CREWAVE

ESG Conduct Standards & Working Guidance

Technology connecting environment, people and trust

2026-10-21 · v1.6 · Public information guide · English

This guide explains CREWAVE's public ESG conduct standards, checks and actions for work. Formal policy approval and implementation results require separate evidence. Actual work and contracts require relevant site rules, applicable requirements and competent judgement.

Contents

1. Sustainability strategy
2. Environment
3. People & social value
4. Safety & health
5. Ethics & integrity
6. Responsible partnerships

https://crewave.com/en/esg

Sustainability strategy

We look at rail communications, traffic safety, AI and digital twins through the lenses of environment, people and trust. From product functions to operation and maintenance, connected decisions support better mobility.

ESG offers a way to examine design, implementation and operation together. The responsibilities around a technology depend on its setting, users and data boundaries. Six working themes explain CREWAVE's public ESG direction.

Key principles

1. Purpose and impact of technology

Standard: Define the problem, users and affected workers before proposal or design. Feature count or publicity alone is not a reason to deploy.

Check: Include safety, accessibility, operating effort and potential adverse effects in requirements, linked to customer and operator feedback.

Action: Remove or revise functions that do not serve the purpose. Record decisions and remaining risks in handover information.

2. Environmental criteria across the life cycle

Standard: Assess electricity, materials and replacement scope across design, procurement, installation, maintenance and disposal.

Check: Compare power assumptions, repairable components, support conditions and disposal requirements on equivalent boundaries.

Action: Choose ways to avoid unnecessary replacement and resource use among options meeting quality and safety requirements, and retain the comparison.

3. Safety and rights of users and workers

Standard: Do not disregard one group's safety or rights for the convenience of pedestrians, drivers, operators or maintainers in another group.

Check: Identify risks, access restrictions, information needs and workload by scenario and include them in design and site reviews.

Action: Document competing requirements and alternatives for an authorised decision. Disclose unresolved limitations to the customer.

4. Public statements supported by evidence

Standard: Distinguish plans, tests, contract awards, delivery and operation. Do not generalise a product or site result to the whole company.

Check: For each metric, certificate or example, check the entity, scope, period, conditions and original evidence, together with disclosure permission.

Action: Correct or withhold unsupported or overstated claims. Retain the original and reasons for correction so earlier statements remain traceable.

5. Responsibilities and approval in collaboration

Standard: Define responsibility and decision authority across design, supply, installation, testing and maintenance according to the contract and scope.

Check: Confirm interfaces, deliverables, acceptance criteria, change approvers and contacts before work starts.

Action: Resolve gaps or conflicting requirements with the relevant parties before implementation. Record verbal changes with their date and confirming parties.

6. Controls for data and AI use

Standard: Use data only for an authorised purpose and within permissions. Do not automatically finalise significant safety or personnel decisions from AI output alone.

Check: Check collection grounds, sources, authorised access, retention and the model's conditions and error risks.

Action: Restrict inappropriate use or erroneous outputs for review. Carry out necessary correction, deletion and communication.

7. Ownership, execution and improvement records

Standard: Distinguish standards from responsibility for carrying them out, and do not report plans as completed results.

Check: Link roles, work scope, review date, findings, action owners and supporting records.

Action: Define causes, actions and completion checks for omissions or recurring problems. A commitment or training plan alone does not prove completion.

8. ESG responses and submission history

Standard: Base assessment responses on the actual question and facts and evidence available at submission. Do not infer earlier answers from a score.

Check: Link each answer to evidence files and versions, applicability period, submission date and receipt. Explain non-applicability.

Action: Preserve the original when correcting an error and record the basis and changes. Do not mark an unavailable submission as verified.

Scope and working process

These are public conduct and review principles for work. Roles describe functions to designate for a task, not established departments or named appointments. Implementation and results require approved policies and records for the relevant period.

Scope

Review environmental, people and integrity impacts across planning, engineering, procurement, manufacture, testing, installation and maintenance. Apply customer requirements within their contractual, site and product boundaries.

Responsibilities

The task owner identifies risks and evidence; the supervisory role reviews priorities, resources and remaining risk. Separate preparation from evidence review and record the publication approval route.

Conduct

Distinguish verified facts, plans and public principles. Do not extend another company's requirements or a site-specific certification into company-wide results, or claim unsupported figures or assessment outcomes.

Workflow

List requirements, assess scope and risk, define responsibility and completion criteria, verify evidence, then review disclosure boundaries. Reassess changes in design, purchasing and working conditions.

Review and records

Link each requirement to its source/version, review date, scope, owner, open issues and follow-up. Preserve actual submitted ESG questions, answers and attachments separately from later improvements.

Concerns and improvement

Check source evidence and correction history when public information is inaccurate. For rights or integrity concerns, first check the ESG concern page for intake availability and a dedicated route rather than sending sensitive details to sales.

Practical considerations

1. **Define** — Problem, users and scope
2. **Design** — Functions, environment, safety and security
3. **Implement & verify** — Site conditions, tests and changes
4. **Operate & maintain** — Monitoring, service, replacement and records

When considering an intersection improvement

Waiting time alone cannot describe an intersection. A review can also consider pedestrian crossings, emergency vehicles, general traffic and operating conditions. Digital-twin scenarios can support that review; simulated comparisons are not measured environmental improvements.

Questions for review

- Are the problem and intended users clearly defined?
- Are technical performance and social or environmental effects distinguished?
- Is there information for operation and maintenance as well as installation?

https://crewave.com/en/esg-strategy

Environment

Consider transport efficiency and product life together. Examine energy and resource use, and explain the potential and limits of technology with comparable data.

Understanding environmental effects requires attention to a system's own electricity and materials as well as installation and operating conditions. Serviceable configurations, considered replacement decisions and transparent comparisons are useful starting points.

Key principles

1. Energy boundaries and source records

Standard: Define whether the boundary covers devices, networks, servers or a site. Do not present a device's consumption as whole-system savings.

Check: Record meter data, hours, load, measurement equipment and baseline period. Identify excluded equipment and differing comparison conditions.

Action: Investigate anomalies or missing data and document corrections. Exclude savings figures that cannot be verified from external materials.

2. Simulation versus measured results

Standard: Distinguish predictions, test results and operational measurements. Improved traffic flow alone does not establish a carbon reduction.

Check: Align demand, vehicle mix, time windows, signal conditions and model versions when comparing options. State factors and formulas for emissions estimates.

Action: Reassess results when inputs or validation scope change. Label results as predictions or tests until field validation is available.

3. Repair, replacement and product life

Standard: Consider repair and reuse where quality, safety and security requirements are met. Do not default to whole-unit replacement before diagnosing the fault.

Check: Check fault history, compatibility, firmware support, service access, obsolescence and post-replacement tests.

Action: Record the repair-versus-replacement decision and hand over changed components and settings. State restrictions where reuse is unsafe or support has ended.

4. Materials and packaging

Standard: Specify packaging sufficient for transport and storage protection while avoiding unnecessary material. Reused packaging must still meet quality and safety needs.

Check: Check cushioning, moisture and electrostatic protection, separation and recovery options. Inspect reused items for contamination, damage and protective performance.

Action: Revise packaging or supply arrangements after damage or excessive waste. Consider alternatives to materials that cannot be separated or recycled.

5. Recovery and disposal of electronic equipment

Standard: Handle obsolete equipment, batteries and electronic parts under applicable waste and site procedures. Do not release equipment containing data without review.

Check: Check ownership, data-erasure needs, battery condition, separation requirements and the receiving contractor's suitability.

Action: Record collection, transfer, disposal and erasure confirmation. Stop handling and escalate leakage, overheating or unauthorised removal concerns.

6. Restricted substances and environmental specifications

Standard: Select components against applicable customer, product and market restrictions and environmental specifications. Do not use another model's report as evidence.

Check: Match the manufacturer, part number, declaration or test version, substances and scope. Compare temperature, humidity, dust and water requirements with the site.

Action: Resolve non-conformity or mismatched evidence through clarification or alternatives. Do not claim unrelated certifications or tests.

7. Environmental claims and reduction statements

Standard: Environmental and savings claims require a verifiable scope and basis. Do not present plans or expected benefits as achieved results.

Check: Check the baseline, comparator, calculation boundary, factors, source data, period and excluded life-cycle stages.

Action: Remove unsupported wording or clearly qualify its scope. Correct both figures and explanations when an error is found and retain the change history.

8. Site environmental compliance and records

Standard: Identify permits, notifications, emissions and waste obligations applicable to the site and activities. Keep product-efficiency information separate from site performance.

Check: Review permit scope and validity, energy and water use, waste handling and relevant emissions records by period. Explain non-applicability.

Action: Assign ownership and corrective action for omissions, expiry or exceedances. Do not delay required reporting or urgent action for an ordinary review schedule.

9. Chemicals, releases and ecological effects

Standard: Use identified chemical containers and designated areas, following safety information for storage, mixing and protection. Keep installation within authorised land and work boundaries.

Check: Check safety information, labels, spill-response provisions and disposal methods. Identify excavation, discharge or outdoor work affecting soil, water or vegetation.

Action: Where safe, limit the spread of a release and alert the site owner. Record causes, recovery, restoration and recurrence-prevention actions.

Scope and working process

These are public conduct and review principles for work. Roles describe functions to designate for a task, not established departments or named appointments. Implementation and results require approved policies and records for the relevant period.

Scope

Review energy and resources in offices, development and testing; product materials, packaging and repairability; and waste or pollution risks during installation and maintenance. Distinguish direct control from customer operations.

Responsibilities

Design reviews lifetime, repair and material conditions; procurement checks supplier material information; site roles review storage, disposal and spill response. Data owners record units, periods and aggregation boundaries.

Conduct

Reduce avoidable resource use and consider reuse or repair. Check material handling requirements and separate waste appropriately. Energy or carbon-reduction claims require a defined baseline and calculation evidence.

Workflow

Identify resource, material and waste flows; review risks and requirements; compare design, purchasing and work options; then verify the outcome. For suspected spills or pollution, secure safety and use the responsible site escalation route.

Review and records

Maintain usage data, disposal/transfer evidence, material information and improvement records with their scope. Do not invent results for unmeasured items; distinguish gaps from plans to obtain data.

Concerns and improvement

Record impact, immediate action, follow-up and recheck results for environmental risks or data errors. Handle external concerns through an available dedicated route and review what can be disclosed.

Practical considerations

1. **Set boundaries** — Devices, facilities and operating hours
2. **Set a baseline** — Comparable conditions and source records
3. **Compare options** — Use, maintenance and replacement
4. **Explain results** — Assumptions, units, scope and limits

Comparing signal-operation options

TPS, TSP and digital twins can support scenario-based reviews of transport operations. For example, different signal strategies can be compared under the same traffic demand. Actual changes in energy or emissions require separate measurement boundaries and evidence.

Questions for review

- Are measured values distinguished from predictions and simulations?
- Have repair and component replacement been considered?
- Do environmental figures have a boundary, period and method?

https://crewave.com/en/esg-environment

People & social value

Respect for dignity and accessible mobility share a common starting point. Consider the different circumstances of colleagues, partners and people who use transport systems.

A people-centred perspective connects working relationships with the places where technology is used. It involves questioning bias unrelated to a person's work and considering differences in how people understand information or interact with systems.

Key principles

1. Dignity and freedom from harassment

Standard: Prohibit abuse, violence, sexual harassment, humiliation, threats and misuse of workplace authority. Apply the same standard to work involving employees, suppliers and customers.

Check: On a report or awareness, distinguish the timing, conduct and available evidence. First assess protection needs and conflicts affecting the reviewer.

Action: Investigate without delay where required by law and take necessary protective and corrective action. Do not retaliate for reporting or circulate case details unnecessarily.

2. Non-discrimination and fair opportunity

Standard: Do not discriminate in recruitment, assignments, training, appraisal, promotion or pay on grounds unrelated to the role, including sex, age, disability, nationality, religion, marriage or pregnancy.

Check: Set job requirements and assessment criteria in advance. Check that information requested from applicants or employees is relevant to the work.

Action: Reassess criteria and decisions when unjustified conditions or bias are identified. Review reasonable accommodation requests against the work and safety requirements.

3. No forced labour or recruitment-fee coercion

Standard: Do not compel work through violence, threats, debt or deposits, or improperly restrict resignation or movement. Do not require surrender of original identity documents as a condition of recruitment.

Check: For direct recruitment and labour agencies, check contract terms, fee allocation, document retention and resignation arrangements. Explain terms in a language the person understands.

Action: Stop coercive demands or improper charges when identified and arrange remedies such as document return or fee correction. Do not shift responsibility to the affected reporter.

4. No child labour

Standard: Do not assign work to children who do not meet applicable minimum employment-age and compulsory-education requirements. Require equivalent age checks for outsourced and site personnel.

Check: Before hiring or deployment, verify age and eligibility using lawful evidence without collecting unnecessary identity information.

Action: Stop the assignment if an age violation is found and assess corrective measures that prioritise the child's safety and education. Record how the hiring occurred and how recurrence will be prevented.

5. Protection of young workers and trainees

Standard: Assign young workers and trainees only to work compatible with their age, educational purpose and applicable law. Do not assign prohibited hazardous work or working hours.

Check: Before placement, check tasks, supervision, training schedules and required consents or documentation. Separately assess rail, road, electrical and work-at-height settings.

Action: Reassign or stop work that fails the protection requirements. Do not use trainee status to impose unrelated hazardous tasks or improper charges.

6. Working time, breaks and rest

Standard: Plan staffing and site work within applicable working-time, overtime, break and holiday requirements. Delivery pressure or urgent work does not remove required procedures.

Check: Separate ordinary, overtime, night and holiday work and compare plans with actual records. Assess travel or standby time according to the work and applicable rules.

Action: Adjust staffing, schedules or scope where excessive hours or inadequate rest are expected. Correct omissions against the facts and record differences between authorised and actual work.

7. Pay, allowances and clear employment terms

Standard: Pay must meet applicable minimum-wage and statutory allowance requirements and agreed payment dates. Explain employment terms and changes in an understandable form.

Check: Compare contracts, actual hours, calculations, deductions and pay statements. Check for unauthorised deductions or costs passed to workers.

Action: Investigate and correct unpaid amounts, calculation errors or improper deductions. Do not penalise a person in appraisal or assignments for asking about pay or requesting correction.

8. Freedom of association and legitimate expression

Standard: Respect lawful union membership, activities and collective bargaining rights. Do not discriminate, threaten or retaliate because of membership or lawful expression.

Check: Hear the parties' views separately from established facts and distinguish matters requiring consultation or bargaining from individual grievances.

Action: Review restrictions on rights or alleged adverse treatment with attention to conflicts of interest and correction. Do not compel participation or non-participation in dialogue.

9. Privacy and personal boundaries

Standard: Handle personnel, health and contact data only to the extent needed for a legitimate purpose. Do not use workplace authority to demand or share unnecessary private information.

Check: Check the data collected, purpose, permitted readers, retention basis and deletion point. Restrict health information separately from general personnel or site communications.

Action: Stop further sharing after misdelivery, excessive collection or unauthorised access and address recovery, permissions and incident response. Observe applicable statutory retention periods.

10. Accessible mobility and information

Standard: Design traffic-safety information and controls for differences in walking speed, vision, hearing, language and comprehension. Review reliance on colour or sound alone for critical states.

Check: Check display size, contrast, recognition of warnings and error recovery in realistic pedestrian, operator and maintainer scenarios.

Action: Improve presentation, placement or interaction when people miss information or cannot operate a control, and reassess. Do not claim validation for users excluded from the testing.

11. Community and site-user rights

Standard: Avoid unnecessary disruption to residents, pedestrians and facility users during installation or testing. Keep video and sensor collection within the authorised site purpose and scope.

Check: Confirm noise, lighting, restricted access, alternative routes, capture areas and required notices with the customer or operator before work.

Action: Record complaints and unexpected effects and adjust methods, timing or communication. Do not present another operator's actions as work completed by CREWAVE.

12. Concerns, protection and remedy

Standard: Do not penalise good-faith reporting, raising a concern or assisting an investigation. Do not automatically forward sensitive concerns to general sales inquiries.

Check: Check the current intake status on the concern page. Confirm receipt, reply route, protection needs and conflicts affecting the reviewer; recipient addresses are not published.

Action: Connect substantiated concerns with protection, correction, remedy and follow-up. The web form sends concerns to the CEO; no independent internal recipient is represented as appointed for matters involving the CEO.

Scope and working process

These are public conduct and review principles for work. Roles describe functions to designate for a task, not established departments or named appointments. Implementation and results require approved policies and records for the relevant period.

Scope

Respect dignity, fairness and voluntary work in hiring, terms, assignments, training, evaluation, departure and work with contractor personnel. Include mobility and information accessibility in service design reviews.

Responsibilities

Personnel/administration roles review terms and rights information; task owners review fairness in assignments and evaluation. Consider separating people with a conflict from fact-finding and decisions.

Conduct

Work relationships should exclude forced or child labour, discrimination, harassment, violence and sexual harassment. Respect understandable terms, appropriate working time, rest and compensation, and legitimate expression.

Workflow

Explain terms, review risks of harm or unfair treatment, hear affected people, consider protection and improvement, and follow up. Review accessibility against real usage conditions and diverse user needs.

Review and records

Keep necessary records of rights information, training, terms and improvement requests. Separate sensitive working-time, pay and personal evidence from public information and restrict it to authorised roles.

Concerns and improvement

Apply a non-retaliation conduct principle. Consider protection and remedy with the affected person or an appropriate representative, including information-sharing and retaliation risks during review. Check the separate page for current online intake availability.

Practical considerations

1. **Understand people** — Users, workers and neighbours
2. **Consider differences** — Accessibility, language and work conditions
3. **Improve clarity** — Understandable instructions and roles
4. **Review effects** — Usability, risk and privacy

Looking from the pedestrian's perspective

Children, older people and people with mobility limitations can experience the same crossing differently. A Smart Crosswalk review can consider sight lines, lighting, pedestrian paths, wet weather and existing safety infrastructure alongside detection functions. Installing a product alone does not remove every risk.

Questions for review

- Have different user and worker circumstances been considered?
- Can people understand the instructions and warnings?
- Does shared material contain unnecessary personal information?

https://crewave.com/en/esg-people

Safety & health

Real site conditions matter in installation, testing and maintenance. Consider worker and user safety together while identifying the distinct risks and checks for each.

Communications and traffic installations may combine electrical, traffic, height, weather and workspace risks. The topics below are general planning considerations. Actual work requires the safety requirements and competent judgement appropriate to the specific site.

Key principles

1. Pre-work site hazard review

Standard: Compare drawings with actual conditions and review task hazards before installation, testing or maintenance. Do not start without required access and work authorisation.

Check: Check traffic, pedestrians, power, nearby equipment, space, weather and visibility, linked to the site risk assessment and work plan.

Action: Reassess methods and protection for unexpected hazards. Hold the affected task until conditions are understood and inform the site owner.

2. Roles, boundaries and simultaneous work

Standard: Define task ownership, safety contacts, operating authority and interfaces before starting. Do not assume each contractor has independently resolved shared risks.

Check: Coordinate simultaneous tasks, live equipment, work-area handover, emergency contacts and escape routes with contractors and operators.

Action: Adjust timing, areas or sequence when conflicts or ownership gaps appear. Communicate revised conditions before resuming.

3. Safe electrical and equipment work

Standard: Only authorised, competent personnel may operate equipment or perform electrical work under site procedures. Prohibit unauthorised energisation, bypasses and setting changes.

Check: A competent person checks energy sources, applicable isolation and lockout procedures, tools, protective equipment and test permission.

Action: Restrict work and access after unexpected energy, damage or overheating. Restore and energise only following required checks and authorisation.

4. Traffic, height and lifting controls

Standard: Control traffic, falls, trapping and falling objects through segregation and suitable methods. Protective equipment alone does not replace a risk review.

Check: Check traffic management, platforms and access, lifting-equipment suitability, handling routes and personnel competence.

Action: Stop the affected task after an intrusion, equipment fault or adverse weather and restore safe conditions. Record the revised plan and decision to resume.

5. Test transitions and restoration

Standard: Separate testing from live operation and agree effects on alarms, communications and signals with the operator. Do not leave a test state in service.

Check: Check baseline settings and backups, changes, temporary connections, operating effects and restoration ownership before testing.

Action: Verify settings, connections, alarms, tools and site condition at completion and hand over to the operator. Do not mark work complete before restoration is confirmed.

6. Stopping and reporting unsafe conditions

Standard: Do not continue work through imminent danger or significant unplanned hazards. Do not penalise raising a hazard or a justified stop.

Check: First assess personal safety, possible further harm, site contacts and emergency needs. Do not require entry into danger to collect evidence.

Action: Follow site evacuation and notification procedures. A competent person must confirm risk control and restart conditions; record causes and actions for future planning.

7. Product performance and site safety

Standard: Do not describe detection performance or certification as a guarantee against every accident. Review product requirements separately from installation and maintenance risks.

Check: Review test scope, conditions and limits, false or missed detection, failure behaviour and operator checks.

Action: Assess and validate uses outside the tested conditions before deployment. State limitations and necessary operating measures in instructions and handover records.

8. Training, health, emergency readiness and improvement

Standard: Check training and competence required for the task and include health risks in planning. A training plan does not establish completion by every employee.

Check: Verify participants, courses, dates, completion records, emergency contacts and contractor training and protection conditions.

Action: Address missing training, incidents and near misses through deployment requirements and prevention. Minimise personal health data and keep it out of general site records.

Scope and working process

These are public conduct and review principles for work. Roles describe functions to designate for a task, not established departments or named appointments. Implementation and results require approved policies and records for the relevant period.

Scope

Review risks in development, testing, assembly, electrical/communications work, installation, maintenance and shared work. Consider office ergonomics, travel and seasonal conditions where relevant.

Responsibilities

The work lead checks hazards, sequence and personnel; participants check training and protection. For contracted/shared work, clarify control, emergency contacts and stop/restart decision roles beforehand.

Conduct

Prioritise removing/substituting hazards and improving equipment or methods, with appropriate protective equipment. For imminent danger, secure safety and follow site emergency procedures; do not continue without verified safe conditions.

Workflow

Check hazards before work, implement controls and training, monitor changes, inspect at completion, then review incidents/near misses and prevention. Reassess changed conditions instead of reusing an outdated assessment.

Review and records

Link risk reviews, pre-work checks, training, equipment inspections and actions to the site, work and period. Incident-free or training-rate claims require complete records and a verified denominator.

Concerns and improvement

Report hazards/near misses through the responsible site route and use emergency arrangements for urgent danger. Do not send sensitive health or examination records to general inquiries; authorised roles should review only necessary information for protection.

Employee health

These principles address work-related effects on health. Implementation must be checked against records for the relevant people and period; individual examination, medical and counselling information is not published.

Plans and actual examinations

The 2026 safety work plan lists annual comprehensive examinations, pre-employment checks and seasonal health education. The 2025 monitoring material includes general/special examination management and working-environment measurement checks. These support planning/review content, not claims of universal completion or an established counselling programme.

Coverage and roles

Administration checks coverage and timing against work/exposure conditions; work leads review scheduling and necessary adjustments. Leave medical judgement to qualified professionals and avoid broad collection of diagnoses by general managers.

Notification, examination and follow-up

Check coverage, provide individual information and practical access, confirm only necessary completion information, review protection/work adjustments, and follow up. Before publishing aggregate indicators, verify non-identifying scope, period and denominator.

Working conditions and prevention

Review work-specific noise, substances, electrical/site climate risks, repetition and prolonged screen work. Consider elimination/substitution, engineering controls, methods, rest and protective equipment, and connect applicable workplace measurements to improvements.

Health concerns and sensitive information

Clarify the route for health concerns, authorised viewers and follow-up responsibility beforehand. Do not publish personal examination, diagnosis or counselling information or send it to sales/general inquiries or the online concern form. Define purpose, minimum fields, retention and deletion before necessary handling.

Scope of safety records

Scope of the ISO 45001 certificate

Certificate OHS-0590, reissued by KOSRE on 28 March 2026, identifies Crewave Co., Ltd., 611Ho, 6F, 268 Hagui-ro, Anyang, for the design, development and manufacture of wired and wireless communication devices. Its stated validity is 22 March 2025–21 March 2028. This scope does not extend to other entities or sites, or certify individual product safety.

Early-2026 industrial safety training records

Completion records are available for the January–February 2026 industrial safety course for SME employees. They relate to that course and its participants, and do not establish completion for every employee or site. Individual certificates and identifying information are excluded from public materials.

Practical considerations

1. **Before work** — Scope, risks, roles and contacts
2. **During work** — Changed conditions and nearby movement
3. **Test & restore** — Operational effects, settings and temporary links
4. **Hand over** — Status, outstanding items and records

Servicing equipment at an operating traffic facility

A purely technical checklist can overlook moving traffic and pedestrian routes. A service plan can also consider access, coordination with operators, effects on operation and restoration checks. This example does not replace a site-specific risk assessment or professional safety procedure.

Questions for review

- Have the work area and public movement been considered?
- Is it clear who to contact about unexpected conditions?
- Have the operational state and handover items been checked after testing?

https://crewave.com/en/esg-safety

Ethics & integrity

Trust in technology begins with trust in business relationships. Fair dealing, accurate records and responsible use of information are essential perspectives for ethical decisions.

Customer and partner relationships, technical information, external statements and personal data all involve responsibilities. In ambiguous situations, separate facts from interests and examine authority, evidence and records.

Key principles

1. Fair dealing and no collusion

Standard: Do not improperly coordinate pricing, bids or trading terms, obtain competitors' confidential information improperly, or use bargaining power to impose unfair conditions.

Check: Check quotation, evaluation and ordering criteria and define what information may be shared with competitors or suppliers.

Action: Decline collusive requests or improper terms, record the facts and notify an authorised reviewer. Do not delete records to conceal the issue.

2. No bribery or improper benefits

Standard: Do not request, offer or accept benefits intended to influence awards, acceptance, selection or payment, including through third parties.

Check: Check the business purpose, actual beneficiary, connection to the transaction, approval basis and applicable law and customer rules.

Action: Reject improper demands and record the offer and response. Hold an unclear benefit for review before giving or accepting it.

3. Disclosing and avoiding conflicts

Standard: Do not conceal interests of yourself, family or personal business that may affect purchasing, evaluation or recruitment decisions.

Check: Check relationships, financial interests and authority before selection or transactions. A person should not solely approve a matter involving their own interest.

Action: Disclose a conflict and arrange recusal or separate review. Record the decision basis and participants.

4. Truthful test, acceptance and expense records

Standard: Do not fabricate or alter test, acceptance, delivery, working-time or expense evidence. Do not present selected favourable results as the complete outcome.

Check: Match source records, authors, dates, models or versions, changes and approval information.

Action: Preserve the original and record who corrected it, when and why. Communicate corrections affecting a contract or customer decision to the relevant party.

5. Technical information, trade secrets and IP

Standard: Use drawings, source code, credentials, proposals and customer information only for permitted purposes. Do not move them to unapproved external services or personal accounts.

Check: Check ownership, contractual use and disclosure rights, authorised readers and return or deletion obligations, including third-party rights in public material.

Action: Contain unauthorised sharing through recovery, access restriction and incident response. Recheck disclosures before delivery or publication.

6. Personal data and access permissions

Standard: Process only necessary personal data and limit access by work responsibility. Do not permit shared accounts or unnecessary access after departure or contract end.

Check: Review collection grounds, recipients, accounts, permissions and retention or deletion rules. Match website inquiry and download handling to the published privacy notice.

Action: Restrict access or sharing after excessive permissions, misdelivery or suspected exposure and assess applicable incident and notification duties. Follow statutory retention where required.

7. Responsible AI use and explanation

Standard: Do not present AI output as verified fact or error-free judgement. Do not submit customer secrets or personal data to external AI without checking authority and handling terms.

Check: Review data rights and sensitivity, false detection and bias, operating conditions, human review points and ways to stop or correct use.

Action: Limit use or disclosure when errors or rights risks appear and correct results. Explain the degree of automation and human responsibility to customers and users.

8. Escalating unclear or improper requests

Standard: Do not carry out a request that may conflict with a contract, law or authority solely because of a deadline or superior's instruction.

Check: Check the requester, requested action, applicable terms, records and conflicts. Distinguish suspicion from established facts.

Action: Hold the affected action for appropriate review until concerns are resolved. Use the published concerns route for reports and do not retaliate for good-faith reporting.

9. Trade restrictions and authentic components

Standard: Do not evade applicable export controls, sanctions or trade restrictions, or supply suspect or untraceable parts as confirmed authentic.

Check: Check counterparties, destination and end use, required permissions, suppliers, part numbers and manufacturing provenance.

Action: Hold transactions or use when restrictions or counterfeiting are suspected for competent review. Assess segregation, replacement and customer notification.

Scope and working process

These are public conduct and review principles for work. Roles describe functions to designate for a task, not established departments or named appointments. Implementation and results require approved policies and records for the relevant period.

Scope

These ethical conduct principles cover sales/tenders, procurement/contracts/payment, R&D, customer/supplier information and external communications. Read them alongside contractual duties and approved internal rules.

Responsibilities

Task owners identify conflicts, improper demands and record errors; approvers review appropriateness and evidence. Separate involvement where personal, family or related-business interests could affect judgement.

Conduct

Do not give or request improper payments, hospitality or favours, collude, abuse bargaining power or falsify records. Review gifts/hospitality by purpose, recipient, circumstances and applicable rules; pause when appropriateness is unclear.

Workflow

Check terms and conflicts, obtain proper approval, document contracts/acceptance/payment accurately, and record changes/exceptions. Preserve relevant records and refer suspected impropriety to an authorised review route.

Review and records

Check selection rationale, approvals/changes, consistency across contracts/acceptance/payment, and publication sources. Record reasons for missing evidence or later corrections; exclude confidential customer, personal and business information from public materials.

Concerns and improvement

The conduct principle prohibits dismissal, threats, retaliation, ridicule or other adverse treatment for good-faith reporting or cooperation. Limit identity/case information to necessary authorised roles and consider remedy with the affected person or representative. Check current availability, the CEO delivery route and data-handling information on the online concern page.

Information security management principles

These public management principles address confidentiality, integrity and availability. They do not assert completed implementation of specific controls or ISMS or ISO 27001 certification.

Assets and responsibility

Identify customer drawings, source code, contracts, personal data and test records by purpose and sensitivity. Distinguish asset management, use and approval roles; review storage, external disclosure and retention needs. Exclude internal accounts, network layouts and vulnerability details from public information.

Granting, changing and removing access

Limit access to people and scope needed for legitimate work. Recheck access on joining, transfer, departure or contract end and record approval/change/removal. Review reasons, ownership and expiry for shared or exceptional access; do not send passwords in documents or inquiry forms.

Awareness and everyday handling

Consider information classification, recipient checks, safe transfer, screen/print handling and suspicious communications in role-based awareness. Before sharing, check recipients, purpose and minimum scope; contain and escalate suspected misdelivery/loss. The 2026 safety work plan includes security education, which does not establish complete information-security implementation.

Supplier and service security

Before outsourcing, remote maintenance or cloud use, check information sharing, access duration, subcontracting, incident contacts and return/deletion terms. Review customer restrictions and retain evidence of how accounts, access and held information are handled at closure.

Incident response and review

Use a sequence of detection, authorised escalation, impact/spread assessment, safe containment and evidence preservation, recovery and prevention review. Protect records of timing, detection, impact, action and rechecks; review applicable duties and approval for external notification. This guidance does not claim ISMS or ISO 27001 certification.

Practical considerations

1. **Establish facts** — People, circumstances and evidence
2. **Review interests** — Conflicts, relationships and authority
3. **Check the decision** — Relevant requirements and clarifications
4. **Record & explain** — Rationale, scope and changes

Communicating a product test result

A basic performance assessment belongs to the model and items actually tested. It should not be generalised to other products or every installation. Relevant CREWAVE product pages identify the model, assessment items, validity and limitations.

Questions for review

- Could another person understand the basis of the decision?
- Have permission and scope for sharing been checked?
- Have uncertain statements been kept distinct from established facts?

https://crewave.com/en/esg-ethics

Responsible partnerships

Mobility systems bring together different technologies and field experience. We value clear responsibilities and a shared understanding of quality, safety, information and environmental considerations.

Supply-chain responsibility extends beyond purchasing a component. Specifications, change communication, working conditions, permission to use information and handover all matter. These topics provide general perspectives for reviewing a collaboration.

Key principles

1. Fair supplier selection and evaluation

Standard: Evaluate suppliers on technical fit, quality, delivery, safety, support and terms. Do not change criteria for personal relationships or improper benefits.

Check: Check specifications, evaluation criteria, submitted evidence and reasoning, requesting evidence appropriate to the actual supply scope.

Action: Clearly identify missing information. Independently review and correct errors or conflicts and retain the result.

2. Contracts, acceptance and payment

Standard: Agree understandable scope, responsibilities, schedule, acceptance and payment terms. Do not impose unagreed costs or work through superior bargaining power.

Check: Compare drawings, specifications, deliverables, acceptance criteria, change approval and payment terms. Identify gaps between customer and supplier commitments.

Action: Document agreed effects on cost and schedule for changes. Resolve acceptance or payment disputes with evidence; do not use unjustified delay as bargaining pressure.

3. Component changes and traceability

Standard: Review substitutions and specification or process changes under approval requirements. Similar appearance does not establish equivalence.

Check: Check the reason, part number, interface, power, environment and security effects, further tests and required customer approval.

Action: Align approved changes across drawings, parts lists, software and acceptance records. Restrict unauthorised changes while assessing impact and recovery.

4. Protecting shared work information

Standard: Limit shared information to the agreed purpose and recipients. Do not permit uncontrolled onward sharing of customer drawings, source code or credentials.

Check: Check confidentiality, subcontracting, access, joint-output rights and return or deletion duties at completion.

Action: Restrict sharing or access after misdelivery or permission breaches and address recovery and response. Verify authority and record any changed sharing scope.

5. Labour and human rights in partnerships

Standard: Apply prohibitions on forced or child labour, harassment, discrimination and improper charges in partnerships. Do not create delivery pressure that encourages violations.

Check: Review relevant age, work, rest, pay, recruitment-cost and reporting arrangements to the extent needed for the contract and site.

Action: Prioritise protection and causes when addressing risks. Set actions, ownership and verification; a supplier's assurance alone does not establish completion.

6. Contractor and shared-site safety

Standard: Share hazards and work boundaries among organisations at the same site. Contracting arrangements do not remove necessary safety coordination.

Check: Confirm plans, responsible contacts, training and competence, protection, simultaneous work and emergency communication before starting.

Action: Hold and coordinate work after significant hazards or conflicts. Record restart conditions, communications and follow-up checks.

7. Environmental and restricted-substance evidence

Standard: Communicate applicable environmental and substance requirements for supplied items. Possession of a document does not establish conformity of every model.

Check: Match issuer, parts or models, revision date, substance scope and customer requirements in declarations and tests.

Action: Resolve missing or inconsistent evidence through clarification or alternatives. Do not deliver non-conforming items without appropriate handling and disclosure.

8. Handover, support and end of supply

Standard: Hand over usable operating and maintenance information as well as installation results. Do not promise unverified long-term supply or indefinite support.

Check: Check configurations, tests, parts, versions, incident handling, warranty, end of support and replacement conditions against the contract.

Action: Assign ownership and timing for missing information. Communicate obsolescence or support changes with alternatives and transition considerations where operations may be affected.

9. Origin, responsible minerals and supply routes

Standard: Check origin and supply information required for the item and review forced-labour, conflict and illicit-sourcing risks. Unknown provenance is not confirmed conformity.

Check: Review suppliers, manufacturing countries and available smelter or refiner information with its product scope and period.

Action: Assess clarification, alternative sourcing or mitigation for uncertain or high-risk routes. Record information limits and decision grounds.

10. Risk findings, correction and verification

Standard: Connect assessments to actual risks and improvement work rather than stopping at a score or signed declaration.

Check: Identify severity, affected people, causes, action ownership and verification evidence. Define communication and review scope for lower-tier suppliers.

Action: Compare completion reports with evidence and check recurrence. Consider further measures within contractual authority if improvement fails; do not promise unauthorised sanctions.

Scope and working process

These are public conduct and review principles for work. Roles describe functions to designate for a task, not established departments or named appointments. Implementation and results require approved policies and records for the relevant period.

Scope

These supply-chain review principles cover components, equipment/software, outsourced engineering/manufacturing, installation and maintenance. Check supplier-code expectations against contractual scope and risk.

Responsibilities

Procurement/contracts explain requirements and evidence requests; technical, quality and site roles assess relevant risks and records. The supervisory role reviews unresolved risk, adequate improvement and relationship decisions.

Conduct

Use transparent terms and proportionate evidence requests. Quality approval does not establish human-rights, environmental or integrity compliance. Distinguish missing evidence from a confirmed breach and avoid excessive collection or disclosure.

Workflow

Identify risks by work, location, materials and labour; explain relevant criteria; review documents/site conditions; agree gaps and actions; and verify follow-through. For serious risks, consider urgency/severity, protection, improvement and relationship terms.

Review and records

Record applicable criteria, assessment scope, evidence dates/sources, action owners, due dates and verification. Distinguish originally submitted evidence from subsequent additions/improvements and check each customer's reassessment rules.

Concerns and improvement

Consider conflicts with commercial contacts when choosing an appropriate dedicated route for supplier concerns. Do not impose unjustified commercial disadvantage for raising concerns; verify agreed improvements. Check current availability on the separate online concern page.

Supplier code of conduct

These public conduct principles express expectations for collaboration. Read them alongside applicable contracts and implementation evidence; another company's rules are not presented as CREWAVE's pre-existing internal regulations.

Human rights and labour

Collaboration should exclude forced and child labour, discrimination and harassment, and respect voluntary work, understandable terms and legitimate rights.

Safety and health

Review work risks, protective measures and health effects, and clarify responsibilities and contacts for contracted work.

Environment

Review applicable environmental requirements, resource use, waste and materials. Environmental statements need verifiable evidence.

Integrity and fair dealing

Exclude bribery, collusion and improper demands; identify conflicts and clarify contractual, acceptance and payment terms.

Information and intellectual property

Respect customer and supplier information and intellectual property. Use and sharing must remain within authorised purposes and scope.

Responsible sourcing

Review material provenance and supply-chain risks, and connect identified risks with appropriate improvement and follow-up.

Concerns and evidence-based collaboration

Clarify grievance responsibilities, access and confidentiality conditions. Reporters should not face improper adverse treatment, and assessment records must reflect actual facts.

Practical considerations

1. **Understand needs** — Specifications, capability and scope
2. **Clarify terms** — Responsibilities, quality, acceptance and payment
3. **Communicate changes** — Effects, compatibility and site conditions
4. **Hand over records** — Tests, configuration and support

Considering a substitute communications component

Similar appearance or price does not establish equivalent interfaces, power requirements, environmental specifications or support. A substitution review can consider differences from the original specification, affected tests, updated drawings and customer handover information.

Questions for review

- Is it clear who needs to understand and decide on a change?
- Are supply scope and maintenance responsibilities understood consistently?
- Are component, test and handover document versions connected?

https://crewave.com/en/esg-partners

Resources & inquiries

This guide and the topic pages can be read without a request form. Company profiles and product documents use the existing document-request process.

https://crewave.com/en/esg-resources

The general inquiry channel is for public information and business questions. Do not send sensitive incident details or identifying records through general sales inquiries. This channel is not presented as a dedicated reporting, anonymity or protection process.

https://crewave.com/en/privacy

ESG concerns and grievances

Purpose, fields and delivery

The CREWAVE CEO is responsible for reviewing concerns, taking action and communicating outcomes. Category, details and consent are required; name and reply email are optional. The server sends the concern and optional reply details to one designated recipient, without sales recipients, CC or BCC.

Transmission and storage

The website does not store the content, name or reply address in its database or application logs and does not save drafts. Email remains in the existing sending and receiving mail systems. The confirmed region for the mail relay function and duplicate-prevention store is Ohio, United States. Request hashes and timestamps are held separately from report content by the mail relay to prevent duplicates. This region does not establish where every service processes logs, backups or support work.

Retention and deletion

Ordinary concern records and mail copies managed by the company are retained only as needed for follow-up, for no more than 90 days after the case is closed following review, action and outcome communication, and are deleted without delay when no longer needed. Records with a separate lawful retention basis, including statutory duties or lawful requests, are managed with the basis, scope, period or review date recorded separately. Staff manually review retention needs and deletion dates; automatic deletion is not configured. This rule does not guarantee complete deletion of every service provider log or backup within the same period and does not limit deletion duties under applicable law.

Acknowledgement and progress targets

Our operating targets are acknowledgement within two business days and action or a progress update within 10 days of receipt. Staff provide these notices where a reply route is available; automatic replies are not provided. Targets are counted from the day after receipt; business days exclude Korean weekends and public holidays, and the 10-day target uses calendar days. Applicable duties and deadlines for investigation, protection and notification take priority. These targets do not replace statutory deadlines or create a waiting period before investigation. A receipt number does not confirm review by the recipient or completion of investigation or remedy.

Confidentiality, protection and anonymity

You may omit your name and reply email, but this form is not a fully anonymous communication channel without technical connection records. Concern information is handled within the authorised scope needed for the case, in accordance with confidentiality and non-retaliation duties and personal-data rights under applicable law. Legal protection and permitted disclosures depend on the nature and route of the report and the relevant law. Absolute anonymity or identical legal protection is not guaranteed for every report.

Consent and personal-data rights

If you refuse consent, the web concern cannot be sent. You may use this form to request access, correction, deletion or withdrawal of consent; include your receipt number if available. Provide a reply email if you want a response. Requests are handled under the requirements and deadlines of applicable law. No independent internal recipient has been designated for matters involving the CEO.

- Human rights / labour / harassment / discrimination
- Health and safety
- Environment
- Ethics / corruption / fair dealing
- Supplier concerns
- Privacy and information security
- Other ESG concerns

https://crewave.com/en/esg-concerns

Review and handling process

These principles guide review of a concern. Scope depends on its nature, urgency, conflicts and applicable rules; they do not guarantee that every investigation finishes within the same period.

Check the concern and reply route

Review circumstances, timing, relevant work and requested action. Request only necessary additional information; acknowledgement does not mean that an allegation has been substantiated.

Assess urgency and protection

First consider physical danger, spreading data exposure, evidence loss and retaliation risk. Immediate danger requires the relevant emergency route rather than waiting for ordinary review.

Check conflicts and assign review

Consider interests of people involved and ways to preserve independent review. No independent alternative internal recipient is represented as appointed for concerns involving the CEO. Use of applicable official external channels is not restricted.

Establish facts and hear relevant people

Distinguish assumptions from direct observations and check sources, timing and changes to evidence. Hear relevant people as needed and minimise sharing of case and identity information.

Consider protection, correction and remedy

Consider correction and remedy based on findings and impact, with input from the affected person or appropriate representative. Do not promise disciplinary or contractual measures without authority and grounds.

Communicate progress and outcome

Where a reply route exists, communicate progress, further review needs and outcomes within permissible disclosure limits. Other people's personal data and protected investigation material may not be fully disclosed.

Check action, recurrence and retaliation

Follow up on implementation, recurrence and adverse treatment connected with reporting. Assess the need for further review when new facts or insufficient action are raised.

Close and manage records

Ordinary concern records and mail copies managed by the company are retained only as needed for follow-up, for no more than 90 days after the case is closed following review, action and outcome communication, and are deleted without delay when no longer needed. Records with a separate lawful retention basis, including statutory duties or lawful requests, are managed with the basis, scope, period or review date recorded separately. Staff manually review retention needs and deletion dates; automatic deletion is not configured. This rule does not guarantee complete deletion of every service provider log or backup within the same period and does not limit deletion duties under applicable law.

Timing, deadlines and replies

Acknowledgement and progress targets

Our operating targets are acknowledgement within two business days and action or a progress update within 10 days of receipt. Staff provide these notices where a reply route is available; automatic replies are not provided. Targets are counted from the day after receipt; business days exclude Korean weekends and public holidays, and the 10-day target uses calendar days. Applicable duties and deadlines for investigation, protection and notification take priority. These targets do not replace statutory deadlines or create a waiting period before investigation. A receipt number does not confirm review by the recipient or completion of investigation or remedy.

Statutory employee grievance processes

Under Article 28 of the Act on the Promotion of Employees' Participation and Cooperation, a grievance committee member must notify the worker of action and results within 10 days of hearing the grievance. For grievances under Article 25 of the Equal Employment Opportunity Act, Article 18 of its Enforcement Decree generally requires handling or referral to the labour-management council within 10 days of receipt, with notice of the result or referral. These have different applicability conditions and are not a universal deadline for external reports. Acknowledgement alone does not fulfil these duties.

Harassment and urgent matters

Where applicable law requires it, workplace bullying or sexual harassment must be investigated without delay after a report or awareness, with necessary protective measures. These duties do not wait for a general reporting schedule or web-form activation, and are distinct from a universal investigation-completion deadline.

Acknowledgement versus completion

Check the current intake status on the concern page. Receipt and investigation completion are distinct; a submission is not presented as completed unless the server confirms acceptance. Submission is available only when server readiness has been checked and the form is enabled.

Start point and counting method

For an individual schedule, specify acknowledgement date, applicable process, start point, business or calendar days and next update. If business days are used, clarify treatment of Korean weekends/public holidays. No fixed completion deadline has been set for general external concerns.

Further review and schedule changes

Where additional evidence, interviews or external review are needed, explain the reason, remaining work and next update to a reachable reporter. Schedule changes do not themselves extend applicable statutory duties.

Limits where a reporter cannot be reached

Even without a name, email addresses and sender information may be conveyed. Without a reachable reply route, further fact-finding, progress updates and outcome communication may be limited. Anonymous two-way messaging is not currently provided.

- Employees' Participation Act, Article 26 ↗ — checked version effective 2022-12-11
- Employees' Participation Act, Article 28 ↗ — checked version effective 2022-12-11
- Equal Employment Opportunity Act Enforcement Decree, Article 18 ↗ — checked version effective 2026-09-18
- Labor Standards Act, Article 76-3 ↗ — checked version effective 2026-10-08
- Equal Employment Opportunity Act, Article 14 ↗ — checked version effective 2026-09-18

Legislation and official agency sources

Legislation and official agency sources

Read legislation, agency guidance, corporate references, CREWAVE's voluntary conduct standards and actual results as distinct types of information. Effective dates identify the checked legal version, not the first introduction of each duty or the adoption or implementation of a CREWAVE policy. Agency revision/publication dates are identified separately. Applicability requires checking the business, size, case and original provisions.

Official sources checked: 2026-10-21

Act

Personal Information Protection Act

Effective 2026-09-11 · Act No. 21445

Articles 15, 21, 23, 26, 28-8 and 30: collection/use, destruction, sensitive information, outsourcing, overseas transfer and privacy notices

Agency guidance

PIPC Guidelines for Preparing a Privacy Policy

Revised April 2026 · posted 2026-04-23

Reference for describing retention, destruction, processors and overseas transfers

Act

Public Interest Whistleblower Protection Act

Effective 2026-10-01 · Act No. 21503

Articles 2, 6, 8-2, 12 and 15: scope, reporting routes, proxy reporting, confidentiality and adverse measures

Official service guidance

ACRC Guidance on Reporting through an Attorney

Service information as checked

Official information on eligibility and procedure for reporting to the ACRC through an attorney

Act

Act on the Promotion of Employees' Participation and Cooperation

Effective 2022-12-11 · Act No. 18927

Articles 26 and 28: grievance committee members and handling procedures

Act

Equal Employment Opportunity and Work-Family Balance Assistance Act

Effective 2026-09-18 · Act No. 21476

Articles 14 and 25: workplace sexual harassment response and grievance resolution

Enforcement decree

Enforcement Decree of the Equal Employment Opportunity Act

Effective 2026-09-18 · Presidential Decree No. 36589

Article 18: handling, notification and records for applicable grievances

Act

Labor Standards Act

Effective 2026-10-08 · Act No. 21533

Article 76-3: measures in response to workplace bullying

Act

Occupational Safety and Health Act

Effective 2026-08-01 · Act No. 21374

Articles 3 and 36: applicability and risk assessment

Act

Serious Accidents Punishment Act

Effective 2022-01-27 · Act No. 17907

Article 3 and supplementary provisions: industrial-accident chapter scope and phased commencement

Act

Act on Fair Labelling and Advertising

Effective 2025-01-21 · Act No. 20712

Article 5: substantiation of factual labelling and advertising claims

Act

Environmental Technology and Industry Support Act

Effective 2026-09-26 · Act No. 21065

Article 16-10: unfair claims about a product's environmental attributes

FTC administrative guidance

Guidelines for Review of Environment-Related Labelling and Advertising

Effective 2023-09-01 · FTC Rule No. 442

Review criteria for evidence, comparison scope and product lifecycle in environmental claims

Official reference frameworks

The guidance draws primarily on Hyundai Rotem's supplier expectations and uses other companies' official materials as structural references. Their policies, organisations, targets and results are not CREWAVE's implementation records. This information does not replace actual assessment responses, evidence submissions or customer evaluation.

Hyundai Rotem Supplier Code of Conduct

Primary reference: ethics, environment, labour and human rights, safety, management systems and due diligence

Hyundai Rotem 2026 Sustainability Report

Supporting reference: pages 68–69, supply-chain assessment and evidence review

Hyundai Motor Company Supplier Code of Conduct

Revised 2026-09-09; supplementary reference from a separate company, subject to the relevant business relationship

Samsung Display Human Rights Principles

Reference for specific human-rights topics, prohibited conduct, scope and action. The company's organisation and implementation results are not attributed to CREWAVE

Samsung Display Sustainability Strategy

Information-architecture reference: connecting strategy to human rights, environment, compliance, suppliers and reports

Samsung Display Supplier Code of Conduct v8.0

Reference topics for labour/human rights, health/safety, environment, ethics and management systems

KAON Group 2025 Sustainability Report

Communications-industry reference: structure of security roles, assets, access and response, health/safety review and supplier improvement

DASAN Ethical Conduct Principles

Reference structure for fair dealings, conflicts, information protection and respectful working relationships

HUMAX Networks Supplier Code of Conduct

Korean edition, June 2026: reference structure for supplier expectations, review, correction and responsible sourcing

HUMAX Networks 2026 Sustainability Report

Pages 53–55 and 60–62: reference structure for employee health, concerns and information security