworks Supplier Code of Conduct are based on local, national laws/regulations, the International Labor Organization's Core Conventions and other relevant international standards. The Supplier Code of Conduct is applicable to all worksites utilized for Global Cyberworks sourcing and associated onsite residential facilities. Suppliers are responsible for ensuring compliance with the Standards, including for next-tier operations.

Suppliers must remediate all violations according to Global Cyberworks Standards and Guidance.



Safe Workplaces

- Responsible fire safety and emergency precautions and practices
- Responsible policies and practices on first aid and occupational safety and health
- Safe and clean dormitory, child care and canteen facilities
- Responsible chemicals and hazardous materials, special equipment and spaces safety management
- Responsible electrical, building and construction permits, policies and practices



Respect Fundamental Rights

- All work is freely chosen
- All workers meet minimum age requirements (15 or the legal age in country, whichever is higher)
- Treat all workers with respect and ensure equality of treatment
- Uphold the right to freedom of association and collective bargaining
- Responsible hiring, wages, benefits, working hours and termination practices
- Functioning grievance mechanisms



Environmental Resilience

- Establish and implement an environmental management system
- Minimize impacts of chemicals, wastewater, air emission, waste and noise pollution
- Improve energy and resource efficiency



Business Transparency and Ethics

- Suppliers are transparent and engage in continuous improvement
- Suppliers engage in ethical business practices
- Subcontracting and homeworking are authorized with prior written consent
- Business licenses meet or exceed legal requirements



Supplier Code of Conducts Standards

Safe Workplaces

Suppliers Shall Apply and Maintain Responsible Fire Safety and Emergency Permits, Precautions and Practices

Locked or systematically obstructed emergency exits are considered a Zero-Tolerance Violation that may result in evacuation and suppliers being permanently prohibited from producing merchandise for Global Cyberworks

Minimum Requirements

I. Fire safety and emergency permits and practices

- Suppliers shall have a valid fire license or acceptance letter from the local fire service authority and keep this license or acceptance letter available for review.
- Flammable and combustible¹ materials should be stored in a safe location with proper controls and appropriate warning signs (e.g. "No Smoking" Signs).
- Smoking and other activities that involve open flame, fire or ignition are prohibited in areas with flammable and combustible materials.
- Suppliers shall assign emergency response personnel (e.g. first aid manager) that are certified and/or trained, and responsible for management of emergency and health and safety policies and procedures. Emergency response personnel shall be present at every shift, and easily identifiable by all employees in the event of an emergency.
- Suppliers shall train all employees on basic fire and emergency preparedness per local law and maintain a log of employee training.
- Suppliers shall conduct evacuation drills (for fires and natural disasters) at least every six months for all shifts and floors, including dormitories of the Supplier, jointly with other occupants of the building, and maintain documentation of the two most recent evacuation drills.
- Multiple Tenancy in a Multi Storied building (MSMT) is not permitted in Bangladesh.

Good Practice

Suppliers should undertake emergency drills with relevant personnel to practice different emergency situations in different locations to practice and improve performance. Evaluate the outcomes of the drill including response time and preparedness and make the necessary corrections for improvement.

II. Adequate and functioning fire safety and emergency equipment

- A B C Type² of fire extinguishers shall be present, mounted and be the appropriate size as required by law. Fire extinguishers must be easily accessible in case of need.
- Suppliers shall maintain the correct type and adequate number of fire extinguishers in areas where flammable or combustible materials³ are stored and along emergency exit

¹ Combustible material: Any material that, in the form in which it is used and under the conditions anticipated, will ignite and burn or will add appreciable heat to an ambient fire.

Flammable material: Any material capable of being set on fire and of burning quickly.

² Fire extinguishers with a Class A rating are effective against fires involving paper, wood, textiles, and plastics. Fire extinguishers with a Class B rating are effective against flammable liquid fires. Fire extinguishers with a Class C rating are suitable for fires in "live" electrical equipment.

³ Combustible material: Any material that, in the form in which it is used and under the conditions anticipated, will ignite and burn or will add

pathways. Extinguishers shall remain accessible, be designated and visible, and have operating instructions and monthly inspection tags.

- Suppliers shall maintain all legally required fire suppression systems, such as a sprinkler and/or fire hydrant system. Fire suppression systems shall have quarterly inspection tags and be inspected annually or as required by law (whichever is the more frequent) by a licensed third party.
- Where applicable, suppliers shall maintain adequate water supply for fire suppression systems. Water supply shall be stored in a suction tank, elevated tank, or reservoir. Suppliers should monitor and inspect water supply level monthly for sufficiency. Water supply shall not be empty.
- Manual or automatic emergency alarm system shall be present in production, distribution and living areas. Manually operated emergency alarm shall be designated, accessible and clearly visible. Alarms shall have notification lighting in areas where the noise level is observed to be above ambient. Alarm signs shall be in a language understood by the majority of employees or provided through pictures or diagrams. The emergency alarm system shall be tested annually by an approved contractor or more frequently if required by law.

III. Emergency Exits are functional and accessible

- Suppliers shall equip all staircases with handrails on both sides of the staircase and height and width of staircases should be as required by local law.
- A minimum of two exits or exit doors shall be provided on every floor or any space greater than 450 m² (or according to local law whichever is more stringent) and be placed a distance apart, equal to or not less than ½ of the length of the maximum overall diagonal dimension of the building.
- Emergency exits (doors and windows) shall be designated with signs that are always visible, and in a language understood by the majority of employees. Emergency exits shall be accessible, unlocked, and manual, single release operable. Emergency exit doors shall open outward and shall have a landing platform on the exit side before any stairs.
- Emergency exit pathways shall be accessible, lit, designated with power backup directional signs that are visible in the dark⁴, lead out of the building and to a public way/ assembly point⁵, and shall have enclosed staircases or external fire escape routes.
- The emergency evacuation plan shall be posted along emergency exit pathways and entrances to stairs. Evacuation plans shall be accessible, shall have pictures or diagrams that reflect the facility's layout accurately and contain the accurate location of the assembly point as well as a "You Are Here" mark. Evacuation plans should be in a language understood by the majority of employees.
- Supplier premises shall be accessible to fire response and emergency response vehicles. Fire response or emergency response vehicles shall access the Supplier

appreciable heat to an ambient fire.

Flammable material: Any material capable of being set on fire and of burning quickly.

⁴ Visible in the dark signs: Signs with illumination from within (i.e. light bulb inside the sign); Day glow or evening glow (i.e. glow-in- dark sign)

⁵ Assembly point: A point of refuge outside of building that is protected from fire (separation or distance).

premises, shall be able to reach the Supplier by road or a cleared path and shall have unobstructed access to water sources, electrical mains and gas cutoffs.

- Suppliers shall provide emergency lighting with backup power along the emergency exit pathway and shall maintain emergency lighting.

Good Practice

Train employees and supervisors to keep emergency exits clear at all times, including the removal of all excess materials. Task one or more managers with ensuring emergency exits are clear and regularly conduct unannounced internal inspections.

Suppliers Shall Apply and Maintain Responsible Policies and Practices on First Aid and Occupational Safety and Health

Gross or repeated factory negligence leading to serious injury or loss of life is considered a Zero-Tolerance Violation that may result in suppliers being permanently prohibited from producing merchandise for Global Cyberworks

Minimum Requirements

I. Suppliers Shall Provide and Maintain First Aid and Medical Care

- Suppliers shall have first aid kit(s) with sufficient and in-date supplies (including basic supplies such as bandages, pain relievers, anti-bacterial ointment, tourniquets, tape, etc.). Supplies must be accessible to all employees during all working hours.
- There shall be an adequate number of employees trained for first aid for all shifts. Suppliers shall provide and maintain first aid training records.
- Suppliers shall have qualified medical professionals to administer medical care, as required by law. Suppliers shall provide accurate qualification records for all professionals.
- Suppliers shall have a clinic and maintain complete medical records, as required by law.
- The Supplier shall maintain a document with emergency procedures and numbers in the event of injury or accidents at each first aid location.
- Medical tests (e.g. a medical examination performed to detect, diagnose, or evaluate the health status of an employee) shall be administered in accordance with local law. Suppliers shall not improperly discriminate based on test results.
- Suppliers shall report, investigate and maintain records of employee and facility accidents, as required by law.
- Suppliers shall engage in root cause analysis and corrective and preventative action to address employee and facility accidents.
- Without sufficient evidence to the contrary, accidents that result in serious physical injury or loss of life due to facility operations in the past twelve months shall indicate

failure of health and safety precautions.

Good Practice

Suppliers should check the first aid kit inventory at minimum on a weekly basis, as well as after any first aid incident, and refill as needed.

Suppliers should have a safety program covering all contractors that includes a qualification assessment process, induction training and monitoring of activities.

II. Suppliers Shall Apply and Maintain Occupational Safety and Health Policies and Practices

- Suppliers shall maintain accurate, valid, up-to-date health and safety permits, licenses and/or certifications for the facility and its operations, as required by law. Suppliers shall maintain and post all applicable health and safety notices, as required by law and in language(s) understood by the majority of employees.
- Suppliers shall establish an Occupational Safety and Health (OSH) committee comprised of worker and management representatives that meet regularly (e.g. monthly) to establish procedures for investigating all health and safety-related incidents, ensure workplace inspections are performed, and make recommendations for actions by the committee. Maintain a log of OSH Committee activities and keep a copy available for review.
- Suppliers shall establish a policy/ code/ system governing identification, use, maintenance and training of personal protective equipment (PPE)⁶. Suppliers shall communicate and train employees at all levels on the Supplier's use and maintenance of personal protective equipment.
- Suppliers shall provide employees with appropriate personal protective equipment in accordance with the established policy/ code/ system and as required by law.
- Employees shall wear personal protective equipment in accordance with established policies, codes, and systems.
- Suppliers shall maintain personal protective equipment and keep inventory as required by law.

Good Practice

Offer flexibility in terms of various models and sizes of the required PPE where possible (while maintaining appropriate protection) to encourage PPE compliance.

III. Suppliers Shall Apply and Maintain Appropriate Lighting, Noise, Comfort and Hygiene Practices

- Suppliers shall maintain and monitor lighting and noise levels, as required by law. Where lightening and/or noise levels depart from the legal limit, suppliers shall comply

⁶ Personal Protective Equipment (PPE): Refers to protective clothing, helmets, goggles, or other garments or equipment designed to protect the wearers' body from injury. Includes the following: Protective laboratory clothing; Disposable gloves; Eye protection; Face masks; Harnesses for working at heights/ equipment to protect from falls; Self-contained breathing apparatus for working in confined spaces.

with legally required remedial action (e.g., PPE, and soundproofing).

- Suppliers shall prevent extreme temperatures by providing heating and cooling mechanisms as required by law.
- Suppliers shall implement ergonomics program(s) to identify, evaluate, and minimize risks from physically demanding work, such as manual lifting and highly repetitive tasks and to prevent work-related injuries.
- Suppliers shall provide training on ergonomics awareness to all employees and necessary equipment and tools to allow work to be conducted in an ergonomically safe manner with increased satisfaction among employees.
- Suppliers shall maintain good housekeeping and cleanliness, as required by law (e.g. suppliers shall not have accumulated dust, lint, waste, and scraps in assessed production or distribution areas). Housekeeping procedures shall be documented and kept available for review.
- Employees shall have unlimited and free access to potable water. Suppliers shall conduct water quality tests for drinking water annually or as required by law (whichever is the most frequent).
- Employees shall have unlimited and free access to toilet facilities. Suppliers shall provide and maintain enough restroom and shower facilities and number of toilets, as required by law.
- Toilet and shower facilities shall be sanitary and have complete supplies (toilet paper, soap, and drying facilities), running water, sufficient ventilation and lighting, privacy, and gender separation. Housekeeping procedures shall be documented and kept available for review.

Suppliers Shall Maintain Safe and Clean Dormitory, Child Care and Canteen Areas

- Suppliers shall maintain accurate, valid, up-to-date dormitory, child care⁷ and canteen⁸ health and safety permits, licenses and/or certifications, and facilities as required by law.
- Such facilities shall be located in an area separate from production, storage and distribution areas and shall maintain clean/ sanitary conditions (e.g. no open sewage, vermin or insects).

⁷ Child care facility: Any room in facility designated for non-working minors.

⁸ Canteen: A place where food is served in the facility.

- Ensure child care facilities are affordable for all employees or free where required by law. Never allow children near production areas nor on the rooftop.
- Emergency precautions for fire extinguishers, emergency alarms, emergency exits and lighting, evacuation pathway and plan, training drills, and electrical safety guidelines and first aid kit shall equally apply at the dormitory, canteen and child care facilities. The emergency alarm system shall be tested annually by an approved contractor or more frequently if required by law.
- Suppliers shall cover and protect the food preparation area/ canteen from contamination and test food quality and hygiene for all facilities as required by law.
- Dormitories shall provide personal storage with locks for safe keeping to dormitory occupants.
- Suppliers shall ensure there is sufficient space for occupants in dormitories and avoid over-crowding. The estimated number of persons in dormitory or dormitory rooms shall be in accordance with local regulations and shall not exceed the number reported by Supplier or maximum occupancy posted near entrance.
- Employees in dormitories shall have access to sanitary food preparation or eating areas, potable water, hot water, toilets and sleeping quarters segregated by gender.
- When a supplier recommends off site housing for employees, specific attention should be paid to renting arrangements, hygiene and housing standards.

Good Practice

Encourage the use of child care facilities by employing qualified child care providers and designing a child friendly space and activities.

Survey employees or solicit other feedback to better understand how to improve dormitory, child care and canteen facilities.

Provide sleeping facilities for married couples and families, with no more than one couple/family per room.

Suppliers Shall Ensure Responsible Chemicals and Hazardous Materials, Special Equipment and Spaces Safety Management

Minimum Requirements

I. Responsible Chemicals and Hazardous Materials Management

- Suppliers shall establish and implement a policy/ code/ system governing the correct identification, labeling, maintenance, storage, use, of chemicals and/or hazardous⁹ materials, including Emergency Management Systems (EMS). Suppliers shall train employees at all levels on how to follow and implement the supplier's chemicals and hazardous materials policy, including EMS procedures.
- Suppliers shall provide specialized training to relevant employees on how to safely handle chemicals and hazardous materials. Only trained and authorized employees shall handle chemicals and hazardous materials.
- Suppliers shall maintain complete Material Safety Data Sheets (MSDS)¹⁰ in compliance with established policies and procedures. Suppliers shall post MSDS in chemical use or storage areas in a language understood by all employees.
- Suppliers shall maintain legally required inventory of chemicals and/or hazardous materials. Suppliers shall maintain procedures that identify, keep up to date, and alert applicable personnel of new chemicals and/or hazardous materials.
- A functioning eye wash station shall be present and located at proper distance, as required according to MSDS. Chemical showers shall be present for facilities where employees risk partial or full body contact with chemicals.
- Suppliers shall store hazardous materials in a safe and secure manner. Hazardous materials should be stored separately from the production area and other facilities (e.g. child care, dormitories and canteen), away from sources of ignition¹¹ and emergency exit pathways, in a separate/ designated chemical storage area. Suppliers shall have a secondary containment system (considering 110% of actual volume) in place in case of chemical spills.
- For temporary use of chemicals near work stations, suppliers should ensure volume of chemicals used and storage arrangements are in accordance with the MSDS.
- Suppliers shall avoid the use of sandblasting and the use of substances listed in **RSL** (Restricted Substances List) and/or MRSL (Manufacturing Restricted Substance List) in their operations.
- Where chemicals are stored or regularly used, suppliers shall maintain and regularly inspect ventilation systems. Ventilation systems must function effectively and remove air

Commented [SC1]: Guessing the initial goes before the brackets

⁹ Hazardous material: Any material which has the potential to cause harm to humans, animals, or the environment, either by itself or through interaction with other factors.

¹⁰ MSDS informational document intended to provide workers and emergency personnel with procedures for handling or working with that substance in a safe manner and includes information such as physical data (melting point, boiling point, flash point, etc.), toxicity, health effects, first aid, reactivity, storage, disposal, protective equipment, and spill-handling procedures

¹¹ Sources of ignition: Spark-producing equipment (e.g., grinder, sander); Open flames; Heated surfaces (e.g., water heater, electric stove); Exposed wires; Electrical panels and equipment; Lamps; Exposed light bulbs (i.e. light bulbs hanging from electrical wire); Smoking areas.

contaminants from the workplace.

Good Practice

Maintain an inventory of the suppliers of chemicals and hazardous materials.

Gradually substitute the use of hazardous chemicals with safer alternatives through the setting of annual targets.

Ensure eye wash station equipment along with specialized PPE for handling chemicals are regularly inspected.

Employees should be trained on how to use the eye wash station (rinsing eyes for at least 15 minutes non-stop).

II. Suppliers Shall Ensure Special Equipment and Spaces Safety Management

- Permits, licenses and/or certification, as applicable, for forklifts, boilers, generators, lifts (elevators), compressors, and industrial refrigerators shall be accurate, complete, and up-to-date.
- Suppliers shall also maintain copies of valid operator licenses for employees or contractors responsible for operating heavy machinery as well as those responsible for transporting employees.
- Suppliers shall establish a policy/ code/ system governing identification and maintenance of safety guards and emergency stops, as required by law.
- Suppliers shall communicate and train employees at all levels on the Supplier's equipment safety policy.
- Suppliers shall have complete machine safety equipment. Equipment shall not pose immediate danger of severe injury due to lack of safety measures.
- Suppliers shall maintain emergency safety equipment and inspection records, specifically for forklifts, boilers, generators, lifts (elevators), compressors, and industrial refrigerators. Emergency safety equipment should be regularly inspected to ensure proper functioning.
- Suppliers should ensure a proper Lockout and Tagout (LOTO) procedure¹² is developed and enforced to protect employees from the dangers of accidental or unexpected startup of electrical equipment, or the release of stored energy during inspection or repairs.
 - Suppliers should ensure guardrails/ fences are installed with sufficient height and strength to prevent falling hazards.
 - Suppliers shall establish a policy/ code/ system governing identification, entrance into, maintenance and training of confined spaces¹³. Suppliers shall communicate and train employees at all levels on the Supplier's confined spaces policy.
 - Suppliers shall establish a policy/ code/ system governing identification, design of, maintenance, spill control and installation of aboveground and underground storage

¹² Lockout/tagout (LOTO): Procedure to ensure that dangerous machines are properly shut off and not started up again prior to the completion of maintenance or servicing work.

¹³ Confined space: Space that has limited or restricted means for entry or exit and is not designed for continuous occupancy. Confined spaces include, but are not limited to, tanks, vessels, silos, storage bins, hoppers, vaults, pits, manholes, tunnels, equipment housings, ductwork, and pipelines.

(AST and UST)¹⁴. Suppliers shall communicate and train employees at all levels on the Supplier's AST and UST policy.

Good Practice

Suppliers should have a solid rescue plan in case of emergencies related to confined spaces and AST and UST. Do not rely alone on local emergency response teams as they may not have specialized training to deal with these spaces.

Suppliers should undertake an assessment of all factory-employed drivers and their vehicles to ensure they have valid driver licenses and their vehicles have proper safety devices (proper seating arrangements and seatbelts for all passengers).

Responsible electrical, building and construction permits, policies and practices

Immediate structural collapse risk is considered a Zero-Tolerance Violation that may result in evacuation and suppliers being permanently prohibited from producing merchandise for Global Cyberworks

Minimum Requirements

I. Ensure electrical components and systems are properly maintained.

- Electrical panels shall be labeled with proper signage mentioning maximum voltage handled, accessible, and covered /dust & vermin proof or specified Ingress Protection (IP) graded. Electrical wiring shall not be damaged or exposed and not pose a trip hazard. To prevent overloading, extension cords shall not be used instead of wall outlets for permanent electrical installations.
- Suppliers shall provide electrical safety equipment to employees working around high voltage electrical hazards, including electrical safety matting, insulated tools etc.
- Train employees on the importance of wearing proper protective clothing (including proper footwear) and use of specialized equipment to protect against electrical hazards.
- Suppliers should have a certified electrician (with a valid license) to perform all electrical work at the factory and its related facilities (dormitory, canteen and child care). Suppliers shall keep an up-to-date copy of the certified electrician's license.
- Lightning protection system (LPS)¹⁵ shall be installed in the premises as protection

¹⁴ Above Ground Storage Tank (AST): ASTs are tanks or other containers that are above ground, partially buried, bunkered, or in a subterranean vault. The majority of storage tanks contain petroleum products (e.g., motor fuels, petroleum solvents, heating oil, lubricants, and used oil). Under Ground Storage Tank (UST): A UST system is a tank (or a combination of tanks) and connected piping having at least 10 percent of their combined volume underground. The tank system includes the tank, underground connected piping, underground ancillary equipment, and any containment system. UST can, e.g., contain petroleum or hazardous substances.

¹⁵ Confined space: Space that has limited or restricted means for entry or exit and is not designed for continuous occupancy. Confined spaces include, but are not limited to, tanks, vessels, silos, storage bins, hoppers, vaults, pits, manholes, tunnels, equipment housings, ductwork, and pipelines.

¹⁴ Above Ground Storage Tank (AST): ASTs are tanks or other containers that are above ground, partially buried, bunkered, or in a subterranean vault. The majority of storage tanks contain petroleum products (e.g., motor fuels, petroleum solvents, heating oil, lubricants, and used oil). Under Ground Storage Tank (UST): A UST system is a tank (or a combination of tanks) and connected piping having at least 10 percent of their combined volume underground. The tank system includes the tank, underground connected piping, underground ancillary equipment, and any containment system. UST can, e.g., contain petroleum or hazardous substances.

from lightning/thunder strikes.

- Motors, drill machines, grinding machines, electric irons, and electric kettles shall be connected with an earth continuity conductor (ECC).
- Ground fault circuit interrupter (GFCI) shall be installed and maintained in all wet or damp areas of operation.
- All electrical installations shall be well maintained annually or as required by law (whichever is the most frequent).

Good Practice

Conduct quarterly inspections of all factory electrical components and system using a certified electrician.

II. Building and construction permits are maintained and accurate.

- Suppliers shall maintain applicable building and construction permits, licenses, and/or certifications. Factory must obtain an occupancy certificate from the local fire service/authority which must be updated if alterations occur to the structure(s) (e.g. erection of roof structures or extensions, conversion of building use etc.).
- There must be a building plan on file for the production site and related facilities (dormitory, canteen and child care) that has been approved by the proper local authorities. Any alterations that occur after the initial approval must also be reviewed and approved by the proper local authorities.
- The number of floors indicated on the Supplier construction permit, license, and/or certification shall reflect the actual number of facility floors.
- The supplier production facility (exterior and interior) and related facilities (e.g. dormitory, child care and canteen) must be free of any major structural defects/ cracks/ corrosion or other issues.
- Suppliers shall maintain load plan with load marking for aboveground floors as permitted by structural design.

Good Practice

Periodically have the production site and related facilities inspected by a structural engineer to guarantee its integrity and conformity of structure. Ensure building is inspected after any natural disasters or emergencies such as flood, earthquake, fire incident, strong winds etc.



Supplier Code of Conducts Standards

Respect Fundamental Rights

Suppliers Shall Ensure all Work is Freely Chosen

All Forms of Forced Labor are Zero-Tolerance Violations that may result in suppliers being permanently prohibited from producing merchandise for Global Cyberworks

Minimum Requirements

I. Suppliers Shall Maintain Responsible Sourcing Practices

- Suppliers must not use or purchase raw materials from regions or countries with systemic forced labor.
- Suppliers must not use or purchase conflict minerals which may directly or indirectly finance or benefit armed groups.

II. Suppliers Shall Maintain Responsible Recruitment Practices

- Suppliers shall maintain a written policy incorporating Global Cyberworks requirements and best practices on responsible recruitment and hiring practices. Suppliers shall communicate the policy to any next-tier suppliers, management personnel, employees and any recruitment agencies (including labor agents, contractors etc.) used in the recruitment, hiring, or management of employees.
- Employees shall be free from paying recruitment fees or related costs. Where recruitment fees or related costs are charged this must be covered by the employer. Indirect fee charging (such as through deductions from wages and benefits) is prohibited. Suppliers must ensure that where employees have paid recruitment fees, fees are reimbursed by the employer within a reasonable period of time.
- Suppliers shall use registered or licensed recruitment agencies when recruiting migrant (domestic and foreign) employees. Suppliers shall have a written contract with all recruitment agencies used to recruit migrant employees, incorporating all principles of responsible recruitment, including the prohibition of worker paid recruitment fees and related costs.
- Migrant workers shall be free to return to their home country, in accordance with legal provisions. Employers shall ensure the safe return of foreign migrant workers at the expiry of the worker's contract, or at an earlier date in accordance with legal provisions.
- Employees shall be provided with a written copy of the labor contract before leaving their country of origin. Contracts shall specify rights with regards to payment of wages, overtime, retention of identity documents, and other issues related to preventing forced labor and shall be in a language understood by the employee. Employee's informed consent to the terms of the contract should be obtained without deception or coercion.
- Employees shall not be required to sign an incomplete labor contract. Terms of employment promised to the employee during recruitment and hire shall meet the actual terms of employment.
- Suppliers must ensure that foreign workers are in the country legally and have valid work permits.

Good Practice

Suppliers should establish due diligence measures to ensure recruitment agencies employ responsible recruitment practices. Conduct regular checks on the agency's licenses and management systems, including agency worker documents (Work permits, Pay slips, Contracts).

Conduct orientation training for migrant workers to ensure workers have not paid any recruitment fees and to ensure they understand the terms and conditions of employment.

III. Suppliers Shall Maintain Responsible Wages, Benefits, Working Hour and Termination Practices

- Suppliers must communicate their policy on freely chosen employment to management personnel, employees and next-tier suppliers. Suppliers shall require next-tier suppliers to implement the same requirements in their own operations.
- Suppliers shall not withhold wages or engage in illegal deductions or deposits, particularly as a means of recovering costs paid during the recruitment process or to prevent workers from leaving their employment.
- Suppliers shall issue pay slips to employees in the language understood by employees. Pay slips should contain, at a minimum, regular and overtime hours worked, regular and overtime earnings, incentives and deductions. Suppliers shall ensure employees understand the pay slip content.
- Suppliers shall abide by all applicable laws on mandatory overtime. Mandatory overtime (if legally permitted) shall be within legal overtime limits in policy and in practice. Mandatory overtime shall not be implemented under the menace of penalty and employees shall provide written consent to mandatory overtime requirements prior to employment or overtime.
- Employees shall not be restricted from terminating employment (other than restrictions pertaining to legal notice periods) through debt bondage, physical or verbal abuse, threats of abuse, or other forms of coercion or deception.

IV. Suppliers Shall Maintain Responsible Treatment of their Employees.

- Employees must be guaranteed freedom of movement, including access to restrooms, drinking water and medical facilities at all times.
- Workers should not be confined, imprisoned or in any way detained in the workplace or employer-operated housing, either during or outside working hours.
- Outside working hours employees shall have regular access to means of communication (mobile phones etc.).
- Workers in employer-operated housing shall not be subject to curfews, particularly those enforced with disciplinary action or electricity shut off.
- Employees shall be free to choose between Supplier-provided housing and other accommodation alternatives except in cases where restricted by law.
- Employees shall maintain custody and/or have free access to personal identity documents (including passports) and access to phones or other means of communication (outside of working hours).
- Employee treatment shall be in accordance with general principles of human dignity, including freedom from all forms of discrimination and violence in the workplace including verbal and mental abuse, coercion, threats, corporal punishment, physical abuse, sexual harassment and gender-based violence.

V. Suppliers Shall Refrain from using Prison Labor or State-Imposed Forced Labor

- Suppliers shall not utilize prison laborers in its production processes, neither within nor outside a prison facility, including through subcontracting arrangements.
- Suppliers shall not utilize state-sponsored forced laborers in its production processes, including through subcontracting arrangements.

Good Practice

Regularly interview samples of all categories of workers (contract, piece-rate or casual workers, foreign and domestic migrant workers, apprentices/trainees etc.) to check that they voluntarily agree to working overtime.

Regularly train human resource staff, supervisors and managers to prevent forced labor and to recognize forced labor indicators.

Provide lockers or other safe storage options to workers to allow them to keep passports or other identity documents

Monitor service providers and contractors (canteen, cleaning companies etc.) that provide goods or services to the supplier facility to ensure all employment of contract/agency workers is freely provided.

Suppliers Shall Ensure all Workers Meet Minimum Age Requirements

All Forms of Child Labor are Zero-Tolerance Violations that may result in suppliers

being permanently prohibited from producing merchandise for Global Cyberworks

Minimum Requirements

I. Minimum Age for Admission to Employment

- Suppliers shall, at minimum, establish written policies governing minimum age requirements and appoint responsibility to personnel for implementing the policies. Suppliers shall communicate the policy to management personnel, employees, recruitment agencies (including labor agents or contractors) and next-tier suppliers.
- Suppliers shall not employ any employee younger than the age of 15¹⁶, or younger than the age of completion of compulsory education, or legal employment age of the relevant country, whichever is higher.
- Suppliers shall request original, legal documentation to verify the employees' age at the time of hire and eligibility to work and maintain documentation or copies of documentation to demonstrate due diligence. Do not allow any exceptions including for contract, piece-rate or casual workers, foreign and domestic migrant workers, apprentices/trainees etc. or for workers in nonproduction areas (e.g. canteens, child care facilities, dormitories, sample rooms or next-tier suppliers).
- Suppliers shall have a system in place to report and remediate cases of child labor in the best interests of the child. Costs of child labor remediation, including child labor identified in next-tier suppliers or contractors shall be charged to the LF supplier. Failure to remediate cases of child labor may result in suspension of orders and permanent cessation of business.

Good Practice

In regions where age falsification is widespread, verify an employee's age through multiple information sources (government databases, medical record etc.)

Restrict access to production areas to any individuals below 15 or the legal working age (whichever is higher). Be particularly vigilant during the summer months when parents may try to bring children to the workplace.

Open child-friendly spaces in factories or offer subsidized or free child care for employees.

II. Minimum Age for Admission to Hazardous Forms of Work

- Suppliers shall ensure working conditions of employees under the age of 18, follow the law, and do not include the type of employment or work which by its nature or the circumstances in which it is carried out is likely to jeopardize the health, safety or morals of these employees.¹⁷
- Payment to juvenile workers, apprentices and trainees should be made directly to the workers and not to a third party, including their parents. Juvenile workers, apprentices and trainees must be paid in accordance with the law.

¹⁶ ILO convention 138 (Basic Minimum Age)

¹⁷ Based on ILO convention 182 and Recommendation (No. 190) on the Worst Forms of Child Labour, The following includes work which by its nature or the circumstances in which it is carried out is likely to jeopardize the health, safety or morals of these employees: Work which exposes children to physical, psychological or sexual abuse; work underground, under water, at dangerous heights or in confined spaces; work with dangerous machinery, equipment and tools, or which involves the manual handling or transport of heavy loads; work in an unhealthy environment which may, for example, expose children to hazardous substances, agents or processes, or to temperatures, noise levels, or vibrations damaging to their health; work under particularly difficult conditions such as work for long hours or during the night or work where the child is unreasonably confined to the premises of the employer.

- Suppliers shall maintain permits, licenses, parental consent forms and other documents related to the employment of apprentices, trainees and employees under the age of 18, as required by law.
- Identified apprenticeship/ traineeships shall be administered by the Supplier, as required by law.
- Suppliers shall have a system in place to report and remediate cases of hazardous form of work for child and juvenile workers. Failure to remediate cases of hazardous forms of work for child and juvenile workers may result in suspension of orders and cessation of business.

Good Practice

Have a system in place to verify that all workers engaged in high-risk activities such as working with hazardous substances, working long hours etc. are above the legal age required for such work.

Suppliers Shall Ensure all Workers are Treated with Respect

The Worse Forms of Workplace Violence (sexual harassment, physical and psychological abuse) are Zero-Tolerance Violations that may result in suppliers being permanently prohibited from producing merchandise for Global Cyberworks

Minimum Requirements

- Employees shall be free from all forms of violence at work, including all forms of gender-based violence¹⁸ (including sexual harassment) and physical and psychological abuse (including threats and coercion).
- Suppliers shall, at minimum, establish written policies and practices to address and prevent violence in the workplace (including during the recruitment process) and appoint responsibility to personnel for implementing the policies and practices. Suppliers shall communicate the policy and practices to all personnel in the workplace, including security guards.
- Suppliers shall have a system to discipline employees (including managers, supervisors and security guards) who engage in any forms of workplace violence.
- Suppliers shall have a system to ensure victims of workplace violence receive the necessary treatment and/or support services.
- Suppliers must maintain written records of incidents of workplace violence, including disciplinary measures against the perpetrator and treatment/support to the victim.
- Suppliers shall ensure that security measures (body searches etc.) are conducted in a way that is gender-sensitive and non-intrusive.

¹⁸ Gender-Based Violence is an umbrella term for unacceptable behaviors and practices – perpetrated against a person's will – that stem from unequal power relationships and negative gender roles. It includes acts that are likely to result in physical, psychological, or sexual harm or suffering; threats of such acts; and coercion and other deprivations of liberty.

Good Practice

Suppliers should provide training to prevent violence (covering all forms) both in the workplace and (where relevant) off the premises to all key personnel, particularly those in positions of power, security guards or those in direct physical contact with employees.

Suppliers should run awareness-raising campaigns to address all forms of violence in the workplace and (where relevant) off the premises.

Suppliers Shall Ensure Equality of Treatment for All Workers

Minimum Requirements

- Employees shall not be discriminated against on the basis of gender, age, religion, marital status, race, sexual orientation, disability, disease, nationality, social status, pregnancy, or trade union and/or political affiliation in employment or occupation.
- Suppliers shall not use discriminatory practices and shall maintain written policies and procedures to prohibit and prevent such practices. Suppliers shall appoint responsibility to personnel for implementing the policies and procedures and communicating them to all personnel (in a language understood by the personnel) and any recruitment agencies (including labor agents or contractors) used in the recruitment, hiring, or management of workers.
- Suppliers shall not use pregnancy or other medical testing as a condition of employment or to terminate employment. Suppliers shall not test for conditions (including but not limited to pregnancy or HIV) unless required by law and the following conditions are met:
 - i. The pregnancy test or the Medical test is required as a safety measure prior to working in a particular environment and the worker is specifically assigned to work in that particular environment.
 - ii. The cost of the Medical Test is paid by the Supplier.
 - iii. The worker receives clear communication regarding the purpose of the test and the specifics of what will be tested.
 - iv. The worker provides written consent to the test.
 - v. Suppliers do not use marriage or pregnancy as a reason for denying or terminating employment.
- Employees shall be hired and maintained in employment regardless of pregnancy or marital status. Suppliers shall ensure employment provisions and practices meet legal requirements related to pregnancy, maternity leave and return from maternity leave.
- Suppliers shall provide equal remuneration for male and female employees for work of equal value.

Good Practice

Suppliers should have training and skills-building programs in place to promote equal opportunity to employment and advancement in employment for women and other under-represented categories of employees (such as disabled persons).

Suppliers should run awareness-raising campaigns on equality in the workplace.

Suppliers should work with human resource personnel to collect data on the number of men and women by job

category and set internal targets to achieve equality of representation.

Suppliers Shall Uphold the Right to Freedom of Association and Collective Bargaining

Minimum Requirements

- Suppliers shall, at minimum, establish written policies governing freedom of association and collective bargaining and appoint responsibility to personnel for implementing the policies and communicating them to employees (in a language understood by the employees).
- Suppliers shall allow all employees to join trade unions or worker organizations of their own choosing in accordance with the law and without interference, intimidation or discrimination from management.
- Where the right to freedom of association is prohibited by law, the Supplier should not interfere with the development of legal alternatives. Suppliers shall not intimidate or discriminate on the basis of the said alternative.
- Factory management and workers should comply with all national or laws, regulations and procedures concerning freedom of association and collective bargaining. Suppliers shall participate in negotiation of legal collective bargaining in good faith.
- Suppliers must consult with workers, through trade unions or other elected representatives when taking workplace decisions that may seriously affect them (workplace closures etc.)

Good Practice

Where trade unions or worker organizations exist, suppliers should provide union or worker representatives with appropriate facilities to organize and/or assist in the development of an effective collective agreement. Suppliers should take steps to improve labor-management relations through social dialogue training.

Suppliers Shall Ensure Responsible Employment and Termination Practices

Withholding Wages for More Than Two Pay Periods is a Zero-Tolerance Violation that may result in suppliers being permanently prohibited from producing merchandise for Global Cyberworks

Minimum Requirements

I. Legal, transparent and Regular Payment of Wages and Benefits

- Suppliers shall classify¹⁹ employees and provide terms of employment, as required by law.
- Payment of wages shall be made directly to the employee or an employee-controlled account.
- Payment frequency shall be at least once per month and there shall be no late payment of wages.
- Suppliers shall maintain complete and accurate payroll and production records as required by law.
- Suppliers shall pay at least the legally required minimum wages, including payment of overtime, according to the applicable legal employee classification.
- Employees shall receive additional remuneration and non-monetary benefits as per the labor contract and/or Supplier policy (e.g., bonuses, incentives, allowances).
- Employees shall receive legally required benefits (including but not limited to the social security branches outlined in ILO Convention No. 102.²⁰). Suppliers shall make legally required employer contributions to social security schemes.
- Suppliers shall provide evidence of financial audits, including audits of payments to respective agencies for taxes, social security, workman's compensation and pension.

Good Practice

Suppliers should commit to progressively implementing a digital wage/remuneration policy and system, where appropriate, to ensure transparency of wage payments.

II. Responsible Working Hours and Overtime

- Suppliers shall have and accurately maintain time records. No time record corrections shall be made without employee written verification/acknowledgment.
- Suppliers shall ensure all regular and overtime working hours are in compliance with the law and legally required overtime waivers are maintained, as applicable. Employees shall not work more than 60 hours per week (including overtime). Suppliers shall not allow off-clock work or work to be taken home to complete a task

¹⁹ Classification: Status of the employee as per legal definition. Examples of classification are salaried, hourly, overtime exempt, trainee, apprentice, temporary, part-time, and intern.

²⁰ The nine social security branches are medical care; sickness benefit; unemployment benefit; old-age benefit; employment injury benefit; family benefit; maternity benefit; invalidity benefit; and survivors' benefit.

or quota.

- Employees shall be informed about overtime policies and processes prior to employment, considering the voluntary nature of all overtime.
- Employees shall receive rest breaks during and between shifts, and weekly, as required by law. Suppliers shall provide break hours and special working hours for vulnerable categories of employees (pregnant, elderly, disabled and young workers, etc.), as required by law.
- Suppliers shall ensure a 7th day of rest is provided to all categories of employees including security, cleaning and canteen staff.²¹

III. Responsible Termination Practices

- Employee probation periods shall be in compliance with the law.
- Suppliers shall not illegally terminate employees and shall maintain termination records, as required by law, and at minimum for the past 12 months.
- Prior to termination suppliers must ensure full payment of employee wages (including overtime payments), benefits (including social security payments), and other forms of compensation (severance etc.). [Global Cyberworks reserves the right to withhold payment of goods until all outstanding payments to workers are settled.](#)

Suppliers Shall Apply and Maintain Functioning Grievance Mechanisms

Minimum Requirements

- Suppliers must establish or participate in functioning grievance mechanisms for individuals (including workers) and communities who may be adversely impacted by their business practices.
- Grievance mechanisms should include a defined process for the reception, assessment and investigation of grievances, as well as for the way in which decisions on remedy are to be made and implemented.
- Grievance mechanisms must be captured in a formal written policy or procedure, which assigns responsibility for the procedure (or parts thereof) to specific personnel.
- Grievance mechanisms must include anonymous channels for reporting, confidentiality for victims and a no-retaliation policy which protects employees from

²¹ 7th day of rest: Employees shall not work more than six consecutive days before receiving a period of 24 hours of rest.

dismissal, penalties, and any other kind of reprisal.

Good Practice: Qualities of a functioning grievance mechanism²²

1. Legitimate: Mechanisms are fair and trustworthy
2. Accessible: To all who may be impacted by a company's actions
3. Predictable: In terms of process and available outcomes (remedies)
4. Equitable: Fair and even access to information and advice for both sides of a complaint
5. Transparent: About the process and progress of grievances
6. Compatible with internationally recognized human rights
7. A source of continuous learning and improvement for the company
8. Based on engagement and dialogue with right's holders and employee representatives

²² United Nations Guiding Principles on Business and Human Rights



Supplier Code of Conducts Standards

Environmental Resilience

Establish and Implement an Environmental Management System

Minimum Requirements

- Suppliers shall establish and implement a suitable environmental management system (EMS) that ensures compliance with applicable laws and regulation and mitigation of environmental impacts linked to their operations, with respect to chemicals, waste, wastewater, air and noise emissions, use of key resources, and other significant environmental risks.
- Suppliers shall assign personnel responsible for managing the EMS and provide training on how to monitor, track and improve performance.
- Suppliers shall identify and maintain all applicable environmental permits, legal documents (e.g. Environmental Impact Assessment), licenses, approvals and/or certifications. All documents required by law or regulation must be available for review.

Good Practice

Suppliers should have a certified EMS, such as ISO 14001 or Europe's Eco-Management and Audit Scheme (EMAS).

Suppliers should provide training to all employees covering good practices on minimizing environmental impacts during operations and production.

Suppliers should measure, track and improve environmental performance through the Higg Index Facilities Environmental Module (FEM) or other available tools.

Minimize Impacts of Chemicals, Wastewater, Air Emission, Waste and Noise Pollution

Minimum Requirements

- Suppliers shall comply with relevant national or local regulations and standards for:
 - i. Chemicals (particularly hazardous chemicals) handling and management
 - ii. Wastewater and air emission treatment and discharge
 - iii. All waste (i.e. non-hazardous waste, hazardous waste and sludge)²³ handling and disposal
 - iv. Noise mitigation and emission
- Suppliers shall maintain an updated total inventory list of all chemicals used in the factory.

²³ Sludge is a by-product of many types of wastewater treatment systems and is therefore an important parameter to sample and test.

- Suppliers shall assign personnel responsible for chemicals, wastewater, air emission, waste and noise control and management.
 - Suppliers shall provide specialized training to all employees who work directly with hazardous chemicals, waste and wastewater on how to appropriately treat and discharge the substances.
 - Suppliers shall conduct routine monitoring of wastewater discharge and sludge ²³, air emission and noise level as required by applicable local or national standards. Suppliers shall segregate non-hazardous and hazardous waste streams and routinely track and document waste (outputs and volumes) being generated.
- Suppliers shall not directly discharge wastewater and hazardous waste into the environment or expose hazardous waste to rain or surface run-off.
-

Good Practice

Suppliers should implement a waste reduction program to reduce the volume and strengths of effluents.

Suppliers should treat sludge to reduce volume and to transform it into recoverable products.

Supplier should regularly quantify and set targets to reduce its emissions of greenhouse gasses through conservation measures.

²³ Sludge is a by-product of many types of wastewater treatment systems and is therefore an important parameter to sample and test.

Improve Energy and Resource Efficiency

Minimum Requirements

- Suppliers shall comply with local government's mandated energy and water consumption and conservation policies and regulations.
- Suppliers shall identify personnel within each facility who will be responsible for all aspects of energy and resource efficiency, including tracking major consumption patterns of key resources (including energy and water) linked to their operations.

Good Practice


Suppliers should use relevant technology and tools to regularly track energy and resource consumption (e.g. sensors).

Supplier should set targets, monitor and reduce consumption of natural resources through conservation, re-use, recycling, substitution, or other measures.



Supplier Code of Conducts Standards

Business Transparency and Ethics



Suppliers are Transparent and Engage in Continuous Improvement

Full Access denied is a Zero-Tolerance Violation that may result in suppliers being permanently prohibited from producing merchandise for Global Cyberworks

Minimum Requirements

- Supplier will be expected to monitor and improve their compliance performance by meeting local law and regulations, Global Cyberworks's minimum requirements and setting targets to achieve good practice.
- Suppliers shall have management systems, policies, procedures, and practices, to ensure compliance with this Code.
- Suppliers shall appoint responsibility to specific personnel to monitor and drive performance on compliance and sustainability including training, corrective action planning, and verification.
- At the sole discretion of Global Cyberworks, Suppliers may be audited with or without prior notice. Suppliers shall grant full access to all operations including related documentation and Supplier-provided housing and child-care facilities, and grant permission to conduct confidential employee interviews. If a Supplier refuses access to Global Cyberworks or its representatives during an audit, unless the supplier presents evidence to the contrary, there shall be a presumption of intent to conceal.
- Suppliers shall not influence employee interviews during an audit, nor shall they retaliate against employees for their participation in an audit or reporting of incidents to Global Cyberworks or its customers.
- Suppliers must remediate non-compliances within the required timeframe. Failure to remediate non-compliances within the specific timeframe, or the repeated non-compliances, particularly those identified through non-transparent means (e.g. complaints or investigations) may result in a Supplier being barred from producing merchandise for Global Cyberworks and its customers.

Good Practice

Suppliers should be open and transparent with Global Cyberworks on their compliance challenges and should engage in capacity building programs to address them.

Suppliers Engage in Ethical Business Practices

Bribery and Fraud are Zero-Tolerance Violations that may result in suppliers being permanently prohibited from producing merchandise for Global Cyberworks

Minimum Requirements

- Global Cyberworks has a strict policy regarding bribery. Any offer (suggested or actual) to Global Cyberworks and/or its customers or designated representatives of money, gifts, hospitality, travel or entertainment or other consideration that is intended to or may be reasonably construed as an inducement to act (whether by commission or omission) is strictly prohibited.
- Suppliers shall not engage in fraudulent behavior, including altering the content or format of an audit report submitted for equivalency purposes.

Definition

Bribery is when a person offers, promises or gives another person a benefit directly or indirectly (e.g. through a third party) intending that benefit to influence that person to perform their job improperly, or as a reward for doing so. Benefit is not limited to cash or cash equivalent items (such as gift vouchers) and benefit includes any type of advantage. Examples of bribery (nonexhaustive) include:

- i. Payment to quality control staff to clear goods for shipment to the customer.
- ii. Offering or providing gifts to Global Cyberworks, its customers or representatives (including auditors) even where it is a locally acceptable practice.

All Subcontracting and Homeworking Activities Must be Disclosed and Authorized

Unauthorized Subcontracting and Homeworking are Zero-Tolerance Violations that may result in suppliers being permanently prohibited from producing merchandise for Global Cyberworks

Minimum Requirements

- Suppliers must not use unauthorized subcontracting or homeworkers:
 - i. All subcontractors and/or homeworkers involved with key production processes must be disclosed and receive written approval from Global Cyberworks and its customers prior to outsourcing production.²⁴
 - ii. Suppliers are responsible for ensuring next-tier Suppliers comply with this Code by performing periodic assessments and training. Assessments shall be performed at a minimum on an annual basis and records kept available for review.

Business Licenses Meet or Exceed Legal Requirements

Lack of business license is a Zero-Tolerance Violation that may result in suppliers being permanently prohibited from producing merchandise for Global Cyberworks

Minimum Requirements

- Suppliers shall maintain up-to-date, valid business license, as required by law, for its operation.

²⁴ This section only relates to goods or services produced for Global Cyberworks or its customers.

Supplier Security Standards

OVERVIEW AND POLICY

Measures must be in place to ensure the integrity and security of processes throughout the supply chain and a written policy has to be established stipulating all security procedures that need to be documented.

- Facility has a policy that requires all security procedures be documented.
- Facility has a security department/ personnel and has designated a security chief.
- Facility has conducted a site security assessment.
- Facility has documented procedure to conduct periodic security checks to ensure that the security procedures are being performed properly.
- Facility has documented security improvement action plan summarizing identified vulnerabilities and their relevant corrective.

PERSONNEL SECURITY

DOCUMENTED PERSONNEL SECURITY POLICIES/PROCEDURES

A documented process must be in place to screen prospective employees in order to evaluate risk associated criminal records, drug usage or other security related risk.

- Facility has written personnel security guidelines for hiring.
- Security guidelines for hiring are evaluated periodically to ensure their effectiveness.
- Facility has conducted a site security assessment.
- Written personnel security guidelines and requirements are being applied to contracting temporary and part time employees.

PERSONNEL SCREENING

A process must be in place to screen prospective employees and obtain application information, such as employment history and references that are verified prior to employment. In addition, periodic background checks of current employees holding sensitive positions should be consistently conducted.

- Employment applications are required of applicants.
- Facility has a process for interviewing applicants.
- Background checks are conducted on all applicants.
- Facility has a process for examining and verifying an applicant's official identification.
- Periodic and follow-up background checks are conducted on employees based on circumstances and/or sensitivity/scope of employee responsibility.

IDENTIFICATION SYSTEM

Identification system must be in place for employees for positive identification and access-control purposes for identified restricted areas.

- Company identification is required for entry of personnel.
- Security guards monitor employee arrival at the facility for positive identification to ensure that only those with a company issued ID badge are allowed entry.
- Identification has unique identifiers.
- The issuance of employee identification is centralized and controlled by a specific department.
- The control over distribution and inventory of employee ID badges and facility access keys/cards/codes is restricted to a limited number of authorized employees.
- Documented procedures and records in place for employees to return their IDs when they leave the facility permanently.
- Documented Employee Termination policy and procedures in place to retrieve IDs

deactivate access as needed and a list of terminated employees is given to security to deny access to facility.

- Lost IDs are replaced and recorded as missing in the employee's personnel file before a replacement badge is issued.
- Lost or stolen keys are replaced and recorded as missing and/or is reported immediately to the facility management.
- The security staff informed of such losses (name, ID number, etc.) to prevent unauthorized use.
- IDs are required to access restricted areas/

EDUCATION/TRAINING/AWARENESS

Employees must be made aware of the security procedures the company has in place to address a situation and how to report a security incident. Additional specific training should be provided to employees to assist them in maintaining cargo integrity, recognizing internal conspiracies, and protecting access controls. A threat-awareness program should be established and maintained and should offer incentives for active employee participation.

- Facility requires new employee orientation.
- Facility has a process in place to publicize the security procedures throughout the facility.
- Facility has written security awareness program covering awareness of current terrorist threat(s), smuggling trends, and seizures in place to ensure employees understand the threat posed by terrorist at each point of the supply chain.

PHYSICAL SECURITY

PLANT SECURITY

Facility premise should be monitored and secured to prevent unauthorized access to restricted and cargo-handling/storage areas. All buildings must be constructed of materials that resist unlawful entry.

- The facility has intrusion detection or alarm system.
- Locking devices secure facility access points and are used to control access to restricted areas.
- Facility has key control program that establishes an individual responsible for distributing and maintaining keys/cards.
- When an employee leaves the company, keys/cards are returned and codes are changed and a record is maintained of these actions.
- Buildings must be constructed of materials that resist unlawful entry.

PERIMETER SECURITY

Facility should be secured with perimeter fencing or physical barriers and deterrents and should enclose areas around cargo-handling and storage facilities that guard against unauthorized access. Gates used for entry should be manned and/or monitored.

- The perimeter of the property is secured.
- The perimeter barrier and gates regularly inspected to check for damage and attempted illegal access, properly maintained and repaired.
- The perimeter barrier and gates are properly maintained and repaired.
- Entrances/exits for the facility are secured by gates.

OUTSIDE LIGHTNING

Adequate lighting must be provided outside the facility, including entrances/exits, cargo-handling/storage areas, fence lines, and parking areas.

- The facility has outside lighting and the entire perimeter of the facility (including gates) is lighted.

CONTAINER STORAGE

Containers must be stored in a secure area to prevent unauthorized access and/or manipulation and to ensure the integrity of cargo. Container storage areas should be enclosed with perimeter fencing.

- The loaded stored containers/trailers are sealed with high security seals that meet or exceed ISO/PAS 17712 standard.
- Containers are stored in a designated container storage area surrounded by a secure fence or wall.
- Facility has documented procedures in place for reporting and neutralizing unauthorized entry to container storage areas.

SECURITY FORCE

The facility should have a designated security guard force that monitors and secures the facility and aims to identify, challenge, and address unauthorized/unidentified persons and stops introduction of illegal materials.

- Facility has a designated security guard force.
- Security supervisor/guards log incidents.
- Security guards report incidents related to compromised seals and/or containers/trailers to appropriate local authorities.
- Security guards should report any security violation incidents, including tampering involving a loaded or empty container/trailer to management personnel.
- Available communication system between the central security office and the exterior guard posts.

- Guards receive specific security training.
- Facility has proper communication mechanism to local law enforcement authorities.

ACCESS CONTROLS

Access controls must be in place to identify, challenge, and address unauthorized/unidentified persons which includes the positive identification of all employees, visitors, and vendors at all entry points.

- Gates for employees and vehicle entrances/exits must be guarded and/ or monitored during operating hours and during non-operating hours.
- Employees' entries and exits must be logged.
- Employees must be observed and/or subject to security inspection when entering the building.
- Guards should patrol the interior of the facility buildings.
- Closed circuit television cameras (CCTVs) should be used to monitor activity in the facility, including fence/wall and entrance gates.
- CCTV recordings (e.g., tapes or electronic files) should be kept for a minimum of 60 days or according to client's specific requirements, whichever is longer.

VISITOR CONTROLS

Visitor access controls must be in place which includes procedure for positive identification of all visitors and vendors at all entry points and monitoring visitors' activities by escorting them or limiting their access if possible.

- Same security control points applied to employees and visitors when entering and exiting the facility.
- Advance information from a vendor required before the visit.
- Facility maintains up-to-date list of names and addresses of all contractor (e.g., canteen staff), vendor, repair personnel.
- Photo identification required of all visitors.
- A positive identification process for recording all vendors and repair personnel and facility have a written procedure to challenge, identify, and remove unauthorized/unidentified persons.
- Visitors log maintained.
- Visitors (including contractors) required to wear temporary ID badges.

ENTERING/EXITING DELIVERIES

Arriving goods, packages and mail should be periodically screened before being distributed and drivers delivering/receiving cargo must be positively identified before

cargo is received/ released.

- Documented procedures implemented to periodically screen arriving packages and mail prior to distribution.
- Both incoming and outgoing cargo vehicles checked.
- Advance notice required for a pick-up or delivery transport company.
- Conveyance drivers required to show positive identification.
- Conveyance drivers required to show a truck manifest upon entry and/or exit.
- Cargo log in and out maintained.
- Full incoming and outgoing containers and/or trailers sealed.
- Documented procedure for handling cases of broken seals.
- Documented procedure to verify seal and seal number.
- Shipping/receiving parking lots separated from all other parking lots.

EMPLOYEE/VISITOR PARKING

Private passenger vehicles should be prohibited from parking in or adjacent to cargo-handling and storage areas.

- Vehicles prohibited/prevented from parking near cargo conveyances.
- Vehicles prohibited/prevented from parking near the perimeter fencing.
- If allowed to enter the facility area, vendor and visitor vehicles should be inspected prior to admission.
- Visitor and employee personal-vehicle parking lots should be monitored by security guards during facility operating hours.
- Facility requires the use of visual identification for visitor and employee parking.
- Cargo log in and out maintained.

PRODUCTION, ASSEMBLY, PACKAGING SECURITY

Measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain.

- Security measures in place to prevent tampering of goods during production.
- Security measures in place to prevent the introduction of foreign material(s) into the assembly area and packing area.
- Procedures for detecting and reporting shortages and overages.

INFORMATION ACCESS CONTROLS

Documentation control must be implemented, including safeguarding computer access and information and procedures are in place to ensure that all information used in clearing merchandise/cargo is legible, complete, accurate, and protected against the exchange, loss, or introduction of erroneous information.

- Procedures for identifying which employees are allowed access to computer and information.
- Controlled access to the server room.
- Electronic information systems password protected.
- Facility has procedures to adjust or rescind such access.
- Facility has designated system administrator.
- A system in place to identify IT abuses, including improper access, tampering, or the altering of business data.
- All computer information saved on a back-up system.

SHIPMENT INFORMATION CONTROLS

All information used in clearing merchandise/cargo is legible, complete, accurate, and protected against the exchange, loss, or introduction of erroneous information and procedures must be in place to ensure that information provided by the company is reported accurately and timely.

- Facility has designated company representative responsible for shipment information control.
- Records maintained on all shipments for at least twelve months.
- Facility conducts a review of shipment information and documentation controls to verify accuracy and security.

STORAGE AND DISTRIBUTION

STORAGE

Containers are stored in a secure area to prevent unauthorized access and/or manipulation.

- Doors secured for empty stored containers/trailers.
- Facility uses fencing or other barrier materials to enclose cargo-handling and storage areas to prevent unauthorized access.
- Dangerous cargo, including hazardous materials, ammunition and explosives, secured and stored separately.
- High value cargo marked, segregated and stored separately within a fenced area or secured room.

- International and domestic cargo segregated and stored separately within a fenced area or secured room.

LOADING FOR SHIPMENT

Control and security measures must be in place to ensure the integrity and security of processes relevant to the handling, storage, loading and transportation of cargo in the supply chain including verifying the physical integrity of the container structure and reliability of door-locking mechanisms prior to stuffing.

- Loading and departure of containers/ trailers are supervised by a security officer or other designated supervisor.
- Loading and departure of containers/ trailers is captured on CCTV and the recording is kept for 60 days.
- Shipping area and loading dock access restricted to authorized personnel only.
- Security controls in place to prevent the introduction of foreign material(s) or non-manifested items at point of loading, and to prohibit employees bringing in their personal items into the shipping area.
- Cargo moved directly from the storage facility/assembly line to the conveyance without intermediate staging.
- Documented and implemented procedures to ensure that accurate, legible, and complete cargo documents and packing slips prepared.
- Documented system in place to ensure that management, customs and/or local law are informed of and investigates all anomalies found in shipments and/or the accompanying documents.
- Cargo verification procedure in place to prevent non-manifested cargo from being loaded.
- Detect and report cargo shortages and overages during container/trailer loading, and ensure cargo is identified and labeled, weighed, and counted before loading.
- All containers checked for tampering, false compartments, and other evidence of unauthorized access before loading.
- Procedures in place to verify the integrity of the container structure through 7- point inspection.
- All trailers checked for tampering, false compartments, and other evidence of unauthorized access before loading.
- Security personnel perform truck outbound inspection.
- Procedure to affix a high-security seal which meets or exceeds ISO/PAS 17712 on each container/trailers bound for the US.
- ISO/PAS 17712 compliant high security seals used on each outbound container/ trailers.
- Procedures for affixing, replacing, recording, and tracking the seals placed on

containers, trailers, trucks, and/or railcars.

- For pick-ups from multiple manufacturers, the facility requires transportation providers to use secure locking devices (e.g., padlocks) for less than-full-load containers.
- There are designated individuals responsible for issuing, accessing and tracking seals.
- Unused seals kept in a locked cabinet and access restricted to authorized employee(s).
- Outgoing cargo verified against transportation/shipping document before departure and facility keep records of verification.
- Trucks sealed as soon as loading is complete.
- Seal numbers verified at time of final sealing before departure.

BUSINESS PARTNER REQUIREMENTS

Facility must have written and verifiable processes for the selection of business partners such other manufacturers, product suppliers, service suppliers and vendors (parts and raw material suppliers, etc.).

- The facility should have a verifiable process for selecting contractors.
- Written security standards and documented procedures for selection of contractors (contracts, manuals, etc.)
- Contractors with access to restricted areas should undergo a background investigation.
- Facility or third-party auditor conduct on-site inspections of the contractors' implementation of the above standards/ procedures.
- Facility requires its contractors to conduct self-assessment of their security policies and procedures and share the results of those assessments with the facility.
- Contractors retained through legally binding contracts.

EXPORT LOGISTICS

Facility must have written and verifiable processes for the selection of carriers and other Third-Party Logistics (3PL) providers and ensuring that eligible partners are certified and ineligible partners are compliant with the international security standards or its equivalent.

- Facility selects the land carriers, sea carriers, rail carriers, consolidators, freight forwarders, NVOCCs (Non-Vessel Operating Common Carriers), or other third-party logistics providers hired to transport goods.
- Facility requires eligible carriers to demonstrate C-TPAT, AEO, PIP certification and/or ineligible carriers to demonstrate compliance with C-TPAT, AEO, PIP

equivalent standards.

- Security measures in place when facility uses in-country transport services.
- Security measures in place when facility uses carrier services.
- Written or electronic confirmation of partners' compliance with C-TPAT or C-TPAT-equivalent security criteria.
- Facility has written legal contract with a transport company who moves a container/trailer from the facility to the next destination in the supply chain.

TRANSPARENCY IN SUPPLY CHAIN

Efforts made by the company to evaluate and address risks of human trafficking and slavery in the supply chain.

- System in place to ensure that management is informed of and investigates all anomalies found in shipments including human trafficking.
- Cargo verification procedure in place to prevent un-manifested cargo and/or irregular migrants from being loaded.
- Facility requires its contractors to conduct self-assessment of their security policies and procedures including status of their compliance with human trafficking and slavery policies and share the results of those assessments with the facility.

RISK ASSESSMENT

Facility should have a documented process for determining and addressing security risks throughout their international and domestic supply chains.

- Facility has a risk assessment program to analyze and identify critical areas of its supply chain that is the most likely targets for infiltration.
- Facility's Risk Assessment program includes identification of "High Risk" supply chains based on the security threats at the point of origin such as: Terrorism; Contraband Smuggling; Organized Crime; Conditions fostering the above threats.
- Facility has written processes for the selection of their business partners to include a detailed risk assessment.
- Facility adopts the "5 Step Risk Assessment Process Guide" in conducting a security risk assessment of their supply chain(s).

Rating Policy And Remediation

Rating	Category	Description	Approval and Remediation
F	Zero Tolerance	<p>ZT issues are those that can occur as part of a Supplier's business operations if internal control systems to prevent them are not well understood, established and maintained. The issues are egregious and unacceptable to Global Cyberworks and its customers.</p> <p>Furthermore, these issues present immediate threats to the Supplier's business operations and employees and therefore require immediate attention and remediation. Failure to immediately correct these issues will result in the termination of the business relationship with Global Cyberworks.</p> <p>Factories with multiple or particularly egregious ZTs (by their scale or nature) may result in suppliers being permanently prohibited from producing merchandise for Global Cyberworks. Global Cyberworks reserves the right to decline receipt of goods produced in factories with one or more ZT issues.</p>	No approval and completion of remediation requirements.
D	Immediate Remediation Required	<p>Immediate Remediation Required issues are unlawful and/or happen in workplaces when occupational safety and workforce well-being are disregarded. The elimination or resolution of severe issues, and reinforcement of internal systems to prevent these issues from recurring is required for a Supplier to maintain its business relationship with Global Cyberworks. It is important for Suppliers to identify and eliminate these issues to be better equipped to manage workplace risks and attract and retain productive workers. Failure to act to correct these issues will result in the termination of the business relationship with Global Cyberworks.</p>	<p>No approval for new factories.</p> <p>6 months approval for existing factories and completion of remediation requirements</p>
C	Substantial Improvement Required	<p>Substantial Improvement Required issues are either unlawful or happen in workplaces when occupational safety and workforce well-being are disregarded. These issues pose threats to the Supplier's business operations. Furthermore, in today's competitive labor market, Suppliers who identify and eliminate these issues are better equipped to manage workplace risks and attract and retain productive workers. A Supplier found to have these issues present at its facilities is required to identify and implement corrective actions, including the reinforcement of internal systems to prevent these issues from recurring. Repeated failure to act and correct these issues will result in the termination of the business relationship with Global Cyberworks.</p>	12 months approval and commitment to correct non-compliances according to a corrective action plan (CAP)
B	Improvement Required	<p>Improvement Required issues are those that are considered important to address to help ensure Suppliers can sustain their operations effectively with a productive workforce and manage the risk. A Supplier found to have these issues present at its facilities is required to identify and implement corrective actions, including the reinforcement of internal systems to prevent these issues from recurring.</p>	24 months approval and commitment to correct non-compliances according to a corrective action plan (CAP)
A	Approaching Compliance	<p>Factories with "Approaching Compliance" status have achieved an audit result without any noted violations.</p>	24 months

Remediation Requirements (D and F-rated Factories)

D – Rating

1. New factories must achieve a compliance rating of C or higher. When an existing factory receives a compliance rating of D, it is approved for 6 months. In addition:
 - The factory is required to submit an acceptable corrective action plan (CAP) within 30 calendar days of the audit.
 - Failure to submit an acceptable corrective action plan (CAP) within 30 calendar days of the audit may result in the approval period being shortened and factory deactivation, which means no new orders will be placed.
2. The factory must comply with the corrective action plan (CAP) and correct identified D-rated compliance issues within 6 months of the audit.
 - Global Cyberworks will monitor and verify the factories' remediation progress periodically. For issues requiring onsite verification, LF or 3rd party representatives may be deployed with prior notification and any relevant costs will be applied to the factory.
 - Failure to rectify non-compliances within 6 months may result in deactivation.
3. Upon completion of non-compliances, the factory will be upgraded to a compliance rating of C or above and be given approval for 12 to 24 months, depending on the final compliance rating.
4. To be reactivated and eligible for new orders, the factory must pass an onsite main audit and achieve a compliance rating of C or above. Equivalency is not accepted as a way to reactivate a D or F-rated factory.

F – Rating (Zero Tolerance)

1. After a factory receives a compliance rating of F, it will be deactivated in the Global Cyberworks system. In some cases, this may result in permanent termination of the factory.
2. A factory with orders in production must submit a corrective action plan (CAP) within 7 calendar days of the audit and make significant progress towards the remediation of non-compliances within 30 calendar days to be eligible to ship goods.
 - Remediating non-compliances does not reactivate the factory. The factory will remain deactivated in the Global Cyberworks system.
 - Customer may impose additional requirements.
3. To be reactivated and be eligible for new orders, the factory must remediate the issue, pass an unannounced main audit and achieve a compliance rating of C or above. Equivalency is not accepted to reactivate a D or F-rated factory.

Table of Zero-Tolerance

Safe Workplaces



- High risk of immediate structural collapse
- Gross or repeated negligence leading to loss of life or serious accident
- Locked or systematically obstructed emergency exits

Respect



- Underage labor (15 or legal age in country, whichever is higher)
- Worst Forms of Workplace Violence (sexual harassment, physical and severe psychological abuse)
 - All Forms of Forced Labor
- Payment of illegal and excessive recruitment fees and related costs
 - Non-payment of wages for more than 2 pay periods
- Attempted or committed bribery
- Critical issues related to audit falsification
- Full access denied or denial of serious accident investigation
- Unauthorized subcontracting
- Unauthorized home working
- Lack of business license

Transparency and Ethics



Factory Activation

1. To activate a new or inactive factory in Global Cyberworks system, a compliance rating of C or above must be achieved through a main audit or equivalency.
2. This policy applies to new factories and factories that have been inactive in the Global Cyberworks system for 24 months or longer.
3. Additional conditions may be applied to activate a Bangladesh factory in Global Cyberworks system.

APPROACH TO REMEDIATION

Suppliers are responsible for remediating violations in line with the UN Guiding Principles on Business and Human Rights (including addressing serious human rights and environmental harms). Suppliers should consult with workers, through trade unions or other elected representatives when developing their Corrective Action Plans (CAP).

If the standards are not followed, Suppliers are encouraged to:

1. Take immediate actions necessary to correct non-compliances, including investigating the root cause of the non-compliance and providing victim support and compensation (where relevant).

2. Contact Global Cyberworks to proactively report serious violations or incidents. Where deemed necessary and appropriate, Global Cyberworks will engage with external partners to support and advise the factory in providing appropriate access to remedy to impacted individuals or communities or to provide specialized training to factory management and/or its workers.
3. Take preventative actions by establishing appropriate policies and procedures (setting the standards), training relevant personnel, followed by due diligence in systematically reviewing actual practices to ensure the policies/procedures are followed.

For additional questions and assistance

It is important to Global Cyberworks that all Suppliers understand the Supplier Code, remediation processes and can successfully implement corrective and preventative actions. If any of the explanations/descriptions contained in this guidance are unclear, please contact your local Global Cyberworks Compliance officer.

GLOBAL CYBERWORKS