WECH-RB

Code of Conduct

We Create Harmony with Responsible Businesses

Document Number	WECH-RB-COC-001
Version	1.1
Status	Effective
Issue Date	August 16, 2026
Effective Date	August 16, 2026
Document Owner	WECH-RB Certification Program

This Code of Conduct defines WECH-RB expectations for responsible business practices across labor, EHS, environment, business ethics, anti-corruption, responsible procurement, supplier due diligence, AI governance, AI security, responsible AI use, and continuous improvement.

WECH-RB Certification Program

Document Control

This controlled document supports the WECH-RB certification process and provides the conduct expectations used for application review, questionnaire evaluation, document review, gap assessment, scoring, certificate decision, and continuous improvement guidance.

Field	Information
Document Title	WECH-RB Code of Conduct
Document Number	WECH-RB-COC-001
Version	1.1
Status	Effective
Issue Date	August 16, 2026
Effective Date	August 16, 2026
Review Cycle	At least annually or when significant program, legal, regulatory, customer, or business changes occu
Document Owner	WECH-RB Certification Program

Revision History

Version	Date	Description	Approved By
1.0	August 11, 2026	Initial formal release	WECH-RB Certification Program
1.1	August 16, 2026	Integrated Chapter 6 - AI Governance, Security, and Responsible Use	WECH-RB Certification Program

Table of Contents

1. Introduction

WECH-RB stands for We Create Harmony with Responsible Businesses. WECH-RB believes that responsible companies committed to fair labor practices, safe workplaces, environmental protection, ethical operations, anti-corruption controls, responsible procurement, responsible business partner due diligence, AI governance, security, responsible AI use, and continuous improvement can help create a safer, more sustainable, more ethical, and more harmonious society.

This WECH-RB Code of Conduct establishes the expectations used in the WECH-RB document-reviewed certification process. It is designed for companies, suppliers, manufacturers, distributors, service providers, contractors, and other business partners seeking to demonstrate responsible business practices through document submission, questionnaire responses, AI-assisted preliminary review, and administrative document review.

The Code of Conduct is structured as a practical business standard. It identifies the commitments, controls, records, and improvement practices that an applicant should maintain to support responsible business performance.

2. Scope and Applicability

This Code of Conduct applies to companies participating in the WECH-RB certification process and, where applicable, their employees, temporary workers, contract workers, agency workers, suppliers, subcontractors, agents, brokers, consultants, AI system users, AI tool administrators, AI vendors, and other third parties acting on their behalf.

Participating companies are expected to:

- Comply with applicable laws and regulations in the countries and regions where they operate.
- Maintain policies, procedures, records, and internal controls appropriate to their business size, industry, risk level, and operating locations.
- Communicate relevant Code of Conduct expectations to employees, suppliers, contractors, and other business partners.
- Provide accurate and complete information during the WECH-RB application, questionnaire, document upload, and review process.
- Identify, manage, and correct risks or gaps related to labor, EHS, environment, ethics, anti-corruption, procurement, business partner due diligence, AI governance and security, and continuous improvement.

Where this Code of Conduct and local law address the same topic, companies should follow the stricter requirement where legally permissible.

Chapter 1 - Labor and Human Rights

1.1 Freely Chosen Employment and Forced Labor Prevention

Companies shall not use, support, or benefit from forced labor, bonded labor, indentured labor, prison labor, human trafficking, slavery, or any form of involuntary labor.

Companies are expected to:

- Employment is voluntary and workers are free to leave employment in accordance with applicable law and employment agreements.
- Workers are not required to pay recruitment fees or similar fees as a condition of employment.
- Workers are not required to surrender passports, identity documents, work permits, immigration documents, or other personal documents unless legally required and voluntarily agreed.
- Any document retention required by law is controlled, documented, and allows workers reasonable access to their documents.
- Labor agents, recruiters, and subcontractors are monitored to prevent forced labor risks.
- Migrant, temporary, contract, and agency workers receive clear employment terms in a language they understand.

Suggested evidence: *forced labor policy, recruitment policy, employment contracts, labor agent agreements, fee repayment procedure, worker handbook, migrant worker controls, and grievance records.*

1.2 Child Labor Prevention and Young Worker Protection

Companies shall not employ child labor. The minimum employment age shall comply with applicable law and shall not be lower than the age for completion of compulsory education where applicable.

Companies are expected to:

- Verify worker age before employment and maintain reliable age verification records.
- Establish a remediation process if child labor is identified.
- Ensure young workers are not assigned hazardous work, night work, overtime beyond legal limits, or work that may affect their health, safety, education, or development.
- Manage internship, apprenticeship, student worker, and vocational training programs in compliance with applicable laws.

Suggested evidence: *age verification procedure, hiring records, young worker list, student worker policy, remediation procedure, and job restriction matrix.*

1.3 Working Hours

Companies shall manage working hours in accordance with applicable laws, customer requirements, and internal policies.

Companies are expected to:

- Track regular working hours, overtime hours, rest days, and legally required breaks.
- Ensure overtime is voluntary where required by law.
- Avoid excessive working hours and manage fatigue risks.
- Provide at least the minimum rest periods required by law.
- Maintain accurate timekeeping records.
- Review working hour trends and take corrective actions when limits are exceeded.

Suggested evidence: *attendance records, overtime approval records, working hour policy, payroll records, shift schedules, and corrective action records.*

1.4 Wages and Benefits

Companies shall pay workers at least the legally required minimum wages and provide legally required benefits.

Companies are expected to:

- Pay wages on time and in full.
- Provide legally required overtime compensation.
- Provide wage statements or equivalent records showing wage calculation.
- Avoid illegal or unauthorized wage deductions.
- Provide legally required benefits, social insurance, leave, and other statutory entitlements.
- Ensure workers understand wage terms, benefit eligibility, and deduction rules.

Suggested evidence: *payroll records, wage statements, benefit records, overtime payment records, employment contracts, and wage deduction procedures.*

1.5 Non-Discrimination, Non-Harassment, and Fair Treatment

Companies shall provide a workplace free from discrimination, harassment, abuse, intimidation, and inhumane treatment. Employment decisions should be based on qualifications, performance, experience, job requirements, and business needs.

Companies are expected to:

- Prohibit discrimination based on race, color, age, gender, sexual orientation, gender identity, ethnicity, national origin, disability, pregnancy, religion, political affiliation, union membership, veteran status, marital status, or other legally protected status.
- Maintain procedures to prevent and respond to harassment, bullying, threats, physical punishment, verbal abuse, sexual harassment, and retaliation.
- Investigate credible concerns and take corrective action where appropriate.
- Communicate fair treatment expectations to workers, supervisors, and relevant business partners.

Suggested evidence: *anti-discrimination policy, anti-harassment policy, employee handbook, investigation records, training records, and grievance records.*

1.6 Freedom of Association and Worker Communication

Where legally applicable, companies shall respect workers' rights to freely associate, join or not join labor organizations, seek representation, and communicate with management regarding working conditions.

Companies are expected to:

- Provide lawful channels for worker communication.
- Avoid retaliation against workers who raise concerns.
- Maintain open communication between workers and management.
- Provide grievance channels that are accessible, confidential where appropriate, and free from retaliation.

Suggested evidence: *grievance procedure, worker communication records, employee committee records, suggestion system records, and non-retaliation policy.*

1.7 Grievance Mechanism and Non-Retaliation

Companies shall provide workers and relevant stakeholders with a mechanism to raise concerns, report misconduct, and seek resolution.

Companies are expected to:

- The mechanism is accessible to workers and relevant stakeholders.
- It allows confidential or anonymous reporting where legally allowed.
- It includes a defined review and response process.
- It protects reporters from retaliation.
- It tracks complaints, investigations, actions, and closure.

- It is communicated in languages workers understand.

Suggested evidence: *grievance procedure, hotline information, case log, investigation reports, corrective action records, and worker communication records.*

Chapter 2 - EHS and Environment

2.1 Occupational Health and Safety Management

Companies shall provide a safe and healthy workplace and manage occupational health and safety risks.

Companies are expected to:

- Identify workplace hazards and assess risks associated with tasks, equipment, materials, processes, and workplace conditions.
- Implement controls using the hierarchy of controls where practical.
- Provide safe work procedures and personal protective equipment where required.
- Train workers on workplace hazards and safe work practices.
- Track incidents, near misses, injuries, occupational illnesses, and corrective actions.
- Review safety performance and continuously improve controls.

Suggested evidence: *safety policy, risk assessment, job safety analysis, safety procedures, training records, inspection records, incident reports, and corrective action records.*

2.2 Emergency Preparedness and Response

Companies shall identify potential emergency situations and establish emergency preparedness and response procedures.

Companies are expected to:

- Address applicable emergencies such as fire, severe weather, medical emergencies, chemical spills, power failure, natural disasters, workplace violence, evacuation, and business continuity concerns.
- Maintain emergency action plans, evacuation maps, emergency contact lists, and emergency equipment inspection records.
- Inspect fire protection equipment, emergency lighting, exits, and evacuation routes.
- Conduct drills and correct findings identified during drills or actual emergency events.

Suggested evidence: *emergency response plan, evacuation drill records, fire extinguisher inspection records, emergency equipment inspection records, and training records.*

2.3 Chemical and Hazardous Materials Management

Companies shall manage chemicals and hazardous materials to prevent harm to workers, the public, property, and the environment.

Companies are expected to:

- Maintain an inventory of chemicals and hazardous materials.
- Maintain current safety data sheets where applicable.
- Label chemical containers properly and store incompatible materials separately.
- Provide spill response materials and train employees on chemical hazards and emergency response.
- Manage hazardous waste according to applicable requirements.
- Control exposure to hazardous substances.

Suggested evidence: *chemical inventory, SDS records, labeling procedure, storage inspection records, spill response plan, hazardous waste records, and chemical safety training records.*

2.4 Machine Safety, Equipment Safety, and Energy Control

Companies shall manage machine and equipment hazards to prevent injury.

Companies are expected to:

- Identify equipment hazards such as moving parts, electrical hazards, stored energy, hot surfaces, pinch points, sharp edges, pressure systems, and automation hazards.
- Provide machine guards, interlocks, emergency stops, barriers, warnings, and safe operating procedures where appropriate.
- Maintain preventive maintenance records.
- Establish lockout/tagout or equivalent energy control procedures where hazardous energy exists.
- Ensure only trained and authorized workers operate, maintain, or service equipment.

Suggested evidence: *equipment risk assessments, machine guarding inspection records, lockout/tagout procedures, maintenance records, and operator training records.*

2.5 Industrial Hygiene and Worker Health Protection

Companies shall identify and manage potential worker exposure to health hazards.

Companies are expected to:

- Evaluate potential exposure to noise, dust, fumes, vapors, solvents, heat stress, cold stress, radiation, biological hazards, ergonomic hazards, repetitive motion, and manual material handling risks.
- Implement controls such as engineering controls, ventilation, administrative controls, PPE, medical surveillance, and worker training where appropriate.
- Review exposure monitoring results and take corrective actions when needed.
- Maintain health-related records consistent with privacy and legal requirements.

Suggested evidence: *exposure assessments, ventilation inspection records, noise monitoring, ergonomic assessments, heat stress program, PPE records, and occupational health records where legally allowed.*

2.6 Sanitation, Food, Housing, and Transportation

Where companies provide or control sanitation facilities, cafeterias, dormitories, transportation, or related services, they shall maintain safe, sanitary, and humane conditions.

Companies are expected to:

- Provide clean drinking water and adequate toilets and washing facilities.
- Maintain safe food preparation and dining areas where applicable.
- Maintain dormitories in a safe and sanitary condition where applicable.
- Provide emergency exits, fire protection, ventilation, lighting, and reasonable living space in company-provided housing where applicable.
- Manage worker transportation safety where applicable.

Suggested evidence: *sanitation inspections, dormitory rules, cafeteria inspections, pest control records, housing safety inspections, and corrective action records.*

2.7 Environmental Permits and Compliance Controls

Companies shall identify, obtain, maintain, and comply with applicable environmental permits, registrations, approvals, and reporting requirements.

Companies are expected to:

- Maintain a list of applicable environmental permits and obligations.
- Monitor expiration dates and renewal requirements.
- Submit required reports on time.
- Maintain records demonstrating compliance with permit conditions.
- Notify relevant authorities where required by law.

- Correct nonconformities and prevent recurrence.

Suggested evidence: *environmental permit list, permit copies, inspection records, monitoring reports, renewal tracking, agency correspondence, and corrective action records.*

2.8 Pollution Prevention and Resource Management

Companies shall seek to prevent pollution and reduce waste, emissions, discharges, and resource consumption where practical.

Companies are expected to:

- Manage air emissions, wastewater, stormwater, solid waste, hazardous waste, energy use, water use, materials use, packaging, and greenhouse gas emissions where applicable.
- Evaluate opportunities for reduction, reuse, recycling, substitution, process improvement, and efficiency.
- Set improvement objectives where appropriate and track progress.
- Review environmental performance trends and corrective actions.

Suggested evidence: *waste records, recycling records, utility data, emissions records, wastewater records, environmental objectives, and reduction projects.*

2.9 Waste Management

Companies shall manage waste in accordance with applicable laws and responsible environmental practices.

Companies are expected to:

- Identify and classify waste streams appropriately.
- Store waste safely and label waste containers.
- Prevent leaks, spills, and releases.
- Use authorized waste vendors where required.
- Maintain disposal, recycling, or treatment records.
- Track hazardous waste generation and disposal where applicable.

Suggested evidence: *waste inventory, waste manifests, vendor permits, inspection records, waste storage area procedures, and disposal records.*

2.10 Energy and Greenhouse Gas Management

Companies should identify major energy uses and, where applicable, track greenhouse gas emissions.

Companies are expected to:

- Track electricity, natural gas, fuel, or other relevant energy sources.
- Identify energy efficiency opportunities.
- Maintain records supporting energy and emissions data.
- Set improvement objectives where appropriate.
- Communicate environmental improvement actions internally.

Suggested evidence: *utility bills, GHG inventory, energy review records, reduction targets, project records, and management review records.*

Chapter 3 - Business Ethics and Anti-Corruption

3.1 Anti-Bribery and Anti-Corruption

Companies shall prohibit bribery, corruption, extortion, embezzlement, kickbacks, improper payments, and other unethical business practices.

Companies are expected to:

- Prohibit improper payments or anything of value offered, promised, authorized, requested, accepted, or provided to improperly influence a business decision or obtain an improper advantage.
- Apply anti-corruption expectations to interactions with government officials, state-owned enterprise employees, customers, suppliers, contractors, agents, brokers, consultants, and other third parties.
- Maintain policies, procedures, training, approval controls, and reporting channels to prevent and detect bribery and corruption risks.
- Investigate credible concerns and take corrective action where appropriate.

Suggested evidence: *anti-bribery policy, anti-corruption procedure, training records, approval matrix, investigation records, and disciplinary records.*

3.2 Government Officials and FCPA-Style Controls

Companies shall establish controls for interactions with government officials and state-owned enterprises.

Companies are expected to:

- Prohibit improper payments to government officials.
- Review high-risk transactions involving government officials.
- Control gifts, entertainment, travel, hospitality, donations, sponsorships, and facilitation payments.
- Maintain accurate records for government-related transactions.
- Conduct appropriate due diligence on third parties interacting with government officials on the company's behalf.
- Escalate potential red flags for review.

Suggested evidence: *government interaction procedure, gift approval records, third-party due diligence records, training records, and books and records controls.*

3.3 Gifts, Entertainment, Meals, Travel, and Hospitality

Companies shall ensure that gifts, entertainment, meals, travel, and hospitality are reasonable, transparent, lawful, properly approved, and not used to improperly influence business decisions.

Companies are expected to:

- Define allowed and prohibited gifts and entertainment.
- Set approval thresholds and apply stricter controls for government officials.
- Prohibit cash or cash equivalents unless specifically allowed by policy and law.
- Require documentation of business purpose.
- Maintain gift and hospitality registers where appropriate.
- Prohibit gifts or hospitality that create conflicts of interest or the appearance of improper influence.

Suggested evidence: *gifts and entertainment policy, approval records, gift register, training records, and expense records.*

3.4 Facilitation Payments

Companies should prohibit facilitation payments unless there is a documented emergency involving immediate risk to health, safety, or personal security.

Companies are expected to:

- Define facilitation payments and train employees and third parties on prohibited payments.
- Require reporting of any requested or made facilitation payment.
- Review incidents and take corrective actions.
- Accurately record any payment in company books and records.

Suggested evidence: *anti-corruption policy, reporting records, investigation records, and accounting records.*

3.5 Political Contributions, Charitable Donations, and Sponsorships

Companies shall ensure that political contributions, charitable donations, and sponsorships are lawful, transparent, approved, and not used as improper payments.

Companies are expected to:

- Establish approval controls and verify the recipient organization.
- Document the legitimate purpose.
- Review potential conflicts of interest.
- Apply enhanced review where government officials, customers, or business decision-makers are involved.
- Maintain accurate records.

Suggested evidence: *donation policy, approval records, recipient due diligence, payment records, and conflict review records.*

3.6 Conflicts of Interest

Companies shall identify, disclose, and manage actual, potential, or perceived conflicts of interest.

Companies are expected to:

- Address personal relationships with suppliers, customers, or government officials.
- Address ownership interest in business partners, outside employment, family relationships, gifts, benefits, undisclosed commissions, and referral fees.
- Maintain a conflict disclosure process.
- Ensure conflicts are reviewed and managed appropriately.

Suggested evidence: *conflict of interest policy, disclosure forms, review records, and mitigation actions.*

3.7 Accurate Books, Records, and Internal Controls

Companies shall maintain accurate books, records, accounts, and supporting documentation.

Companies are expected to:

- Record transactions accurately and completely.
- Prohibit false, misleading, incomplete, or off-book records.
- Maintain proper approval and payment controls.
- Segregate duties where appropriate.
- Retain records according to legal and business requirements.
- Ensure financial records reflect the true nature and purpose of transactions.
- Review high-risk payments and third-party expenses.

Suggested evidence: *accounting policy, approval matrix, payment records, audit records, internal control procedures, and record retention policy.*

3.8 Fraud Prevention

Companies shall prohibit fraud, misrepresentation, theft, embezzlement, falsification of records, and misuse of company assets.

Companies are expected to:

- Establish reporting channels for suspected fraud.
- Investigate credible allegations.
- Protect reporters from retaliation.
- Take corrective and disciplinary action where appropriate.
- Maintain internal controls to prevent and detect fraud.

Suggested evidence: *fraud policy, investigation records, internal audit records, disciplinary records, and corrective action records.*

3.9 Fair Competition and Fair Dealing

Companies shall compete fairly and comply with applicable antitrust and competition laws.

Companies are expected to:

- Prohibit price fixing, bid rigging, market allocation, collusion with competitors, and improper exchange of competitively sensitive information.
- Prohibit misleading statements about competitors and improper restrictions on customers or suppliers.
- Provide training for employees involved in sales, purchasing, pricing, tendering, and competitor interactions.
- Review high-risk agreements and communications.

Suggested evidence: *competition law policy, sales training records, contract review procedures, and investigation records.*

3.10 Data Privacy, Confidentiality, and Information Security

Companies shall protect personal information, confidential information, and business-sensitive data.

Companies are expected to:

- Collect, use, store, transfer, and dispose of personal data lawfully and responsibly.
- Limit access to sensitive data.
- Protect customer, employee, supplier, and business partner information.
- Maintain reasonable cybersecurity controls.
- Report data breaches where required.
- Train employees on confidentiality and privacy obligations.

Suggested evidence: *privacy policy, data protection procedure, access control records, cybersecurity policy, breach response plan, and training records.*

3.11 Whistleblower Reporting and Non-Retaliation

Companies shall provide channels to report ethics, compliance, corruption, labor, EHS, environmental, or supplier-related concerns.

Companies are expected to:

- Allow confidential or anonymous reporting where legally allowed.
- Investigate credible reports.
- Protect reporters from retaliation.
- Track investigation results and corrective actions.
- Communicate reporting channels to workers and relevant third parties.

Suggested evidence: *whistleblower policy, hotline records, investigation procedure, case log, and non-retaliation policy.*

Chapter 4 - Responsible Procurement and Supplier Due Diligence

4.1 Responsible Procurement Commitment

Companies shall integrate responsible business expectations into procurement and supplier management processes.

Companies are expected to:

- Communicate supplier responsibility expectations.
- Require suppliers to comply with applicable laws and relevant Code of Conduct requirements.
- Evaluate supplier risks before and during business relationships.
- Monitor supplier performance based on risk.
- Require corrective actions when gaps or red flags are identified.
- Maintain records of supplier evaluation and monitoring.

Suggested evidence: *supplier code of conduct, supplier onboarding procedure, supplier contracts, procurement policy, supplier evaluation records, and corrective action records.*

4.2 Supplier Onboarding Questionnaire

Companies should use a supplier onboarding questionnaire to collect information needed for risk assessment.

Companies are expected to:

- Collect legal company name, business registration information, address, and operating locations.
- Collect ownership information and beneficial ownership declaration where appropriate.
- Identify industry, business activities, government customer interaction, and use of agents, brokers, consultants, or subcontractors.
- Collect labor, human rights, EHS, environmental, anti-bribery, and ethics control information.
- Request disclosure of sanctions, watchlist, legal history, certifications, audits, and customer assessment history where applicable.

Suggested evidence: *supplier onboarding form, completed questionnaires, risk review records, and approval records.*

4.3 Business Registration and Beneficial Ownership Review

Companies should verify supplier identity and understand ownership structure, especially for higher-risk suppliers.

Companies are expected to:

- Collect business registration documents and identify legal name and registration number.
- Identify owners, parent companies, subsidiaries, and beneficial owners where appropriate.
- Review ownership changes where relevant.
- Escalate unclear, hidden, or inconsistent ownership information.
- Identify potential government official ownership or politically exposed person connections.

Suggested evidence: *business registration documents, ownership declarations, corporate structure charts, beneficial ownership forms, and review records.*

4.4 Sanctions, Watchlist, PEP, and Adverse Media Screening

Companies should conduct risk-based screening of suppliers and relevant third parties.

Companies are expected to:

- Screen for sanctions lists, denied party lists, watchlists, politically exposed persons, adverse media, corruption allegations, forced labor allegations, environmental violations, safety violations, fraud, and financial crime allegations where applicable.

- Document screening results and escalate potential matches for review before onboarding or continuing a high-risk relationship.
- Resolve false positives through documented review.
- Repeat screening periodically or when risk factors change.

Suggested evidence: *screening records, adverse media review records, escalation records, false positive resolution records, and approval records.*

4.5 Human Rights and Forced Labor Due Diligence

Companies should evaluate supplier risks related to human rights, forced labor, child labor, recruitment fees, migrant labor, modern slavery, and unsafe working conditions.

Companies are expected to:

- Identify high-risk countries, industries, labor arrangements, and suppliers.
- Review supplier labor policies and controls.
- Request evidence where appropriate.
- Escalate red flags.
- Require corrective actions where gaps are identified.
- Avoid knowingly benefiting from forced labor or human trafficking.

Suggested evidence: *human rights policy, forced labor risk assessment, supplier questionnaire, audit reports, corrective actions, and training records.*

4.6 EHS and Environmental Due Diligence

Companies should evaluate supplier risks related to health and safety, environmental compliance, hazardous materials, waste, emissions, and emergency preparedness.

Companies are expected to:

- Identify high-risk supplier activities.
- Review relevant EHS and environmental documents.
- Request permits or records where applicable.
- Review safety and environmental incidents where available.
- Require corrective actions for significant gaps.
- Consider enhanced review for suppliers with hazardous operations or significant environmental impact.

Suggested evidence: *supplier EHS questionnaire, environmental permit records, safety policy, chemical management records, waste records, customer audit results, and corrective action records.*

4.7 Anti-Bribery and Corruption Due Diligence

Companies should conduct risk-based anti-bribery and corruption due diligence on suppliers and third parties.

Companies are expected to:

- Apply enhanced attention to sales agents, brokers, customs brokers, consultants, lobbyists, distributors, resellers, government-facing service providers, and third parties interacting with government officials on the company's behalf.
- Review the third party's business purpose, qualifications, compensation structure, ownership, and potential government connections.
- Screen for adverse media and corruption concerns.
- Include anti-corruption contract clauses where appropriate.
- Monitor payments and performance.
- Require training or certification where appropriate.

Suggested evidence: *due diligence forms, anti-corruption certification, contract clauses, payment review records, screening records, and approval records.*

4.8 Country, Industry, and Transaction Risk

Companies should consider country risk, industry risk, transaction risk, and business model risk when evaluating third parties.

Companies are expected to:

- Consider operations in high-corruption-risk jurisdictions, high-risk industries, government customers, public tenders, customs or import/export activities, high-value contracts, cash-intensive transactions, use of intermediaries, urgent or unusual payment requests, incomplete documentation, and lack of transparency.
- Define risk criteria and apply approval controls based on risk level.
- Maintain a documented rationale for enhanced review or approval decisions.

Suggested evidence: *risk assessment criteria, supplier risk rating records, approval records, and enhanced due diligence records.*

4.9 Supplier Risk Ratings

Companies should classify suppliers and third parties based on risk.

Companies are expected to:

- Low Risk: Limited risk indicators, complete documentation, low-risk country or industry, and no significant red flags.
- Medium Risk: Some risk factors exist, but documentation and controls are generally acceptable.
- High Risk: Multiple risk factors, missing documents, high-risk country or industry, government interaction, or unresolved concerns.
- Critical Risk: Sanctions match, credible corruption concern, forced labor concern, serious EHS or environmental allegation, refusal to disclose ownership, fake documents, or other severe red flags.
- Define review frequency, approval level, and monitoring requirements based on risk rating.

Suggested evidence: *supplier risk matrix, risk rating records, escalation records, enhanced review records, and approval records.*

4.10 Red Flags

Companies shall identify and escalate red flags before onboarding or continuing a business relationship.

Companies are expected to:

- Refusal to disclose ownership or provide basic company information.
- Unusual payment terms, cash payment requests, payment to unrelated third parties, or payment to offshore or unrelated accounts.
- Government official ownership, close relationship, sanctions or watchlist match, PEP connection, repeated adverse media, or allegations involving corruption, fraud, forced labor, environmental violations, or safety violations.
- No anti-bribery policy, no grievance mechanism, no supplier code of conduct, fake or inconsistent documents, or high-risk country with weak controls.
- Use of undisclosed subcontractors, agents, brokers, or consultants.
- Refusal to certify compliance with responsible business requirements.

Suggested evidence: *red flag logs, escalation records, enhanced due diligence files, mitigation records, rejection records, and corrective action records.*

4.11 Ongoing Monitoring and Periodic Reassessment

Supplier due diligence should not be limited to onboarding.

Companies are expected to:

- Reassess suppliers periodically based on risk.

- Monitor changes in ownership, scope, geography, or business activities.
- Review new adverse media or red flags.
- Update supplier questionnaires where appropriate.
- Track corrective actions.
- Suspend or terminate relationships where significant unresolved risks remain.

Suggested evidence: *monitoring records, periodic reassessment records, updated questionnaires, corrective action logs, and supplier review meeting records.*

Chapter 5 - Management System and Continuous Improvement

5.1 Management Commitment and Accountability

Companies shall establish management responsibility for implementing this Code of Conduct.

Companies are expected to:

- Assign responsible personnel or functions and define roles and responsibilities.
- Provide management oversight and review performance and risks periodically.
- Allocate resources appropriate to company size and risk.
- Support corrective actions and continuous improvement.

Suggested evidence: *organization charts, role descriptions, management review records, meeting minutes, and action plans.*

5.2 Policies and Procedures

Companies shall maintain written policies and procedures appropriate to their size, industry, risk profile, and operating locations.

Companies are expected to:

- Address relevant topics in this Code of Conduct, including labor, EHS, environment, ethics, anti-corruption, procurement, and due diligence.
- Keep documents current and maintain version control where appropriate.
- Communicate requirements to affected employees.
- Review documents periodically.
- Ensure procedures align with actual practices.

Suggested evidence: *policy documents, procedure documents, revision history, communication records, and training records.*

5.3 Training and Communication

Companies shall communicate Code of Conduct expectations and provide training appropriate to worker roles and risk exposure.

Companies are expected to:

- Provide training on labor rights, workplace safety, emergency response, chemical safety, environmental responsibilities, anti-bribery and anti-corruption, conflicts of interest, data privacy, whistleblower reporting, and supplier due diligence where applicable.
- Maintain training records showing participant names, dates, topics, and materials where appropriate.
- Refresh training based on risk, role, incidents, findings, or program changes.
- Communicate expectations to suppliers and business partners where applicable.

Suggested evidence: *training materials, attendance records, communication records, supplier communication records, and refresher training plans.*

5.4 Risk Assessment

Companies shall identify and assess risks related to labor, EHS, environment, ethics, anti-corruption, procurement, and suppliers.

Companies are expected to:

- Identify legal and business requirements.
- Assess operational risks and consider country, industry, process, supplier, and third-party risks.

- Prioritize higher-risk areas.
- Define controls and corrective actions.
- Review risks periodically or when significant changes occur.

Suggested evidence: *risk assessment records, compliance obligation registers, supplier risk matrices, and corrective action plans.*

5.5 Document and Record Control

Companies shall maintain records sufficient to demonstrate implementation of this Code of Conduct.

Companies are expected to:

- Records should be accurate, complete, legible, protected from unauthorized alteration, retained for appropriate periods, available for review when required, and consistent with privacy and confidentiality obligations.
- Documents should be controlled, current, and accessible to authorized personnel.
- Obsolete documents should be removed from routine use or clearly identified.
- Record retention expectations should be communicated to relevant personnel.

Suggested evidence: *record retention policy, document control procedure, controlled forms, and sample records.*

5.6 Internal Review and Corrective Action

Companies shall review their own performance and take corrective actions when gaps, incidents, nonconformities, or red flags are identified.

Companies are expected to:

- Corrective action should describe the issue, root cause or contributing factors where appropriate, corrective action owner, due date, completion evidence, and effectiveness review where appropriate.
- Internal reviews should be risk-based and documented.
- Repeat findings should receive additional management attention.
- Corrective action status should be tracked until closure.

Suggested evidence: *internal audit reports, self-assessment records, corrective action logs, investigation records, and management review records.*

5.7 Supplier Monitoring

Companies shall monitor suppliers based on risk level and business importance.

Companies are expected to:

- Supplier monitoring may include questionnaire updates, document review, certification review, performance review, customer audit review, corrective action tracking, enhanced due diligence, suspension, or disqualification where appropriate.
- Supplier monitoring frequency should be based on risk.
- Significant supplier concerns should be escalated to responsible management.
- Supplier corrective actions should be reviewed for closure and effectiveness where appropriate.

Suggested evidence: *supplier scorecards, supplier review records, monitoring plan, and corrective action records.*

5.8 Continuous Improvement

Companies shall pursue continuous improvement in responsible business practices.

Companies are expected to:

- Set improvement objectives where appropriate.
- Track progress and review performance trends.
- Learn from incidents, complaints, audits, assessments, and corrective actions.

- Update policies, procedures, training, and controls as needed.

Suggested evidence: *objectives and targets, improvement plans, KPI dashboards, management review records, and completed corrective actions.*

Chapter 6 - AI Governance, Security, and Responsible Use

Artificial intelligence systems, AI tools, AI agents, chatbots, automated decision tools, and third-party AI services can create significant business value, but they may also introduce risks related to data privacy, cybersecurity, confidentiality, fairness, transparency, legal compliance, human oversight, and responsible business decision-making.

Companies using AI are expected to establish appropriate governance, security, privacy, vendor management, employee training, incident response, and continuous improvement controls based on the nature, scale, sensitivity, and risk level of their AI use cases.

This chapter applies where companies develop, procure, deploy, administer, or use AI systems or AI-enabled tools in business operations, customer interactions, employee-related processes, supplier or business partner management, compliance activities, risk assessment, content generation, decision support, or other business processes.

6.1 AI Governance and Accountability

Companies shall establish governance, ownership, and accountability for the development, procurement, deployment, and use of artificial intelligence systems, AI tools, AI agents, chatbots, automated decision tools, and third-party AI services.

Companies are expected to:

- Assign responsible personnel or functions for AI governance, AI security, privacy, legal compliance, and responsible use.
- Maintain an inventory of AI systems, AI tools, AI agents, chatbots, automated decision tools, and third-party AI services used by the company.
- Define acceptable and prohibited uses of AI, including employee use of public AI tools.
- Classify AI use cases based on risk level, business impact, data sensitivity, and potential impact on employees, customers, suppliers, applicants, investors, or other business partners.
- Require appropriate management approval before deploying AI systems that may affect people, business decisions, compliance obligations, financial decisions, safety, environmental performance, or external commitments.
- Maintain records of AI risk assessments, approvals, changes, incidents, and periodic reviews.

Suggested evidence: *AI governance policy, AI acceptable use policy, AI system inventory, AI risk classification matrix, approval records, responsible owner list, management review records, and AI governance meeting records.*

6.2 Data Privacy and Confidential Information Protection

Companies shall protect personal data, confidential business information, customer data, employee data, supplier data, trade secrets, intellectual property, and regulated information when using AI systems or AI-enabled tools.

Companies are expected to:

- Prohibit employees from entering confidential, regulated, proprietary, customer, supplier, employee, or personal data into unauthorized public AI tools.
- Define what types of information may and may not be processed by approved AI tools.
- Apply data minimization, access control, retention control, and purpose limitation when using AI systems.
- Review third-party AI vendors for data retention, data sharing, model training use, confidentiality, deletion, and subcontractor practices.
- Protect AI-related data using reasonable cybersecurity, privacy, and confidentiality controls.
- Ensure AI use aligns with applicable privacy laws, contractual obligations, customer requirements, and internal data protection requirements.
- Maintain records showing how sensitive data is protected in AI workflows.

Suggested evidence: *AI data use policy, privacy policy, data classification procedure, approved AI tool list, vendor privacy review records, data protection impact assessment, access control records, confidentiality training records, and AI data handling procedure.*

6.3 AI System Security and LLM Application Security

Companies shall implement security controls to prevent misuse, unauthorized access, data leakage, prompt injection, insecure output handling, excessive agency, and other AI-related security risks.

Companies are expected to:

- Evaluate AI systems and LLM applications for risks such as prompt injection, sensitive data exposure, insecure plugin or tool access, excessive permissions, model manipulation, data poisoning, and insecure output handling.
- Apply secure software development, testing, change management, and release controls to AI-enabled applications.
- Restrict AI agent permissions based on least privilege and business need.
- Require human approval before AI agents perform high-impact actions, such as sending external communications, approving payments, changing official records, accessing confidential files, making commitments, or triggering business transactions.
- Monitor AI system activity, access logs, abnormal behavior, unauthorized access attempts, and security events.
- Test AI applications before release and after material changes.
- Establish escalation and response procedures for AI-related security incidents.

Suggested evidence: *AI security policy, LLM application security checklist, prompt injection testing records, access control records, AI agent permission matrix, change management records, penetration test or security review records, monitoring logs, and AI security incident response records.*

6.4 Accuracy, Transparency, and Human Oversight

Companies shall use AI outputs in a manner that supports accuracy, transparency, accountability, and appropriate human review.

Companies are expected to:

- Inform users when they are interacting with AI where appropriate.
- Define when AI-generated outputs require human review before use.
- Require human review for AI outputs used in legal, compliance, financial, employment, safety, environmental, medical, customer-impacting, or other high-impact decisions.
- Prohibit AI from making final decisions without human oversight in high-risk or high-impact use cases.
- Establish procedures for reviewing AI-generated content before external publication or customer communication.
- Identify limitations of AI outputs, including hallucination, outdated information, incomplete context, bias, source reliability concerns, and lack of professional judgment.
- Maintain evidence of human review, approval, correction, or override for high-impact AI-supported decisions.

Suggested evidence: *human oversight procedure, AI output review checklist, AI-generated content review records, approval records, user disclosure language, high-impact AI use case register, quality review records, and corrective action records.*

6.5 Fairness, Bias, and Non-Discrimination

Companies shall assess and manage potential bias, unfair outcomes, or discriminatory impacts arising from AI-supported decisions or AI-enabled processes.

Companies are expected to:

- Identify AI use cases that may affect employment, hiring, promotion, discipline, customer access, pricing, credit, housing, benefits, services, or other individual rights or opportunities.
- Evaluate AI systems for potential bias, unfair treatment, discriminatory outcomes, or disproportionate impact.
- Avoid using AI outputs as the sole basis for decisions affecting individuals where legal, ethical, or business risks are significant.
- Provide a process for affected individuals, employees, customers, applicants, or business partners to raise concerns or request review where appropriate.
- Review AI outputs periodically for fairness, consistency, and unintended impacts.
- Maintain documentation of bias review, mitigation actions, human review, and corrective actions.

Suggested evidence: *AI bias assessment, fairness review records, non-discrimination policy, high-impact AI use case register, human review records, complaint or appeal procedure, mitigation action records, and periodic monitoring records.*

6.6 Third-Party AI Vendor and Tool Management

Companies shall evaluate and monitor third-party AI vendors, AI APIs, AI platforms, AI agents, AI-enabled software, and AI service providers for privacy, security, legal, contractual, and responsible-use risks.

Companies are expected to:

- Maintain a list of approved AI tools, vendors, platforms, APIs, and AI-enabled software.
- Review AI vendor terms for confidentiality, data ownership, data retention, model training use, data sharing, security controls, privacy controls, subcontractors, and incident notification.
- Require vendor risk review before using AI tools with personal data, confidential information, customer data, supplier data, employee data, trade secrets, or regulated information.
- Confirm whether vendor AI systems use customer or company data to train models.
- Define contractual requirements for confidentiality, data protection, security, audit rights, data deletion, service availability, and incident notification where appropriate.
- Periodically review the continued suitability of AI vendors and tools.
- Escalate high-risk AI vendors or tools for management, legal, privacy, or security review.

Suggested evidence: *approved AI vendor list, AI vendor risk assessment, vendor security questionnaire, privacy review records, contract review records, data processing agreements, vendor monitoring records, and AI tool approval records.*

6.7 Employee AI Use and Training

Companies shall provide employees and relevant users with clear rules, communication, and training for safe, ethical, secure, and responsible AI use.

Companies are expected to:

- Provide AI acceptable-use guidance to employees and relevant contractors.
- Train employees on prohibited uses, including uploading confidential data, personal data, customer data, supplier data, trade secrets, regulated information, or proprietary information into unauthorized AI tools.
- Train employees to verify AI outputs before relying on them.
- Require employees to disclose or label AI-generated content where appropriate.
- Provide role-based training for employees who develop, procure, approve, administer, or use AI systems in higher-risk activities.
- Refresh AI training based on risk, incidents, findings, regulatory changes, or program changes.
- Maintain training records showing participant names, dates, topics, and materials where appropriate.

Suggested evidence: *AI acceptable-use policy, training materials, attendance records, employee communication records, role-based AI training records, AI user acknowledgment forms, refresher training plans, and disciplinary or corrective action records where applicable.*

6.8 AI Legal and Regulatory Compliance

Companies shall identify and comply with applicable AI-related legal, regulatory, contractual, customer, privacy, employment, consumer protection, cybersecurity, sector-specific, and responsible-use requirements.

Companies are expected to:

- Identify whether AI systems are used in regulated, high-impact, customer-facing, employee-facing, or externally facing activities.
- Evaluate whether AI systems may be subject to applicable laws, regulations, customer requirements, contractual obligations, or industry expectations.

- Maintain documentation for AI systems, including intended purpose, data inputs, limitations, risk assessment, human oversight, monitoring, and approval status.
- Review customer, buyer, investor, regulator, and business partner requirements related to AI use.
- Update AI governance, security, privacy, and responsible-use controls when laws, standards, customer expectations, or business risks change.
- Escalate high-risk AI use cases to legal, compliance, privacy, security, or responsible management where appropriate.

Suggested evidence: *AI legal compliance register, AI regulatory review records, customer requirement review records, AI system documentation, AI risk assessment records, approval records, legal review records, and periodic compliance review records.*

6.9 AI Incident Management and Continuous Improvement

Companies shall identify, report, investigate, correct, and learn from AI-related incidents, concerns, misuse, errors, and control gaps.

Companies are expected to:

- Define what qualifies as an AI-related incident, including data leakage, unauthorized AI use, harmful output, false or misleading output, biased decision support, unauthorized AI agent action, security breach, privacy incident, regulatory concern, or AI-generated misinformation.
- Establish reporting channels for AI incidents, concerns, misuse, and control weaknesses.
- Investigate credible AI-related incidents and document root cause, impact, corrective action, preventive action, and closure.
- Track AI incidents, complaints, findings, and corrective actions to closure.
- Review AI risks periodically and after significant changes to AI tools, vendors, use cases, data inputs, regulations, or business processes.
- Update policies, procedures, training, technical controls, vendor controls, and approval processes based on lessons learned.
- Maintain continuous improvement records for AI governance, security, privacy, compliance, and responsible-use controls.

Suggested evidence: *AI incident response procedure, incident log, investigation records, corrective action records, root cause analysis, AI risk review records, management review records, updated policies or procedures, and continuous improvement records.*

Certification Review Statement

The WECH-RB certification process is based on submitted documents, applicant declarations, questionnaire responses, AI-assisted preliminary review, and administrative document review.

WECH-RB may evaluate:

- Whether required documents exist and appear relevant to the applicant's operations.
- Whether documents appear complete, current, and internally consistent.
- Whether evidence aligns with the WECH-RB Code of Conduct, including Chapter 6 where the applicant selects or is reviewed under the AI Governance, Security, and Responsible Use scope.
- Whether gaps, missing evidence, or red flags are present.
- Whether corrective actions may be needed.
- Whether the applicant meets the applicable scoring threshold for the requested certification level or add-on scope.

Unless separately stated in the certificate scope, the WECH-RB certification review is document-based and does not include an on-site audit, employee interviews, facility inspection, regulatory inspection, legal opinion, financial audit, forensic investigation, cybersecurity penetration test, AI system certification, or technical validation of AI model performance.

Applicant Acknowledgment

By participating in the WECH-RB certification process, the applicant acknowledges that:

- Submitted information should be accurate, complete, and not misleading.
- Submitted documents should be authentic and relevant to the applicant's operations.
- WECH-RB may request additional information, clarification, or corrective actions.
- WECH-RB may reject, suspend, revoke, or expire certification if information is incomplete, misleading, fraudulent, expired, or materially inconsistent with this Code of Conduct.
- Certification status may be displayed through the WECH-RB public verification page when applicable.
- If Chapter 6 is included in the certification scope or selected as an AI Trust Add-On, the applicant should disclose relevant AI tools, AI systems, AI vendors, AI data practices, and AI governance controls truthfully and completely.