

Overview

IEM International, Inc. and its divisions, business units, subsidiaries, and affiliates (collectively “IEM”) require all providers of products or services to or for IEM, including contractors, consultants, vendors, and lower-tier providers (“Suppliers”), to meet these Supplier Standards of Conduct (“Standards”).

Suppliers must comply with these Standards, applicable laws and regulations, and their agreements with IEM when seeking, obtaining, or conducting IEM business. Compatible requirements apply together; conflicts are governed by the Order of Precedence section. Direct questions and misconduct reports to ethics@iem.com. The Reporting and Nonretaliation section provides reporting protections and general procedures; topic-specific notification requirements also apply.

Suppliers must explain applicable requirements to their directors, officers, employees, temporary workers, agents, and other representatives involved in IEM business in a form and language they understand, and ensure compliance. Required training must be completed and documented before affected work begins, when requirements change, and periodically as risk warrants. Lower-tier duties appear in the Compliance Management and Lower Tiers section.

Suppliers must not bind or speak for IEM, or appoint another party to do so, without prior written authorization from an authorized IEM representative. Approval to subcontract does not confer that authority.

People and Workplace

Human Rights Due Diligence

Suppliers must respect internationally recognized human rights and conduct due diligence proportionate to the risks to workers, disaster survivors, and communities in their operations and supply chains that support IEM work. They must identify, prevent, and mitigate adverse impacts; consult affected persons or their legitimate representatives where appropriate and safe; and assess the effectiveness of their actions. Suppliers must provide for or cooperate in the lawful remediation of harm they cause or contribute to, and use available influence to prevent or mitigate harm directly linked to their products or services through their business relationships.

Nondiscrimination and Harassment Prevention

Suppliers must provide equal employment opportunity, base employment decisions on lawful, job-related criteria, and comply with applicable nondiscrimination,

accommodation, and anti-retaliation requirements. Required accommodations include those for disability, religion, pregnancy, childbirth, and related medical conditions. Workplaces must be free of unlawful discrimination, harassment, including sexual harassment, bullying, threats, intimidation, and physical or psychological abuse.

Suppliers must treat workers, applicants, IEM personnel, customers, disaster survivors, program beneficiaries, and the public with dignity and respect. Employment and supplier outreach and selection must be lawful and support fair access. These Standards neither authorize unlawful preferences, exclusions, or quotas nor excuse legally required affirmative obligations.

Protection of Survivors and Program Beneficiaries

Suppliers must not exploit disaster survivors or program beneficiaries, solicit sexual or other personal favors, or condition assistance, referrals, or services on unauthorized payments or personal benefits. They must follow applicable safeguarding, accessibility, and beneficiary-protection requirements, including mandatory reporting of suspected child abuse or abuse of vulnerable adults. Suspected abuse related to IEM work must be reported promptly through these Standards’ reporting and emergency channels without delaying required reports to authorities. Assistance must follow authorized program criteria and must not be withheld in retaliation for a complaint. Suppliers working with survivors or beneficiaries must communicate safe, accessible reporting options appropriate to children, persons with disabilities, and persons with limited literacy or language access. Responses must protect affected persons’ safety, dignity, privacy, and access to support, respect their wishes where lawful, and avoid further harm without delaying mandatory reports.

Wages and Working Conditions

Suppliers must comply with applicable wage, overtime, benefit, working-hour, meal and rest period, leave, and worker-classification requirements, including for temporary and outsourced labor. They must accurately record all compensable time, prohibit off-the-clock work, pay amounts due on time, and provide understandable wage statements sufficient to verify compensation. Unlawful deductions and deductions as disciplinary punishment are prohibited.

Suppliers must comply with applicable wage determinations, prevailing-wage and fringe-benefit requirements, payroll certifications, and lower-tier labor

clauses. Scheduling must comply with legal limits, ensure adequate rest, and control fatigue-related safety risks, including during emergency deployments. Overtime must not be obtained through threats or coercion.

Workplace Substance Use and Fitness for Duty

Suppliers must prohibit unlawful controlled-substance use, possession, sale, or distribution in IEM work. Personnel must not work when alcohol, drugs, medication, fatigue, or another condition prevents safe performance. Suppliers must assess fitness for assigned duties through lawful, job-related procedures and provide required reasonable accommodations. Lawful medication use or a medical diagnosis alone does not establish unfitness.

Suppliers must comply with applicable testing, medical confidentiality, transportation, and customer requirements. A safety concern requires prompt protection of affected persons and a lawful assessment before assigning duties that present an unresolved risk.

Labor Exploitation and Human Trafficking

Suppliers must not use or procure forced, bonded, indentured, involuntary, or exploitative prison labor, slavery, or human trafficking in goods or services supplied to IEM. Coercion, deceptive recruitment, and unreasonable movement restrictions are prohibited. Workers must be free to leave or end their employment, subject only to lawful, reasonable notice, without coercion or penalties that compel continued service. Suppliers and recruitment agents must not destroy, confiscate, conceal, or deny access to workers' identity or immigration documents, charge recruitment fees, or use debt to compel service. Prohibited fees must be promptly reimbursed.

Suppliers must provide written employment terms in a language workers understand before work begins and before recruitment-related relocation, with at least five days' advance delivery where required. They must provide lawful, safe housing when furnished and return transportation when required by law or contract. Suppliers, their personnel, and agents must not procure commercial sex acts during the agreement's performance. Suppliers must monitor recruitment agents and affected lower tiers, immediately report credible allegations of trafficking or other violations of this section concerning IEM work to ethics@iem.com, and support lawful protection and remediation for affected workers. Independently applicable government notices,

compliance plans, certifications, and flow-downs must be completed without awaiting IEM approval.

Child Labor

Workers supporting IEM must meet the highest of age 15, the applicable minimum employment age, or the age of completion of compulsory education. Suppliers must verify age lawfully. Workers under 18 must not perform hazardous work, night work, overtime, or other work prohibited for their age. Educational placements, internships, and apprenticeships must meet these age and safety requirements and applicable student and young-worker protections.

On identifying prohibited child labor, Suppliers must immediately remove the child from prohibited work, notify IEM, and arrange lawful remediation protecting the child's safety and education. Suppliers must not conceal the violation or transfer the child to other prohibited work.

Employment Authorization

Suppliers must verify and maintain employment authorization as required where the individual works, at legally prescribed times, and through lawful, consistent procedures. For U.S. Form I-9 verification, employees must be allowed to choose acceptable documents that are examined under the legal standard of reasonably appearing genuine and relating to the individual. Suppliers must not demand unnecessary or specific documents or unlawfully discriminate based on citizenship, immigration status, or national origin.

Suppliers must securely retain verification forms and copies of documents as required by law or the verification procedure, or under a lawful, consistent copying policy, and only for permitted periods. E-Verify and additional screening apply where required by law or contract.

Freedom of Association

Suppliers must respect workers' lawful rights to organize, join or assist a union, bargain collectively, engage in protected concerted activity, and refrain from such activity, without interference, threats, discrimination, or retaliation. Where law restricts union activity, Suppliers must allow lawful alternative worker representation. These Standards do not restrict protected discussion of wages, hours, or working conditions, lawful representation, or other protected communications.

Business Integrity

Bribery and Anticorruption

Suppliers must not directly or indirectly offer, promise, authorize, provide, solicit, or accept bribes, kickbacks, or other improper benefits in public or private dealings. Unofficial payments to expedite routine government actions are prohibited, regardless of local practice. If an imminent health or safety threat compels payment, personnel must prioritize safety and report and accurately record it as soon as it is safe to do so; commercial pressure is no exception. Employment offers, referrals, donations, political contributions, sponsorships, and subcontract awards must not be used to secure improper advantages. Suppliers must promptly disclose to ethics@iem.com improper-benefit requests, public-official referrals or recommendations that could influence IEM-related decisions, and relevant personnel's outside offices that could do so. Suppliers must conduct proportionate due diligence on agents used in IEM business, document legitimate services and compensation, and maintain controls to prevent and detect improper payments.

Business Courtesies

Suppliers must not offer, request, provide, or accept business courtesies to improperly influence decisions or obtain advantages. Cash, cash equivalents, personal loans, and discounts unavailable to the public must not be offered to IEM personnel or their families in connection with IEM business. Gifts, meals, entertainment, and travel must not be offered to personnel involved in an active solicitation, an award decision, a significant contract negotiation, a performance remediation, or a dispute involving the Supplier.

Otherwise, modest, infrequent noncash courtesies that serve a legitimate business purpose require compliance with applicable law, recipient rules, and IEM's written policy, as well as advance approval by IEM's authorized ethics and compliance representative. Suppliers must accurately record the courtesy, recipient, purpose, value, and approval. Courtesies to public officials involving IEM business require separate advance written IEM approval and compliance with the official's rules. IEM approval cannot override law or recipient rules.

Conflicts of Interest

Suppliers must identify and promptly disclose actual, potential, or apparent conflicts affecting IEM business

before accepting affected work and when circumstances change. Disclosures must cover relevant financial interests, outside positions, close personal or family relationships with persons able to influence the work or award, and conflicting customer duties. Organizational conflicts include nonpublic information conferring unfair competitive advantage, development of requirements that could favor the Supplier, and work evaluating the Supplier's own interests or prior work.

Suppliers must disclose conflicts to ethics@iem.com and IEM's contract representative, refrain from affected decisions or activities while a material conflict remains unresolved, and implement IEM's written mitigation requirements. IEM approval does not replace customer consent, contracting officer determinations, or legal restrictions. Suppliers must not use nonpublic procurement information or unauthorized contacts to seek an advantage.

Accurate Records and Retention

Suppliers must maintain complete, accurate, timely, and retrievable records supporting IEM business, including invoices, time charges, expenses, qualifications, inspections, deliverable reviews, certifications, and required evidence of compliance. Entries must reflect actual work or transactions and have supporting documentation. Suppliers must not falsify, backdate, conceal, or alter records to misrepresent facts, create misleading records, or improperly charge the same work to multiple customers or funding sources.

Suppliers must retain records, including relevant electronic messages and collaboration records, for legally and contractually required periods and suspend destruction for applicable audits, claims, investigations, litigation, or preservation directions. They must provide lawful access under the agreement and applicable audit provisions and securely dispose of records after retention and preservation duties end.

Money Laundering and Payment Integrity

Suppliers must not use IEM business to launder money, finance terrorism, disguise illegal funds, or evade financial restrictions. Payment arrangements must be legitimate and documented, with contracting and payee entities accurately identified. Suppliers must promptly disclose unexplained third-party payment requests, material discrepancies, or suspected payment fraud. Bank details and payee changes must follow IEM's independently verified change process. Splitting invoices, concealing beneficial recipients, or misstating

transactions to evade approval or legal requirements is prohibited.

Fair Competition and Antitrust

Suppliers must compete independently and comply with antitrust and competition laws. Price-fixing, bid-rigging, unlawful market or customer allocation, wage-fixing, and unlawful recruitment or hiring restrictions are prohibited. Competitively sensitive information must not be exchanged in circumstances that unlawfully restrict competition, even with the information owner's consent. Teaming, subcontracting, and joint development must comply with applicable laws and procurement rules.

Suppliers must protect procurement integrity, communicate about pending bids through authorized channels, and promptly disclose improperly received competitor, bid, or source-selection information without further use or distribution. Channel restrictions do not limit conflict disclosures or protected reports. Deception, misuse of confidential information, and unlawful exclusionary or unfair practices are prohibited. Statements about IEM, Suppliers, competitors, and their products or services must be truthful and supportable.

Insider Trading

Suppliers and their directors, officers, employees, representatives, and business partners must not trade in a company's securities while aware of related material nonpublic information obtained through IEM business, recommend such trading, or improperly disclose that information. They must comply with securities laws and safeguard the information until it is lawfully made public.

Safe and Reliable Operations

Health and Safety

Suppliers must comply with applicable health and safety laws, maintain controls to prevent injury and occupational illness, and provide safe workplaces for workers and affected members of the public. Workers must receive relevant safety training, information, and support before exposure to hazards and when conditions change.

Drivers on IEM work must comply with traffic and transportation laws, hold required licenses, and be fit to drive. Suppliers must provide or require lawful, safe vehicles suited to the assignment and maintained in accordance with applicable requirements and manufacturer instructions. Drivers must wear seat belts and must not text or use devices in ways that impair safe driving.

Suppliers must maintain and periodically test emergency plans appropriate to IEM work, covering evacuation, contacts, medical assistance, and communications. Potable water and sanitary restrooms must be accessible; supplied food facilities and housing must be safe and sanitary.

Suppliers must assess hazards before work and when conditions change, including public safety and relevant heat, fatigue, hazardous-substance, driving, and disaster-site risks. They must eliminate hazards where practicable and otherwise reduce exposure through engineering and administrative controls and appropriate protective equipment, provided to workers without charge. Suppliers must provide understandable training and coordinate emergency arrangements with IEM and site operators. Workers must be authorized to stop or decline reasonably perceived unsafe work without retaliation; work may resume only after hazards are evaluated and adequately controlled.

Suppliers must immediately notify IEM's site or contract representative of serious injuries, imminent danger, violence, or other significant safety events affecting IEM work, and promptly report other work-related incidents and near misses. They must preserve required records, investigate causes, and take corrective action. Threats, violence, and physical intimidation are prohibited. Weapons are prohibited in IEM-controlled workplaces and work areas unless IEM authorizes them in writing for the assignment or law requires otherwise, including protected possession or storage rights.

Environment

Suppliers must comply with environmental laws and maintain required licenses, permits, and registrations. Measures proportionate to environmental impacts must conserve resources, prevent pollution, protect the environment, and reduce waste, emissions, and energy and water use.

Suppliers must identify and control the material environmental impacts of IEM work, including hazardous material handling and disposal, pollution, waste, and discharges. Assessments must address climate risks, water use, biodiversity, and community impacts where material to the work. Suppliers must meet applicable restricted-substance and environmental labeling requirements and promptly notify IEM of any releases, permit failures, or enforcement actions that materially affect work. Upon reasonable contract-related request, they must provide supportable information on resource

use, waste, and emissions; identify estimates and methodologies; cooperate with agreed-upon improvements; and assess their effectiveness. Environmental claims concerning IEM work must be accurate and supported.

Registrations and Certifications

Suppliers must maintain legally or contractually required licenses, registrations, certifications, insurance, and supporting documentation, and immediately inform IEM of any lapses, changes, or inaccuracies in required documentation.

Suppliers must provide accurate, current representations of required eligibility, ownership, qualifications, licensing, insurance, and socioeconomic status. They must immediately notify IEM of suspension, debarment, proposed debarment, exclusion, loss of required status, or other restrictions affecting eligibility or performance. Suppliers must not use ineligible lower-tier parties where prohibited and must support required screening and disclosures.

Government Contracts and Public Funds

For publicly funded work, including government contracts, grants, and cooperative agreements, Suppliers must meet requirements applicable to their scope and funding, incorporated clauses, and required lower-tier flow-downs. They must not submit or cause to be submitted false claims, certifications, time charges, expenses, eligibility statements, or reimbursement requests. Discovered billing errors or overpayments must be promptly disclosed and corrected or refunded, as required by law and the agreement. Suppliers must not misrepresent qualifications, small-business status, work performed, domestic origin, or compliance with labor, security, or purchasing restrictions.

Suppliers must comply with applicable lobbying, gratuity, procurement information, prohibited product or technology, cost allowability, allocation, payment, and subcontracting requirements. They must make required government disclosures and cooperate with lawful audits and investigations; notice to IEM does not replace or postpone independent reporting duties. Uncertainty about required clauses or customer instructions must be raised with IEM's contract representative for written direction before affected work proceeds.

Supply Chain Security

Suppliers must protect supplied goods and materials through controls appropriate to their role, including the

use of approved transport providers, shipment identification, tamper prevention, and traceability. International shipments must comply with customs and cargo security laws and with applicable authorized economic operator or comparable program requirements, including those expressly required by the agreement. Suppliers must promptly notify IEM of material loss, tampering, diversion, or security failures affecting IEM shipments and cooperate in containment and investigation.

Business Continuity

Suppliers of contractually designated critical goods or services must maintain, periodically test, and update appropriate continuity and recovery arrangements, reassessing them after material changes or disruptions. Arrangements must address loss of key personnel, facilities, systems, utilities, transport, and critical lower tiers, and identify responsible contacts and alternate performance methods. Suppliers must meet agreed recovery objectives, promptly notify IEM of actual or reasonably anticipated material disruptions, expected effects, and mitigation, and cooperate with IEM's response and contractually required transitions while maintaining safety, security, and legal compliance.

Quality and Counterfeit Prevention

Suppliers must safeguard the health and safety of workers, customers, and end users when designing, producing, and delivering products and services. Appropriate quality assurance must prevent, detect, report, and correct defects and ensure contractual, legal, and regulatory compliance. Qualified, authorized personnel must complete and document required inspections and tests.

Suppliers must use appropriate sourcing and traceability controls to prevent counterfeit parts and materials. Goods must come from original manufacturers or authorized sources where available; alternative sources must be contractually permitted, with risks documented and controlled. Suspected counterfeits must be segregated and kept out of circulation. Suppliers must notify IEM and other recipients as required, cooperate in lawful disposition, and impose equivalent duties on relevant lower tiers.

Professional and technical services require qualified personnel, verification of material facts and calculations, and appropriate review. Suppliers must not fabricate qualifications, resumes, sources, inspection results, site visits, work records, or evidence. They must promptly

identify and disclose material errors, defects, suspected counterfeits, or unauthorized substitutions affecting IEM work that pose risks, and cooperate in contractually required correction, replacement, or recall. Changes to approved personnel, materials, methods, or deliverables require contractually specified approvals. These duties also apply to work produced using automation or artificial intelligence ("AI").

International Trade

Suppliers must comply with applicable import, export, re-export, retransfer, sanctions, embargo, and antiboycott requirements, obtain the required registrations, licenses, and authorizations before engaging in affected activities, and comply with their conditions. U.S. Department of State Directorate of Defense Trade Controls (DDTC) registration, where required, does not, by itself, authorize exports. Suppliers must identify and communicate relevant classifications and restrictions for goods, software, technology, technical data, defense articles, and defense services provided for IEM work, and prevent unauthorized transfers or access, including controlled access by foreign persons.

Suppliers must conduct proportionate due diligence on relevant parties, beneficial ownership and control, destinations, end users, and end uses, including restricted-party screening and review of changes during performance. Prohibited transactions require legally effective authorization. Suppliers must promptly notify IEM of restrictions, denied or revoked authorizations, prohibited boycott requests, or suspected violations affecting IEM work, and independently make required reports. Intermediaries and altered shipment or payment information must not be used to evade restrictions.

Suppliers must not supply goods prohibited by forced-labor import laws. For goods and materials that present sourcing risks, they must retain and, upon reasonable request, provide origin and supply chain information to support applicable import and customer requirements. Suppliers must conduct risk-based due diligence on conflict and human-rights risks in minerals and other materials, comply with applicable conflict-minerals laws, and provide accurate information for IEM's required sourcing disclosures.

Information and Assets

Information Security and Privacy

Suppliers must protect the confidentiality, integrity, and availability of IEM and customer information, including

personal, proprietary, and regulated information. Collection, use, disclosure, and retention must be authorized for the work and lawful. A documented security program proportionate to the information and services must include least-privilege access for authorized persons with a business need, multifactor authentication for remote and privileged access, appropriate encryption in transit and at rest, timely vulnerability remediation, malware protection, logging, secure backups with tested restoration, and tested incident response. Suppliers must maintain an inventory of systems that handle IEM information, use supported software, and periodically test safeguards.

Suppliers must comply with applicable privacy laws and contractual processing restrictions. IEM's prior written authorization and compliance with legal transfer requirements are required before adding processors, processing or storage countries, or access from unapproved countries for IEM or customer information. Approved sub-processors must be bound to appropriate protective terms. Suppliers must not sell IEM or customer personal information or use it for unrelated advertising. Training or improving AI systems with that information requires IEM's express written authorization and a lawful basis. They must use approved channels and timely assist with required privacy assessments, notices, and individual rights requests.

Suppliers must immediately notify IEM's designated security contact and contract representative of actual or reasonably suspected incidents affecting IEM or customer information security or contracted service delivery, with initial notice no later than 24 hours after discovery or any shorter legal or contractual deadline. If no security contact is designated, notify ethics@iem.com and the contract representative. Notice must not await confirmation or a completed investigation. Initial notice must provide known facts and a response contact; updates must cover material developments, containment, affected information and services, and corrective actions. Suppliers must promptly contain and mitigate incidents, preserve evidence, cooperate in response, and exchange sensitive details through approved secure channels. The IEM notice does not replace the required reports to authorities or affected persons. Where required, Suppliers must promptly provide IEM the government incident-report number.

Suppliers must not receive or access classified information, controlled unclassified information, federal

contract information, or other specially restricted information before required authorizations, personnel and facility requirements, and contractual safeguards are satisfied. They must comply with applicable federal safeguarding, cyber-reporting, assessment, certification, and lower-tier requirements, including required National Institute of Standards and Technology (NIST) SP 800-171 implementation, assessment results, Cybersecurity Maturity Model Certification (CMMC) status and affirmations, and cloud safeguards. The agreement and binding requirements govern the version, level, scope, and timing; these Standards do not independently require certification from every Supplier. At the end of authorized use or upon IEM's request, Suppliers must return or securely delete information as contractually required, subject to lawful retention and preservation, and protect retained copies against further use or disclosure.

Intellectual Property

Suppliers must use intellectual property only with valid rights and permissions and meet contractual ownership, licensing, confidentiality, and delivery requirements. They must identify third-party and open-source components, comply with their licenses, and obtain required approval before including material whose terms limit agreed customer rights or require disclosure or licensing of IEM or customer proprietary material.

Software and Technology Security

Suppliers developing, configuring, or maintaining technology for IEM must use secure development and change controls proportionate to risk, protect access to development and production environments, assess third-party components, and address known vulnerabilities. They must promptly disclose material vulnerabilities, provide agreed security updates and support, and give contractually sufficient end-of-support notice. Software inventories, component disclosures, and secure-development attestations must be provided where legally or contractually required.

Artificial Intelligence

Suppliers must obtain IEM's prior written approval before using AI for IEM deliverables, entering IEM or customer nonpublic information into AI systems, or using AI to make or materially inform decisions affecting individuals in IEM work. Approval must specify tools, purposes, information, and safeguards, including embedded AI features, and be renewed before material changes in use or risk. Suppliers must meet applicable IEM and customer

requirements and prevent unauthorized model training, unauthorized retention of information, or unauthorized secondary use of information.

Suppliers remain responsible for the accuracy, completeness, security, legality, and intellectual property compliance of AI-assisted work. Qualified personnel must verify material outputs against reliable sources before delivery or use and review the risks of material errors and unlawful discrimination. Suppliers must disclose approved material AI use with deliverables, retain records demonstrating the required review, and promptly report material AI errors or incidents affecting IEM work. AI must not independently determine public-benefit eligibility, employment outcomes, or other consequential decisions unless permitted by law and customer requirements, and expressly authorized in writing by IEM for the specific process and safeguards, including qualified human oversight and review of challenged outcomes.

Protection of Property and Access

Suppliers must safeguard IEM and customer property, funds, equipment, systems, credentials, keys, badges, and access devices and use them only for authorized work. Account or password sharing, access device duplication, security control bypasses, and unauthorized entry or access are prohibited. Personnel must follow applicable site and system rules provided for the assignment.

Suppliers must promptly report loss, theft, misuse, or unauthorized access. When worker authorization ends, or access is no longer needed, they must immediately notify IEM, restrict access they control, and return property and access devices as directed. IEM credentials or access must not be used to market unrelated services, imply endorsement, or gain personal advantage.

Publicity and External Communications

Suppliers must obtain IEM's authorized communications representative's prior written approval to use IEM or customer names, logos, trademarks, project details, testimonials, or work product in advertising, proposals to unrelated parties, press releases, case studies, or social media. Required customer authorization must also be obtained. Suppliers must not imply IEM or customer endorsement or authorize anyone to speak for IEM without written approval.

Before photographing, recording, or publishing images or information about IEM work, facilities, personnel, customers, or beneficiaries, Suppliers must meet

applicable privacy, consent, confidentiality, and site requirements. Media inquiries concerning IEM business must go to IEM's contract representative, subject to the Reporting and Nonretaliation section's protected communications.

Compliance and Accountability

Compliance Management and Lower Tiers

Suppliers must implement these Standards through policies, assigned responsibility, training, and controls proportionate to their IEM work and risk. They must assess lower-tier risks before engagement, periodically during performance, and after material changes; management must periodically review controls and correct weaknesses. Suppliers must communicate applicable requirements to lower tiers, contractually require substantively equivalent compliance, and, where appropriate, further flow down requirements and monitor compliance. Exact language must be flowed down where legally or contractually required. Suppliers must obtain required approval before subcontracting or changing approved lower tiers and keep current records of lower tiers engaged in IEM work. Suppliers remain responsible to IEM for obligations performed through their personnel, agents, and lower tiers.

Verification and Cooperation

Upon request, an authorized Supplier representative must acknowledge in writing receipt of and agreement to comply with the applicable Standards, and confirm that the requirements have been communicated to the responsible persons. After reasonable inquiry, the representative must confirm compliance or, in writing, disclose known material noncompliance, relevant conflicts, or inability to comply, along with corrective actions. Suppliers must promptly disclose material changes and provide accurate supporting evidence, including records of training, due diligence, and corrective actions. Acknowledgment neither authorizes exceptions nor limits reporting or cooperation. IEM or its authorized assessor may review relevant records, facilities, systems, and practices through proportionate assessments on reasonable notice, subject to law and reasonable security safeguards. Credible allegations or imminent risks require cooperation with urgent review without unnecessary delay. No attorney-client privilege or work-product waiver, or legally prohibited disclosure, is required; Suppliers must identify limitations' bases and cooperate in lawful alternatives. Unrelated customer

information must be protected. Government audit and access rights remain unaffected.

Corrective Action and Remedies

Suppliers must promptly contain and correct noncompliance and notify IEM of material findings. Corrective action must be proportionate, address harm to people and process failures, and be assessed for effectiveness. Within 10 business days after IEM's request, or a shorter reasonable period IEM specifies for urgent risks, Suppliers must submit a plan identifying causes, responsible persons, actions, and completion dates, and provide completion evidence. As the agreement and law permit, IEM may require further verification, restrict access, suspend affected work or new awards, require removal of affected personnel from IEM work, or terminate for material or repeated violations, materially false certifications, obstruction of authorized review, or failure to complete required corrective action. IEM may immediately restrict access to IEM-controlled premises, systems, or information or suspend affected work when reasonably necessary to address imminent safety or security threats or credible evidence of fraud or trafficking affecting work, as the agreement and law permit. Notice, cure, termination, costs, and payment treatment remain governed by the agreement and law. No IEM review, inspection, payment, or acceptance, including of corrective action, waives violations or relieves Supplier obligations except by an express written waiver authorized under the agreement.

Order of Precedence

Law and binding regulatory requirements control. Subject to them, the agreement's express order of precedence governs; otherwise, the agreement and its other incorporated terms prevail over these Standards. Silence is not a conflict; compatible requirements apply together. Suppliers must promptly disclose any inconsistencies and seek written clarification before any affected work proceeds, without performing any unlawful work. Exceptions require specific written approval by an authorized IEM representative and cannot waive law or binding customer requirements. Contractual changes require the amendment procedure set out in the agreement. The identified or incorporated version of these Standards governs; later publication or delivery changes obligations only through that procedure. These Standards do not themselves create IEM employment or third-party contractual rights, or limit statutory rights or protected reporting.

Reporting and Nonretaliation

Suppliers must provide accessible reporting channels for workers, business partners, and affected persons, including anonymous reporting where lawful, and explain handling procedures in an understandable form and language. Reports must be promptly assessed and impartially investigated, with appropriate feedback and the protection of reports and reporters' identities, consistent with the law and a fair investigation. Suppliers must promptly report actual or reasonably suspected violations of law, these Standards, or applicable IEM requirements affecting IEM business to ethics@iem.com without awaiting an internal investigation. Anyone may report directly to IEM. Suppliers must protect persons who raise good-faith concerns, seek advice, refuse to engage in misconduct, or assist in investigations, even if the concerns are unsubstantiated. Retaliation, threats, intimidation, and attempts to identify or punish anonymous reporters are prohibited. Suppliers must provide legally or contractually required written whistleblower notices, cooperate with lawful investigations, preserve evidence, and take corrective action. IEM will limit disclosure to persons with a legitimate need to know, subject to investigative and legal requirements.

Nothing in these Standards or related instructions restricts lawful communications with government agencies, law enforcement, inspectors general, legal counsel, or worker representatives; protected disclosures or participation in investigations; lawful discussion of wages or working conditions; or legally available whistleblower awards. No prior notice or approval from IEM or the Supplier is required. Confidentiality terms and other instructions must not restrict these rights or require internal reporting before protected external disclosure. These protections govern every provision, including confidentiality, publicity, records, and cooperation. Suppliers must withdraw conflicting existing restrictions and notify affected personnel and lower tiers. Lawful safeguards for classified information remain applicable.

Under 18 U.S.C. § 1833(b), individuals are immune from civil or criminal liability under federal or state trade-secret law for disclosing a trade secret in confidence, directly or indirectly, to a federal, state, or local government official or an attorney solely to report or investigate a suspected legal violation, or in a document filed under seal in a lawsuit or other proceeding. Individuals suing for employer retaliation for reporting a

suspected legal violation may disclose trade secrets to their attorneys and use them in the proceeding if documents containing them are filed under seal and further disclosure occurs only by court order. Suppliers must provide legally required notice of this immunity in covered confidentiality agreements with employees, including individual contractors and consultants.

Except for protected communications or legally prohibited notice, Suppliers must promptly notify IEM's contract representative of subpoenas, regulatory requests, media inquiries, and other third-party requests concerning IEM business. Independently required authority reports must meet applicable deadlines. For immediate threats to life or safety, contact emergency services first, then IEM's applicable site or contract emergency channel.